PERATURAN MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2026
TENTANG
PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA,

Menimbang :

a. bahwa untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya, perlu meningkatkan penerapan sistem pemerintahan berbasis elektronik;
b. bahwa berdasarkan ketentuan Pasal 60 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, setiap pimpinan instansi pusat mempunyai tugas melakukan koordinasi dan menetapkan kebijakan sistem pemerintahan berbasis elektronik di instansi pusat;
c. bahwa Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 9 Tahun 2023 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik sudah tidak sesuai dengan perkembangan hukum dan kebutuhan organisasi, sehingga perlu diganti;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Menteri Pekerjaan Umum tentang Penerapan Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916) sebagaimana telah diubah dengan Undang-Undang Nomor 61 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 225, Tambahan Lembaran Negara Republik Indonesia Nomor 6994);

3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
5. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);
6. Peraturan Presiden Nomor 170 Tahun 2024 tentang Kementerian Pekerjaan Umum (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 366);
7. Peraturan Menteri Pekerjaan Umum Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja Kementerian Pekerjaan Umum (Berita Negara Republik Indonesia Tahun 2024 Nomor 955);
8. Peraturan Menteri Pekerjaan Umum Nomor 1 Tahun 2025 tentang Organisasi dan Tata Kerja Unit Pelaksana Teknis di Kementerian Pekerjaan Umum (Berita Negara Republik Indonesia Tahun 2025 Nomor 252);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PEKERJAAN UMUM TENTANG PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

## BAB I
## KETENTUAN UMUM

### Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
2. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
3. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta Layanan SPBE yang berkualitas.
4. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi Aplikasi SPBE dan yang memiliki nilai manfaat.
5. Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi Proses Bisnis, Data dan Informasi, Infrastruktur SPBE, Aplikasi SPBE, dan Keamanan SPBE untuk menghasilkan Layanan SPBE yang terintegrasi.
6. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan serta pelaksanaan SPBE yang terintegrasi.

7. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi.
8. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
9. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
10. Pusat Data Nasional adalah sekumpulan pusat data yang digunakan secara bersama dan bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung yang terdiri atas pusat data yang diselenggarakan oleh instansi pusat/pemerintah daerah dengan memenuhi persyaratan pusat data atau pusat data yang dibangun khusus untuk digunakan secara bersama dan bagi pakai oleh instansi pusat dan pemerintah daerah.
11. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
12. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
13. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah.
14. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh Kementerian untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
15. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
16. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/standar yang telah ditetapkan.
17. Data adalah catatan atas kumpulan fakta atau deskripsi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, suara, dan/atau bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.
18. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik

19. Pusat Data dan Teknologi Informasi yang selanjutnya disebut Pusdatin adalah unit kerja di bawah koordinasi Sekretaris Jenderal Kementerian yang mempunyai tugas melaksanakan pengelolaan Data, Informasi, dan teknologi informasi Kementerian serta pengelolaan sistem dan data bencana infrastruktur.
20. Unit Data dan Informasi yang selanjutnya disebut Unit Datin adalah unit kerja di masing-masing Unit Organisasi yang melaksanakan fungsi pengelolaan Data, Informasi, dan teknologi informasi.
21. Unit Organisasi adalah satuan organisasi dalam Kementerian yang dipimpin oleh pimpinan tinggi madya.
22. Unit Kerja adalah satuan organisasi dalam Kementerian yang dipimpin oleh pimpinan tinggi pratama.
23. Unit Pelaksana Teknis yang selanjutnya disingkat UPT adalah satuan kerja yang bersifat mandiri yang melaksanakan tugas teknis operasional tertentu dan/atau tugas teknis penunjang tertentu di Kementerian.
24. Kementerian adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pekerjaan umum.
25. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pekerjaan umum.

Pasal 2

(1) Peraturan Menteri ini dimaksudkan sebagai pedoman bagi Unit Organisasi, Unit Kerja, dan UPT dalam penyelenggaraan SPBE di Kementerian.
(2) Peraturan Menteri ini bertujuan untuk mewujudkan keterpaduan dan efisiensi dalam penyelenggaraan SPBE dan mendukung pencapaian indeks SPBE sesuai sasaran strategis Kementerian.

Pasal 3

Lingkup Peraturan Menteri ini meliputi:
a. Tata Kelola SPBE;
b. Manajemen SPBE;
c. Audit TIK;
d. tim koordinasi SPBE; dan
e. pemantauan dan evaluasi SPBE.

BAB II
TATA KELOLA SPBE

Pasal 4

(1) Menteri menyelenggarakan penataan dan pengelolaan SPBE secara terpadu.
(2) Penataan dan pengelolaan sebagaimana dimaksud pada ayat (1) dilakukan terhadap unsur SPBE.
(3) Unsur SPBE sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. Arsitektur SPBE;
    b. Peta Rencana SPBE;
    c. rencana dan anggaran SPBE;
    d. Proses Bisnis;
    e. Data dan Informasi;

f. Infrastruktur SPBE;
g. Aplikasi SPBE;
h. Keamanan SPBE; dan
i. Layanan SPBE.

Pasal 5

(1) Arsitektur SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf a bertujuan untuk memberikan panduan dalam pelaksanaan integrasi Proses Bisnis, Data dan Informasi, Infrastruktur SPBE, Aplikasi SPBE, dan Keamanan SPBE untuk menghasilkan Layanan SPBE yang terpadu sesuai dengan ketentuan peraturan perundang-undangan.
(2) Arsitektur SPBE sebagaimana dimaksud pada ayat (1) disusun dalam bentuk:
    a. referensi arsitektur;
    b. domain arsitektur; dan
    c. metadata arsitektur.
(3) Referensi Arsitektur sebagaimana dimaksud pada ayat (2) huruf a mendeskripsikan komponen dasar arsitektur baku yang dapat digunakan sebagai acuan untuk penyusunan domain arsitektur.
(4) Domain arsitektur sebagaimana dimaksud pada ayat (2) huruf b mendeskripsikan substansi arsitektur yang memuat domain arsitektur:
    a. Proses Bisnis;
    b. Data dan informasi;
    c. Infrastruktur SPBE;
    d. Aplikasi SPBE;
    e. Keamanan SPBE; dan
    f. Layanan SPBE.
(5) Metadata arsitektur sebagaimana dimaksud pada ayat (2) huruf c memberikan informasi terstruktur setiap entitas yang disebutkan dalam domain arsitektur.

Pasal 6

(1) Penyusunan Arsitektur SPBE sebagaimana dimaksud dalam Pasal 5 ayat (1) dilakukan oleh Pusdatin.
(2) Dalam penyusunan Arsitektur SPBE sebagaimana dimaksud pada ayat (1) Pusdatin berkoordinasi dengan seluruh unit kerja.
(3) Dalam menyusun Arsitektur SPBE sebagaimana dimaksud pada ayat (2), Pusdatin dapat:
    a. berkoordinasi dengan instansi pusat dan/atau daerah lainnya untuk memastikan terjadinya integrasi penerapan SPBE yang dibutuhkan; dan
    b. melakukan konsultasi dengan tim koordinasi SPBE nasional untuk menyelaraskan dengan Arsitektur SPBE nasional.
(4) Arsitektur SPBE ditetapkan oleh Menteri untuk jangka waktu 5 (lima) tahun.

Pasal 7

(1) Arsitektur SPBE sebagaimana dimaksud dalam Pasal 6 ayat (4) dilakukan reviu pada paruh waktu dan tahun terakhir pelaksanaan atau sesuai dengan kebutuhan.
(2) Reviu Arsitektur SPBE Kementerian dilakukan berdasarkan:
    a. perubahan Arsitektur SPBE nasional;
    b. hasil pemantauan dan evaluasi SPBE di Kementerian;
    c. perubahan pada unsur SPBE; atau
    d. perubahan rencana strategis Kementerian.
(3) Reviu sebagaimana dimaksud pada ayat (2) dilakukan oleh Pusdatin.
(4) Hasil reviu sebagaimana dimaksud pada ayat (3) dilaporkan pada tim koordinasi SPBE.
(5) Dalam hal hasil reviu sebagaimana dimaksud pada ayat (4) terdapat perubahan, Arsitektur SPBE ditetapkan kembali.

Pasal 8

(1) Peta Rencana SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf b disusun sesuai ketentuan peraturan perundang-undangan.
(2) Peta Rencana SPBE sebagaimana dimaksud pada ayat (1) memuat perencanaan kegiatan:
    a. Tata Kelola SPBE;
    b. Manajemen SPBE;
    c. Layanan SPBE;
    d. Infrastruktur SPBE;
    e. Aplikasi SPBE;
    f. Keamanan SPBE; dan
    g. Audit TIK.
(3) Penyusunan Peta Rencana SPBE dilakukan oleh Pusdatin.
(4) Dalam penyusunan Peta Rencana SPBE sebagaimana dimaksud pada ayat (3) berkoordinasi dengan seluruh unit kerja dalam menyusun Peta Rencana SPBE.
(5) Dalam menyusun Peta Rencana SPBE, Pusdatin dapat melakukan konsultasi dengan tim koordinasi SPBE nasional untuk menyelaraskan dengan Peta Rencana SPBE nasional.
(6) Peta Rencana SPBE ditetapkan oleh Menteri untuk jangka waktu 5 (lima) tahun.

Pasal 9

(1) Peta Rencana SPBE sebagaimana dimaksud dalam Pasal 8 ayat (6) ditindaklanjuti dengan menyusun rancangan rinci inisiatif pada Peta Rencana SPBE oleh Unit Organisasi dan Unit Kerja.
(2) Dalam menyusun rancangan rinci inisiatif sebagaimana dimaksud pada ayat (1) Unit Organisasi dan Unit Kerja berkoordinasi dengan Pusdatin dan Unit Datin.

Pasal 10

(1) Peta Rencana SPBE sebagaimana dimaksud dalam Pasal 8 ayat (6) dilakukan reviu pada paruh waktu dan tahun terakhir pelaksanaan atau sesuai dengan kebutuhan.

(2) Reviu Peta Rencana SPBE dilakukan berdasarkan:
a. perubahan Arsitektur SPBE;
b. perubahan Rencana Kerja Kementerian; atau
c. hasil pemantauan dan evaluasi SPBE Kementerian.
(3) Reviu sebagaimana dimaksud pada ayat (2) dilakukan oleh Pusdatin.
(4) Hasil reviu sebagaimana dimaksud pada ayat (3) dilaporkan pada tim koordinasi SPBE.
(5) Dalam hal hasil reviu sebagaimana dimaksud pada ayat (4) terdapat perubahan, Peta Rencana SPBE ditetapkan kembali.

Pasal 11

(1) Rencana dan anggaran SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf c disusun secara terpadu.
(2) Rencana dan anggaran SPBE sebagaimana dimaksud pada ayat (1) disusun oleh Unit Organisasi, Unit Kerja, dan/atau UPT berdasarkan pada Arsitektur SPBE dan Peta Rencana SPBE sesuai dengan ketentuan peraturan perundang-undangan.
(3) Unit Organisasi, Unit Kerja, dan/atau UPT dalam penyusunan rencana dan anggaran SPBE harus berkoordinasi dengan Pusdatin bersama dengan unit kerja di sekretariat jenderal yang mempunyai tugas melaksanakan koordinasi administrasi penganggaran, pemantauan dan evaluasi program dan kegiatan, serta kerja sama luar negeri Kementerian.
(4) Rencana dan anggaran SPBE Unit Organisasi, Unit Kerja, dan/atau UPT harus mendapat rekomendasi dari Pusdatin berdasarkan hasil koordinasi sebagaimana dimaksud pada ayat (3).

Pasal 12

(1) Proses Bisnis sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf d sebagai acuan dalam penggunaan Data dan Informasi serta penerapan Aplikasi SPBE, Keamanan SPBE, dan Layanan SPBE.
(2) Penyusunan Proses Bisnis sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Pusdatin bersama dengan unit kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian sesuai dengan ketentuan peraturan perundang-undangan.
(3) Proses Bisnis sebagaimana dimaksud pada ayat (1), dilakukan penyesuaian melalui inovasi Proses Bisnis yang dikoordinasikan oleh Pusdatin bersama dengan unit kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian.

Pasal 13

(1) Data dan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf e mencakup semua jenis Data dan Informasi yang dimiliki oleh Kementerian dan/atau yang diperoleh dari masyarakat, pelaku usaha, dan/atau pihak lain.

(2) Penyediaan dan pengelolaan Data dan Informasi dilakukan berdasarkan pada prinsip Satu Data Indonesia.
(3) Pihak terkait dalam penyediaan, pengelolaan, dan penggunaan Data dan Informasi Kementerian terdiri atas:
   a. Walidata Kementerian yaitu Pusdatin dan mewakili Kementerian pada forum satu data indonesia;
   b. koordinator produsen data yaitu Unit Datin;
   c. produsen data yaitu Unit Kerja dan/atau UPT yang menghasilkan data sesuai dengan tugas dan fungsinya;
   d. Pengguna Data Kementerian yaitu instansi pusat, pemerintah daerah, perseorangan, kelompok orang, atau badan hukum yang menggunakan data dariKementerian; dan
   e. Forum Satu Data Kementerian yaitu wadah komunikasi dan koordinasi Kementerian dan/atau antar Unit Organisasi untuk penyelenggaraan Satu Data Indonesia bidang pekerjaan umum.

Pasal 14

(1) Penggunaan Data dan Informasi sebagaimana dimaksud dalam Pasal 13 ayat (3) dilakukan dengan mengutamakan bagi pakai Data dan Informasi antar Unit Kerja di Kementerian, instansi pusat, dan/atau pemerintah daerah dengan berdasarkan tujuan dan cakupan, penyediaan akses Data dan Informasi, dan pemenuhan standar interoperabilitas Data dan Informasi.
(2) Bagi pakai Data dan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Pusdatin.
(3) Standar interoperabilitas Data dan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

(1) Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf f digunakan untuk meningkatkan efisiensi, keamanan, dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur SPBE bagi Unit Organisasi, Unit Kerja, dan UPT.
(2) Pembangunan dan pengembangan Infrastruktur SPBE harus didasarkan pada Arsitektur SPBE.
(3) Infrastruktur SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. Pusat Komputasi;
   b. Pusat Kendali;
   c. Jaringan Intra Kementerian;
   d. Sistem Penghubung Layanan Kementerian; dan
   e. Platform.
(4) Setiap Unit Organisasi, Unit Kerja, dan UPT harus memanfaatkan Infrastruktur SPBE sebagaimana dimaksud pada ayat (3).
(5) Dalam memanfaatkan Infrastruktur SPBE sebagaimana dimaksud pada ayat (4) Unit Organisasi, Unit Kerja, dan UPT harus berkoordinasi dengan Unit Datin dan Pusdatin.

(6) Kementerian harus memanfaatkan Pusat Data Nasional sebagai jaringan server utama.
(7) Penggunaan infrastruktur di luar Pusat Data Nasional dapat dilakukan dengan kajian dan pertimbangan Unit Datin dan persetujuan Pusdatin serta tim koordinasi SPBE.
(8) Pemanfaatan Pusat Data Nasional sebagaimana dimaksud pada ayat (5) dikelola dan dikoordinasikan oleh Pusdatin bekerja sama dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 16

(1) Pusat Komputasi sebagaimana dimaksud dalam Pasal 15 ayat (3) huruf a merupakan fasilitas yang digunakan untuk keperluan pemrosesan komputasi tertentu atau penempatan sistem komputasi tertentu.
(2) Pusat Komputasi sebagaimana dimaksud pada ayat (1) dikelola oleh Pusdatin.

Pasal 17

(1) Pusat Kendali sebagaimana dimaksud dalam Pasal 15 ayat (3) huruf b merupakan fasilitas yang digunakan untuk keperluan pengendalian dan pengoperasian dari sebuah lingkungan sistem.
(2) Pusat Kendali sebagaimana dimaksud pada ayat (1) dikelola oleh Pusdatin.

Pasal 18

(1) Jaringan Intra Kementerian sebagaimana dimaksud dalam Pasal 15 ayat (3) huruf c merupakan jaringan tertutup yang menghubungkan antara subsistem atau simpul jaringan dalam Kementerian.
(2) Jaringan Intra Kementerian sebagaimana dimaksud pada ayat (1) dikelola oleh Pusdatin.
(3) Jaringan Intra Kementerian sebagaimana dimaksud pada ayat (2) berinterkoneksi dengan Jaringan Intra instansi pusat dan/atau pemerintah daerah lainnya melalui Jaringan Intra Pemerintah.
(4) Pemanfaatan Jaringan Intra Pemerintah sebagaimana dimaksud pada ayat (3) dikelola dan dikoordinasikan oleh Pusdatin bekerja sama dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi sesuai dengan ketentuan peraturan perundang-undangan.
(5) Subsistem atau simpul jaringan Kementerian sebagaimana dimaksud pada ayat (1) yang berlokasi di luar kantor pusat Kementerian, dikelola oleh Unit Datin berkoordinasi dengan Pusdatin.
(6) Integrasi antar Subsistem atau simpul jaringan Kementerian yang dikelola oleh Unit Datin sebagaimana dimaksud pada ayat (5) dilaksanakan oleh Pusdatin.

Pasal 19

(1) Penggunaan Sistem Penghubung Layanan Kementerian sebagaimana dimaksud dalam Pasal 15 ayat (3) huruf d bertujuan untuk memudahkan dalam melakukan integrasi antar Layanan SPBE.
(2) Sistem Penghubung Layanan Kementerian sebagaimana dimaksud pada ayat (1) diselenggarakan, dikelola, dan dikoordinasikan oleh Pusdatin.
(3) Sistem Penghubung Layanan Kementerian harus memiliki konektivitas dengan Sistem Penghubung Layanan Pemerintah sesuai dengan ketentuan peraturan perundang-undangan.
(4) Pemanfaatan Sistem Penghubung Layanan Pemerintah sebagaimana dimaksud pada ayat (3) dikelola dan dikoordinasikan oleh Pusdatin bekerja sama dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

(1) Platform sebagaimana dimaksud dalam Pasal 15 ayat (3) huruf e merupakan kerangka infrastruktur dan aplikasi yang digunakan lingkungan kerja yang mendukung aplikasi atau lingkungan dengan virtualisasi sebagai layanan platform berdasarkan teknologi awan untuk lingkungan kerja aplikasi.
(2) Platform sebagaimana dimaksud pada ayat (1) dikelola oleh Pusdatin dan Unit Datin.
(3) Pemanfaatan platform sebagaimana dimaksud pada ayat (1) harus dikoordinasikan dan mendapat persetujuan dari Pusdatin sejak tahap perencanaan sampai dengan tahap implementasi.

Pasal 21

(1) Pusdatin melakukan reviu dan evaluasi terhadap Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 15 ayat (3) minimal 1 (satu) tahun sekali.
(2) Hasil reviu dan evaluasi terhadap Infrastruktur SPBE sebagaimana dimaksud pada ayat (1) dilaporkan kepada Sekretaris Jenderal Kementerian selaku ketua tim pengarah pada tim koordinasi SPBE Kementerian.

Pasal 22

(1) Aplikasi SPBE sebagaimana dimaksud dalam Pasal 4 ayat 3) huruf g digunakan oleh Kementerian untuk memberikan Layanan SPBE.
(2) Aplikasi SPBE terdiri atas:
    a. Aplikasi Umum; dan
    b. Aplikasi Khusus.
(3) Aplikasi SPBE sebagaimana dimaksud pada ayat (2) dibangun, dikembangkan, dan dimanfaatkan, berdasarkan:
    a. Arsitektur SPBE;
    b. hasil reviu dan evaluasi; dan
    c. rekomendasi hasil Audit TIK.

(4) Pembangunan atau pengembangan dan pemanfaatan aplikasi sejenis Aplikasi Umum hanya dapat dilakukan pada kondisi tertentu dengan persetujuan tim koordinasi SPBE melalui Pusdatin serta mematuhi ketentuan peraturan perundang-undangan.
(5) Pembangunan atau pengembangan dan pemanfaatan Aplikasi SPBE sebagaimana dimaksud pada ayat (2) harus memenuhi standar teknis dan prosedur pembangunan dan pengembangan aplikasi sesuai dengan ketentuan peraturan perundangan-undangan.

Pasal 23

(1) Aplikasi Khusus sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b yang telah dibangun, dikembangkan, dan dimanfaatkan oleh Kementerian dapat diajukan menjadi Aplikasi Umum sesuai dengan ketentuan peraturan perundang-undangan.
(2) Pengajuan Aplikasi Khusus menjadi Aplikasi Umum sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Pusdatin.

Pasal 24

(1) Aplikasi Khusus sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b dapat dirancang, dibangun, dan/atau dikembangkan oleh Unit Organisasi, Unit Kerja, atau Pusdatin.
(2) Dalam melakukan perancangan, Pembangunan, dan/atau pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (1), Unit Kerja atau UPT harus berkoordinasi dengan Unit Datin.
(3) Dalam koordinasi sebagaimana dimaksud pada ayat (2), Unit Datin melakukan tindak lanjut evaluasi dan persetujuan bersama Pusdatin.
(4) Dalam pembangunan dan/atau pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (2), dibentuk kelompok kerja minimal:
    a. pemilik Proses Bisnis atau Unit kerja penanggung jawab tugas dan fungsi;
    b. pengembang aplikasi;
    c. pengendali mutu;
    d. pengguna aplikasi;
    e. Unit Datin; dan
    f. Pusdatin.
(5) Pembangunan dan/atau pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (2) menggunakan kerangka kerja pemrograman yang disetujui oleh Pusdatin.
(6) Implementasi di lingkungan produksi pada pembangunan dan/atau pengembangan Aplikasi Khusus sebagaimana dimaksud pada ayat (2) harus dilakukan oleh Unit Datin dan berkoordinasi dengan Pusdatin.

Pasal 25

(1) Aplikasi Khusus sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b harus dilengkapi minimal terdiri atas:
   a. kode sumber;
   b. basis data;
   c. dokumentasi; dan
   d. fasilitas berbagi pakai data secara elektronik.
(2) Dokumentasi sebagaimana dimaksud pada ayat (1) huruf c minimal terdiri atas:
   a. laporan hasil aktivitas setiap tahapan dalam siklus pembangunan aplikasi;
   b. petunjuk penggunaan administrator dan pengguna; dan
   c. materi alih pengetahuan dan materi pelatihan.

Pasal 26

(1) Kelengkapan Aplikasi Khusus sebagaimana dimaksud dalam Pasal 25 ayat (1) didaftarkan dan disimpan pada repositori Aplikasi SPBE yang diselenggarakan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi dan Pusdatin.
(2) Repositori Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dimanfaatkan secara aktif dalam kegiatan pengembangan dan/atau pemeliharaan Aplikasi SPBE.
(3) Pemanfaatan repositori Aplikasi SPBE sebagaimana dimaksud pada ayat (1) dikelola dan dikoordinasikan oleh Pusdatin sesuai dengan ketentuan peraturan perundang-undangan.
(4) Aplikasi Khusus beserta kelengkapannya yang dibangun dan/atau dikembangkan atas biaya Kementerian sebagaimana dimaksud dalam Pasal 24 ayat (1) menjadi milik Kementerian.
(5) Pemanfaatan Aplikasi Khusus sebagaimana dimaksud pada ayat (3) oleh instansi lain harus mendapatkan izin dari Pusdatin.

Pasal 27

(1) Pusdatin dan Unit Datin melakukan reviu dan evaluasi terhadap Aplikasi SPBE sebagaimana dimaksud dalam Pasal 22 ayat (2) minimal 1 (satu) tahun sekali.
(2) Hasil reviu dan evaluasi terhadap Aplikasi SPBE sebagaimana dimaksud pada ayat (1) dilaporkan kepada Sekretaris Jenderal Kementerian selaku ketua tim pengarah pada tim koordinasi SPBE Kementerian.

Pasal 28

(1) Keamanan SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf h ditujukan untuk melindungi aset Data dan Informasi dari pihak yang tidak bertanggung jawab.
(2) Keamanan SPBE sebagaimana dimaksud pada ayat (1) meliputi penjaminan:
   a. kerahasiaan;
   b. keutuhan;
   c. ketersediaan;
   d. keaslian;

e. kenirsangkalan,

pada sumber daya terkait Data dan Informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

(3) Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (1) huruf a ditujukan untuk memastikan sumber daya SPBE hanya dapat diakses oleh pihak yang berwenang.

(4) Penjaminan keutuhan sebagaimana dimaksud pada ayat (1) huruf b ditujukan untuk memastikan sumber daya SPBE tidak dapat diubah, dirusak, atau dimanipulasi tanpa izin.

(5) Penjaminan ketersediaan sebagaimana dimaksud pada ayat (1) huruf c ditujukan untuk memastikan sumber daya SPBE dapat diakses dan digunakan kapan pun dibutuhkan oleh pihak yang berwenang.

(6) Penjaminan keaslian sebagaimana dimaksud pada ayat (1) huruf d ditujukan untuk memastikan sumber daya SPBE adalah sah dan berasal dari sumber yang benar melalui penyediaan mekanisme verifikasi dan validasi.

(7) Penjaminan kenirsangkalan sebagaimana dimaksud pada ayat (1) huruf d ditujukan untuk memastikan tindakan atau transaksi yang telah dilakukan terhadap sumber daya SPBE tidak dapat disangkal oleh pihak yang melakukannya.

Pasal 29

(1) Setiap Unit Organisasi, Unit Kerja, dan/atau UPT harus memastikan Keamanan SPBE sebagaimana dimaksud dalam Pasal 28 melalui penerapan kendali keamanan.

(2) Penerapan kendali keamanan sebagaimana dimaksud pada ayat (1) paling sedikit melalui:
   a. pemanfaatan teknologi kriptografi;
   b. sertifikat elektronik;
   c. pembatasan akses berbasis peran;
   d. pencatatan dan monitoring aktivitas;
   e. penerapan sistem pencadangan, replikasi, rendudansi; dan/atau
   f. kendali keamanan lainnya.

(3) Penerapan kendali Keamanan SPBE sebagaimana dimaksud pada ayat (2) diselenggarakan dengan mengacu pada ketentuan peraturan perundang-undangan tentang standar teknis dan prosedur Keamanan SPBE dan dilaksanakan berdasarkan hasil manajemen risiko keamanan informasi yang menjadi bagian dari manajemen risiko SPBE.

(4) Penerapan Keamanan SPBE sebagaimana dimaksud pada ayat (3) di tingkat Unit Organisasi dikoordinasikan oleh Unit Datin.

(5) Penerapan Keamanan SPBE sebagaimana dimaksud pada ayat (3) di tingkat Kementerian dikoordinasikan oleh Pusdatin.

Pasal 30

(1) Layanan SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf i terdiri atas:
   a. layanan administrasi pemerintahan berbasis elektronik; dan
   b. layanan publik berbasis elektronik.

(2) Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud pada ayat (1) huruf a merupakan Layanan SPBE yang mendukung tata laksana internal birokrasi dalam rangka meningkatkan kinerja dan akuntabilitas pemerintah di Kementerian.

(3) Layanan administrasi pemerintahan berbasis elektronik sebagaimana dimaksud pada ayat (1) huruf a meliputi layanan yang mendukung kegiatan di bidang:
   a. perencanaan;
   b. penganggaran;
   c. keuangan;
   d. pengadaaan barang dan jasa;
   e. kepegawaian;
   f. kearsipan;
   g. pengelolaan barang milik negara;
   h. pengawasan;
   i. akuntabilitas kinerja; dan
   j. layanan lain sesuai dengan kebutuhan internal birokrasi pemerintahan.

(4) Layanan publik berbasis elektronik sebagaimana dimaksud pada ayat (1) huruf b merupakan Layanan SPBE yang mendukung pelaksanaan pelayanan publik di Kementerian.

(5) Layanan publik berbasis elektronik meliputi layanan yang mendukung kegiatan:
   a. pengaduan publik;
   b. dokumentasi dan informasi hukum;
   c. *whistle blowing system*; dan/atau
   d. layanan publik lainnya yang sesuai dengan kebutuhan Kementerian.

(6) Layanan administrasi pemerintahan sebagaimana dimaksud pada ayat (3) dan layanan publik berbasis elektronik sebagaimana dimaksud pada ayat (5) direncanakan, diselenggarakan, dan dikembangkan dengan mempertimbangkan kemampuan adaptasi terhadap kebutuhan pengguna atas pemanfaatan kecerdasan buatan dan perkembangan teknologi tingkat lanjut lain sesuai kebutuhan.

(7) Layanan administrasi pemerintahan sebagaimana dimaksud pada ayat (3) dan layanan publik berbasis elektronik sebagaimana dimaksud pada ayat (5) diselenggarakan dengan tetap menerapkan:
   a. standar teknis dan prosedur penerapan teknologi terkait;
   b. standar teknis dan prosedur Keamanan SPBE; dan
   c. norma dan etika,

   sesuai dengan ketentuan peraturan perundang-undangan.

(8) Ketentuan mengenai pemanfaatan kecerdasan buatan dan perkembangan teknologi tingkat lanjut lain sebagaimana dimaksud pada ayat (6) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 31

(1) Layanan SPBE sebagaimana dimaksud dalam Pasal 30 ayat (1) diselenggarakan oleh Unit Organisasi, Unit Kerja, dan/atau UPT secara terpadu dan terintegrasi sesuai dengan tugas dan fungsinya.
(2) Integrasi Layanan SPBE sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Pusdatin menjadi Layanan SPBE Kementerian.
(3) Integrasi Layanan SPBE sebagaimana dimaksud pada ayat (2) dilakukan berdasarkan Arsitektur SPBE.

BAB III
MANAJEMEN SPBE

Pasal 32

(1) Manajemen SPBE meliputi:
    a. manajemen risiko SPBE;
    b. manajemen keamanan informasi;
    c. manajemen data;
    d. manajemen aset teknologi informasi dan komunikasi;
    e. manajemen sumber daya manusia;
    f. manajemen pengetahuan;
    g. manajemen perubahan; dan
    h. manajemen layanan SPBE.
(2) Pelaksanaan Manajemen SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 33

(1) Manajemen risiko SPBE sebagaimana dimaksud pada Pasal 32 ayat (1) huruf a bertujuan untuk menjamin keberlangsungan pelaksanaan SPBE dengan meminimalkan dampak risiko dalam mencapai tujuan SPBE.
(2) Manajemen risiko SPBE dilakukan melalui proses identifikasi, analisis, pengendalian, pemantauan, dan evaluasi SPBE terhadap risiko dalam pelaksanaan SPBE di Kementerian.
(3) Manajemen risiko SPBE dilaksanakan oleh setiap unit pemilik risiko dan dikoordinasikan unit kepatuhan internal unit organisasi.
(4) Manajemen risiko SPBE dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 34

(1) Manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf b bertujuan menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.

(2) Manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan SPBE.
(3) Manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan oleh:
a. Unit Organisasi;
b. Unit Kerja;
c. UPT; dan
d. pihak eksternal.
(4) Pihak eksternal sebagaimana dimaksud pada ayat (3) huruf d merupakan mitra kerja dan penyedia barang/jasa di Kementerian.
(5) Pelaksanaan manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Pusdatin.
(6) Manajemen keamanan informasi SPBE dan ketentuan sanksi terhadap pelanggaraan keamanan informasi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 35

(1) Manajemen data sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf c bertujuan untuk menjamin terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional.
(2) Manajemen data sebagaimana dimaksud pada ayat (1) dilakukan melalui proses pengelolaan arsitektur data, data induk, data referensi, basis data, kualitas data, dan interoperabilitas data.
(3) Manajemen data mencakup jenis data dan informasi statistik, data dan informasi geospasial, data dan informasi kebencanaan, data dan informasi digital infrastruktur, serta data dan informasi lainnya yang dikelola oleh Kementerian.
(4) Data dan informasi statistik sebagaimana dimaksud pada ayat (3) merupakan data berupa angka tentang karakteristik atau ciri khusus suatu populasi yang diperoleh dengan cara pengumpulan, pengolahan, penyajian, dan analisis.
(5) Data dan informasi geospasial sebagaimana dimaksud pada ayat (3) merupakan data tentang lokasi geografis, dimensi atau ukuran, dan/atau karakteristik objek alam dan/atau buatan manusia yang berada di bawah, pada, atau di atas permukaan bumi.
(6) Data dan informasi kebencanaan sebagaimana dimaksud pada ayat (3) merupakan kumpulan fakta, karakter, angka, spasial, audio dan visual, dan data lain yang berkaitan dengan kejadian bencana, potensi bencana, serta dampaknya terhadap manusia, lingkungan dan infrastruktur dalam fase prabencana, tanggap darurat, dan pascabencana.

(7) Data dan informasi digital infrastruktur sebagaimana dimaksud pada ayat (3) merupakan data berupa model tiga dimensi beserta atribut geometris dan non-geometris, serta data dan dokumen lain tentang perencanaan, perancangan, konstruksi, pengawasan, dan pengelolaan aset infrastruktur dan bangunan yang diperoleh dan dikelola berdasarkan prinsip *building information modelling*.

(8) Data dan informasi lainnya sebagaimana dimaksud pada ayat (3) merupakan data dan informasi selain data statistik, data geospasial, data dan informasi kebencanaan, dan data dan informasi digital infrastruktur.

Pasal 36

(1) Manajemen Data sebagaimana dimaksud pada Pasal 35 ayat (1) berlaku untuk Unit Organisasi, Unit Kerja, balai/UPT serta pihak yang terkait dengan pengelolaan data di Kementerian.

(2) Penyelenggaraan Manajemen Data Kementerian sebagaimana dimaksud pada ayat (1) melibatkan:
   a. Forum Satu Data Kementerian;
   b. tim pengarah pada tim koordinasi SPBE;
   c. walidata Kementerian;
   d. koordinator produsen data;
   e. produsen Data; dan
   f. pengguna Data.

(3) Forum Satu Data Kementerian sebagaimana dimaksud pada ayat (2) huruf a mempunyai tugas:
   a. menyepakati standar data, metadata, interoperabilitas data, kode referensi dan/atau data induk yang digunakan di Kementerian;
   b. memberikan usulan standar data, metadata, interoperabilitas data, kode referensi, dan/atau data induk di lingkungan Kementerian untuk ditetapkan oleh Menteri sesuai dengan ketentuan peraturan perundang-undangan;
   c. memberikan rekomendasi dalam proses perencanaan pengumpulan data;
   d. menyepakati jadwal pemutakhiran data.

(4) Tim Pengarah pada tim koordinasi SPBE sebagaimana dimaksud pada ayat (2) huruf b menetapkan Kode Referensi dan/atau Data Induk dalam hal Forum Satu Data Kementerian tidak mencapai kesepakatan terhadap Kode Referensi dan/atau Data Induk.

(5) Walidata Kementerian sebagaimana dimaksud pada ayat (2) huruf c mempunyai tugas:
   a. memberikan usulan standar data, metadata, interoperabilitas data, kode referensi dan/atau data induk ke Forum Satu Data Kementerian yang berlaku di Kementerian;
   b. melakukan bagi pakai Data dan Informasi antar Unit Kerja di Kementerian, Instansi Pusat, dan/atau Pemerintah Daerah;

c. memberikan rekomendasi dalam proses perencanaan pengumpulan data;
d. melakukan pemeriksaan ulang terhadap data prioritas;
e. melakukan pembinaan penyelenggaraan satu data Kementerian termasuk melakukan pembinaan Produsen Data sesuai dengan ketentuan peraturan perundang-undangan;
f. melakukan konsultasi kepada Tim Pengarah tim koordinasi SPBE untuk mendapat arahan terkait dengan kualitas data Kementerian menuju Satu Data Indonesia;
g. mengonsolidasikan hasil pembahasan Forum Satu Data Kementerian; dan
h. menyebarluaskan kode referensi dan/atau Data Induk Kementerian dalam Portal Satu Data Indonesia.

(6) Koordinator Produsen Data sebagaimana dimaksud pada ayat (5) huruf d mempunyai tugas:
a. mengoordinasikan perencanaan dan pengumpulan data bersama Produsen Data dan Walidata Kementerian;
b. mengumpulkan, memeriksa, dan mengelola kesesuaian data yang disampaikan oleh Produsen Data sesuai dengan prinsip Satu Data Indonesia;
c. mengusulkan daftar data sebagai Data Prioritas;
d. memastikan keamanan data dan informasi;
e. memberikan masukan kepada Forum Satu Data Kementerian mengenai Standar Data, Metadata, dan Interoperabilitas Data sesuai dengan bidang tugasnya;
f. membantu Walidata Kementerian dalam pembinaan penyelenggaraan satu data Kementerian di Unit Organisasinya;
g. melakukan pemantauan Satu Data Bidang Pekerjaan Umum di Unit Organisasinya;
h. melakukan evaluasi penyelenggaraan Satu Data Bidang Pekerjaan Umum di Unit Organisasinya.
i. mengumpulkan, memeriksa kesesuaian data, dan mengelola data yang disampaikan oleh Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya sesuai dengan prinsip Satu Data Indonesia;
j. menyebarluaskan data, metadata, kode referensi, dan data induk ke dalam media bagi pakai data di Pusat Data Kementerian;
k. membantu Walidata Kementerian dalam membina Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya;
l. Menetapkan pembatasan akses data bersama Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya sesuai dengan tingkat klasifikasi keamanan data; dan
m. menyebarluaskan kode referensi dan/atau Data Induk dalam media bagi-pakai data di tingkat

kementerian yang dapat diakses melalui pemanfaatan teknologi informasi dan komunikasi dalam Pusat Data Nasional dan/atau Platform dengan mengacu pada klasifikasi informasi yang telah ditetapkan pada Manajemen Keamanan Informasi.

(7) Produsen Data sebagaimana dimaksud pada ayat (2) huruf e mempunyai tugas:
   a. menghasilkan data yang berkualitas, yaitu data yang akurat, mutakhir, terpadu, dapat dipertanggungjawabkan, serta mudah diakses dan dibagipakaikan melalui pemenuhan standar data, metadata, kaidah interoperabilitas data, dan menggunakan kode referensi dan/atau data induk yang telah ditetapkan;
   b. melakukan verifikasi dan validasi data bersama Unit Kerja di masing-masing Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi;
   c. memberi masukan kepada Unit Kerja di masing-masing Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi terkait dengan standar data, format baku metadata, kaidah interoperabilitas data, penggunaan kode referensi dan/atau data induk, proses perencanaan pengumpulan data, dan data prioritas;
   d. memutakhirkan data sesuai dengan jadwalnya;
   e. menyampaikan data, metadata, dan pembatasan aksesnya kepada Unit Kerja di masing-masing Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi;
   f. menetapkan pembatasan akses data bersama Unit Kerja di masing-masing Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi sesuai dengan tingkat klasifikasi keamanan data; dan
   g. menjaga keamanan Data dan Informasi.

(8) Pengguna Data sebagaimana dimaksud pada ayat (2) huruf f merupakan instansi pusat, instansi daerah, perseorangan, kelompok orang, atau badan hukum yang menggunakan data dari Kementerian.

Pasal 37

(1) Penyelenggaraan Manajemen Data mencakup siklus pengelolaan data sebagai berikut:
   a. perencanaan Data;
   b. pengumpulan Data;
   c. pemeriksaaan Data; dan
   d. penyebarluasan Data.

(2) Perencanaan Data sebagaimana dimaksud pada ayat (1) huruf a diselenggarakan dengan ketentuan:
   a. Forum Satu Data Kementerian menentukan daftar data yang dikumpulkan, daftar data prioritas, Produsen Data, dan jadwal rilis atau update yang harus disusun kode referensi dan/atau data induknya;

b. Walidata bersama Koordinator Produsen Data dan Produsen Data menyusun standar data, metadata, kode referensi dan/atau data induk berdasarkan arsitektur data dan informasi Kementerian, rekomendasi Walidata Kementerian, dan rekomendasi Forum Satu Data Kementerian;
c. Forum Satu Data Kementerian menyepakati kode referensi dan/atau data induk, serta Walidata atas kode referensi dan/atau data induk tersebut;
d. Walidata Kementerian dapat mengusulkan standar data, metadata, kode referensi dan/atau data induk yang yang telah disepakati oleh Forum Satu Data Kementerian untuk ditetapkan oleh Menteri; dan
e. Walidata Kementerian mengkomunikasikan penetapan ayat (10) huruf d kepada pihak-pihak terkait dalam pengelolaan data, Unit Organisasi, Unit Kerja, dan UPT.

(3) Pengumpulan Data sebagaimana dimaksud pada ayat (1) huruf b diselenggarakan dengan ketentuan:
a. Walidata Kementerian menyiapkan layanan media bagi-pakai data di Pusat Data Nasional dan/atau Platform yang sesuai dengan peraturan perundangan yang berlaku;
b. koordinator Produsen Data Mengumpulkan, memeriksa kesesuaian data, dan mengelola data yang disampaikan oleh Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya sesuai dengan prinsip Satu Data Indonesia;
c. menyebarluaskan data, metadata, kode referensi, dan data induk ke dalam media bagi-pakai data di Pusat Data Kementerian;
d. membantu Walidata Kementerian dalam membina Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya;
e. menetapkan pembatasan akses data bersama Unit Kerja dan UPT yang menghasilkan data sesuai dengan tugas dan fungsinya sesuai dengan tingkat klasifikasi keamanan data;
f. Produsen Data menghasilkan dan menyiapkan data untuk dikumpulkan, sesuai dengan:
    1. standar data;
    2. metadata;
    3. daftar data yang telah ditentukan dalam Forum Satu Data Kementerian; dan
    4. jadwal pemutakhiran data atau rilis data;
g. koordinator Produsen Data memeriksa kesiapan Infrastruktur SPBE untuk melakukan pengiriman data ke Walidata Kementerian sesuai dengan periode waktu yang telah ditetapkan oleh Walidata Kementerian atau apabila diperlukan, dilakukan pengiriman ulang:
    1. jika Infrastruktur SPBE siap, Koordinator Produsen Data melakukan pengiriman data melalui Infrastruktur SPBE pertukaran data ke dalam media bagi-pakai data di Pusat Data

Nasional dan/atau Platform dan memberikan notifikasi daftar data, periode, pembatasan aksesnya, dan jumlah data yang dikirim kepada Walidata Kementerian sebagai pembanding;

2. jika infrastruktur SPBE belum siap atau terjadi gangguan, pelaksanaan pengiriman data dari Koordinator Produsen Data dilakukan secara luring melalui media penyimpanan data berupa CD/DVD/External Hard Disk/Flashdisk sesuai dengan klasifikasi data mengacu pada Manajemen Keamanan Informasi.

(4) Pemeriksaan Data sebagaimana dimaksud pada ayat (1) huruf c diselenggarakan dengan ketentuan:

a. Walidata Kementerian bersama Koordinator Produsen Data memeriksa data yang dihasilkan oleh Produsen Data sesuai dengan Prinsip Satu Data Indonesia, yaitu pemenuhan standar data, metadata, kaidah interoperabilitas data, dan penggunaan kode referensi dan/atau data induk yang telah ditetapkan.
b. koordinator Produsen Data mencatat status kesesuaian dan status data, serta menyampaikan kepada Produsen Data.
c. dalam hal data yang disampaikan oleh Produsen Data belum sesuai dengan Prinsip Satu Data Indonesia, Koordinator Produsen Data mengembalikan data tersebut kepada Produsen Data.
d. Walidata Kementerian memeriksa ulang data prioritas oleh Produsen Data dan menyetujui hasil pemeriksaan data prioritas yang sudah sesuai dengan Prinsip Satu Data Indonesia.
e. dalam hal hasil pemeriksaan data prioritas belum sesuai dengan Prinsip Satu Data Indonesia, Walidata Kementerian mengembalikan data tersebut kepada Koordinator Produsen Data untuk disesuaikan dan selanjutnya disetujui untuk disebarluaskan.

(5) Penyebarluasan Data sebagaimana dimaksud pada ayat (1) huruf d diselenggarakan dengan ketentuan:

a. penyebarluasan data merupakan kegiatan pemberian akses, pendistribusian, dan pertukaran data.
b. setelah penetapan persetujuan hasil pemeriksaan, Walidata Kementerian menyebarluaskan data melalui media bagi-pakai data di Pusat Data Nasional dan/atau Platform untuk kebutuhan distribusi dan pertukaran data dengan mengacu pada klasifikasi informasi yang telah ditetapkan pada Manajemen Keamanan Informasi.
c. Walidata Kementerian mengatur penyediaan akses data pada media bagi-pakai data untuk:
    1. Kode Referensi;
    2. Data induk;
    3. Data;
    4. metadata;
    5. Data prioritas, jadwal rilis, dan/atau pemutakhiran Data; dan
    6. interoperabilitas data;

d. media bagi-pakai data di Pusat Data Nasional dan/atau Platform dapat diakses sesuai dengan pembatasan akses yang telah ditetapkan;
e. pengguna Data dapat mengajukan hak akses secara tertulis melalui sarana resmi kepada Walidata Kementerian;
f. Walidata Kementerian menyampaikan izin akses/penolakan izin akses melalui sarana resmi dengan tembusan kepada Forum Satu Data Indonesia; dan
g. Walidata Kementerian menyebarluaskan kode referensi dan/atau data induk Kementerian ke dalam Portal Satu Data Indonesia dengan pembatasan akses untuk kebutuhan distribusi dan pertukaran data.

(6) Manajemen data dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 38

(1) Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf d bertujuan untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE.
(2) Pelaksanaan manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) terdiri atas proses perencanaan, pengadaan, pengelolaan, dan penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.
(3) Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh seluruh pemilik aset teknologi informasi dan komunikasi di Kementerian.
(4) Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh unit kerja di sekretariat jenderal mempunyai tugas melaksanakan pembinaan, pengawasan, dan koordinasi penyelenggaraan pengelolaan barang milik negara dan/atau kekayaan negara Kementerian.
(5) Manajemen aset teknologi informasi dan komunikasi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 39

(1) Manajemen sumber daya manusia sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf e bertujuan untuk untuk menjamin keberlangsungan dan peningkatan mutu dan Layanan SPBE termasuk di dalamnya kegiatan peningkatan kompetensi sumber daya manusia SPBE dan promosi literasi SPBE.
(2) Pelaksanaan manajemen sumber daya manusia sebagaimana dimaksud pada ayat (1) terdiri atas proses perencanaan, pengembangan, pembinaan, dan pendayagunaan sumber daya manusia SPBE.

(3) Manajemen sumber daya manusia sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Unit Organisasi, Unit Kerja, dan UPT yang memiliki sumber daya manusia SPBE.
(4) Manajemen sumber daya manusia sebagaimana dimaksud pada ayat (2) pada proses perencanaan dikoordinasikan oleh unit kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian, pada proses pengembangan dikoordinasikan oleh unit organisasi yang mempunyai tugas menyelenggarakan pengembangan sumber daya manusia bidang pekerjaan umum Kementerian, dan pada proses pembinaan serta pendayagunaan sumber daya manusia sebagaimana dimaksud pada ayat (3) SPBE dikoordinasikan oleh Pusdatin bersama dengan Unit Organisasi.
(5) Manajemen sumber daya manusia dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 40

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf f bertujuan untuk meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE.
(2) Pelaksanaan manajemen pengetahuan sebagaimana dimaksud pada ayat (1) terdiri atas proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.
(3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Unit Organisasi, Unit Kerja, dan UPT.
(4) Pelaksanaan manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh unit organisasi yang mempunyai tugas menyelenggarakan pengembangan sumber daya manusia bidang pekerjaan umum.
(5) Pelaksanaan manajemen pengetahuan sebagaimana dimaksud pada ayat (1) diterapkan menggunakan aplikasi manajemen pengetahuan.
(6) Manajemen pengetahuan dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 41

(1) Manajemen perubahan sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf g bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE.
(2) Pelaksanaan manajemen perubahan sebagaimana dimaksud pada ayat (1) terdiri atas proses perencanaan, analisis, pengembangan, implementasi, pemantauan, dan evaluasi terhadap perubahan SPBE.
(3) Manajemen perubahan sebagaimana dimaksud pada ayat (1) dilaksanakan dan dikoordinasikan oleh tim koordinasi SPBE.

(4) Manajemen perubahan dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 42

(1) Manajemen Layanan SPBE sebagaimana dimaksud dalam Pasal 32 ayat (1) huruf h bertujuan untuk memberikan dukungan terhadap Layanan SPBE sehingga dapat berjalan secara berkesinambungan, berkualitas, responsif, dan adaptif dalam rangka menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE kepada Pengguna SPBE.
(2) Pelaksanaan Manajemen Layanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas proses pelayanan kepada pengguna SPBE, pengoperasian Layanan SPBE, dan pengelolaan Aplikasi SPBE.
(3) Manajemen Layanan SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Unit Organisasi, Unit Kerja, dan/atau UPT sebagaimana dimaksud dalam Pasal 31 ayat (1) sesuai dengan tugas dan fungsinya.
(4) Manajemen Layanan SPBE sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh tim koordinasi SPBE.
(5) Manajemen Layanan SPBE dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 43

Ketentuan mengenai Manajemen SPBE sebagaimana dimaksud dalam Pasal 32 ayat (1) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB IV
AUDIT TIK

Pasal 44

(1) Audit TIK dilaksanakan untuk memastikan keandalan dan keamanan sistem teknologi informasi dan komunikasi.
(2) Audit TIK sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. audit Infrastruktur SPBE;
    b. audit Aplikasi SPBE; dan
    c. audit Keamanan SPBE.
(3) Audit TIK sebagaimana dimaksud pada ayat (2) dilakukan secara:
    a. internal; dan
    b. eksternal.

Pasal 45

(1) Audit TIK internal sebagaimana dimaksud dalam Pasal 44 ayat (3) huruf a dilaksanakan oleh unit organisasi yang mempunyai tugas menyelenggarakan pengawasan intern Kementerian.
(2) Pelaksanaan Audit TIK internal sebagaimana dimaksud pada ayat (1) harus berkoordinasi dengan Sekretaris Jenderal Kementerian selaku ketua tim pengarah pada tim koordinasi SPBE.

Pasal 46

(1) Audit TIK eksternal sebagaimana dimaksud dalam Pasal 44 ayat (3) huruf b dilaksanakan oleh:
    a. lembaga pelaksana Audit TIK pemerintah; atau
    b. lembaga pelaksana Audit TIK yang terakreditasi,
    sesuai dengan ketentuan peraturan perundang-undangan.
(2) Pelaksanaan Audit TIK eksternal sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Sekretaris Jenderal Kementerian selaku ketua tim pengarah pada tim koordinasi SPBE.
(3) Audit TIK eksternal dilakukan setelah Audit TIK internal dilaksanakan.

Pasal 47

(1) Audit TIK dilaksanakan minimal 1 (satu) kali dalam 2 (dua) tahun.
(2) Pelaksanaan Audit TIK sebagaimana dimaksud pada ayat (1) sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
TIM KOORDINASI SPBE

Pasal 48

(1) Dalam mewujudkan penguatan kapasitas pengelolaan dan sistem koordinasi pelaksanaan pembangunan SPBE, perlu dibentuk tim koordinasi SPBE.
(2) Tim koordinasi SPBE Kementerian merupakan para pejabat dalam tim yang diberi tugas untuk mengendalikan, mengarahkan, dan mengevaluasi SPBE, termasuk didalamnya melaksanakan perumusan kebijakan dan penerapan SPBE di Kementerian serta melakukan koordinasi kerjasama untuk mendukung penerapan SPBE antarinstansi pusat dan/atau pemerintah daerah.
(3) Tim koordinasi SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. tim pengarah yang dipimpin oleh seorang ketua;
    b. tim pelaksana yang dipimpin oleh seorang ketua; dan
    c. sekretariat.
(4) Kapasitas kepemimpinan, pengetahuan, dan praktik terbaik tim koordinasi SPBE perlu diperkuat atau ditingkatkan melalui sosialisasi, diskusi, pelatihan, dan studi banding.
(5) Keanggotaan, tugas, dan fungsi tim koordinasi SPBE Kementerian sebagaimana dimaksud pada ayat (1) ditetapkan oleh Menteri.

## BAB VI
## PEMANTAUAN DAN EVALUASI SPBE

### Pasal 49

(1) Pemantauan dan evaluasi SPBE bertujuan untuk mengukur kematangan dan meningkatkan kualitas SPBE di Kementerian.
(2) Pemantauan dan evaluasi SPBE mencakup kebijakan internal SPBE, Tata Kelola SPBE, Manajemen SPBE, dan Layanan SPBE.
(3) Pelaksanaan pemantauan dan evaluasi SPBE sebagaimana dimaksud pada ayat (2) dilaksanakan oleh tim asesor internal.
(4) Tim asesor internal sebagaimana dimaksud pada ayat (3) ditetapkan oleh Menteri.
(5) Pelaksanaan pemantauan dan evaluasi SPBE sesuai dengan ketentuan peraturan perundang-undangan.

## BAB VII
## KETENTUAN PENUTUP

### Pasal 50

Pada saat Peraturan Menteri ini mulai berlaku, ketentuan yang mengatur SPBE Kementerian sebagaimana diatur dalam Peraturan Menteri Pekerjaan Umum dan Perumahan Rakyat Nomor 9 Tahun 2023 tentang Penerapan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2023 Nomor 871), dicabut dan dinyatakan tidak berlaku.

### Pasal 51

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 24 Februari 2026

MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA,

PU Ditandatangani Secara Elektronik

DODY HANGGODO

Diundangkan di Jakarta
pada tanggal 10 Maret 2026

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2026 NOMOR 165

LAMPIRAN I
PERATURAN MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2026
TENTANG
PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

PEMANFAATAN KECERDASAN BUATAN DAN PERKEMBANGAN TEKNOLOGI TINGKAT LANJUT LAIN

A. DAFTAR ISTILAH

Istilah yang dipergunakan pada lampiran Peraturan Menteri ini adalah sebagai berikut:

1. *Actuator* adalah perangkat yang memberikan respon sesuai desain penerapannya (misalnya memberikan peringatan, menyambungkan atau memutuskan arus listrik).
2. *Alert* adalah peringatan untuk deteksi masalah, misalnya peringatan dihasilkan oleh perangkat IoT.
3. *Anomaly Detection* adalah teknik analisis (seringkali menggunakan *Machine Learning*) untuk mengidentifikasi pola, perilaku, atau *event* yang tidak biasa atau menyimpang dari perilaku atau pola normal (yang disebut *baseline*). Dalam keamanan, ini digunakan untuk mendeteksi *event* yang mencurigakan yang mungkin mengindikasikan serangan siber.
4. *API Abuse* adalah penyalahgunaan *Application Programming Interface* (API), yaitu antarmuka yang memungkinkan dua aplikasi saling berkomunikasi. Penyerang bisa mengeksploitasi API yang tidak aman untuk mengakses, memanipulasi data, atau membebani sistem.
5. *Application Layer* adalah lapisan yang bertanggung jawab dalam pemrosesan dan menampilkan data kepada pengguna, termasuk aplikasi seperti *smart home* atau *smart city*.
6. *Big Data Analgtics* adalah teknologi analisis terhadap data yang berukuran sangat besar, tidak terstruktur, dan tidak diketahui pola, korelasi ataupun relasi antar data.
7. *Business Layer* adalah lapisan yang berperan untuk mengintegrasikan aplikasi IoT dengan kebutuhan strategi organisasi, serta mengelola aplikasi, pengguna, dan data untuk mencapai tujuan organisasi.
8. *Business Logic Attacks* adalah serangan yang mengeksploitasi kelemahan dalam alur kerja atau aturan aplikasi (logika bisnis), bukan kelemahan teknis.
9. *Cloud computing* adalah teknologi layanan berbagi pakai yang dapat diakses melalui internet untuk memberikan layanan data, aplikasi, dan infrastruktur kepada pengguna.
10. CoAP (*Constrained Application Protocol*) adalah Protokol transfer dokumen yang sangat ringan, mirip dengan HTTP (protokol dasar web), tetapi dioptimalkan untuk perangkat *constrained* (perangkat yang terbatas)

seperti sensor kecil. CoAP bekerja di atas UDP (*User Datagram Protocol*), menjadikannya lebih efisien dan cepat, cocok untuk jaringan *low-power*.

11. *Compliance Framework* adalah sekumpulan kebijakan, prosedur, dan kontrol terstruktur yang dirancang untuk membantu organisasi memenuhi persyaratan hukum, regulasi, dan standar industri tertentu.
12. *Data Anonymization* adalah proses menghapus atau memodifikasi informasi identitas pribadi (seperti nama, alamat, atau nomor KTP) dari kumpulan data sehingga data tersebut tidak dapat lagi dikaitkan secara langsung dengan individu mana pun, demi menjaga privasi.
13. *Data Corruption* adalah kondisi di mana data rusak, tidak akurat, atau diubah secara tidak sengaja (karena kegagalan sistem atau transmisi) atau sengaja (karena serangan siber), sehingga data tersebut menjadi tidak valid atau tidak dapat digunakan.
14. *Data Leakage* adalah bocornya data sensitif ke lingkungan yang tidak sah (misalnya ke internet publik atau pihak ketiga yang tidak berhak), baik karena kegagalan keamanan sistem maupun disengaja.
15. DDoS (*Distributed Denial of Service*) adalah potensi risiko pada *Network Layer* yang berupa serangan siber yang bertujuan membuat layanan jaringan atau server tidak dapat diakses oleh pengguna sah karena kelebihan beban trafik (lalu lintas data) yang dikirim dari banyak sumber secara terdistribusi.
16. *Digital Signature* adalah teknik matematis yang digunakan untuk memverifikasi keaslian dan integritas suatu dokumen digital atau pesan. Ini memastikan bahwa data benar-benar berasal dari pengirim yang diklaim dan belum dimodifikasi.
17. *Eavesdropping* adalah tindakan mendengarkan atau mencegat secara rahasia transmisi data di jaringan tanpa izin. Mirip dengan *tapping* telepon, ini bertujuan mencuri informasi sensitif saat data sedang bergerak (*in transit*).
18. *Edge Computing* adalah Konsep pemrosesan atau analisis data yang dilakukan sedekat mungkin dengan sumber data (sensor atau gateway) yang bertujuan untuk mengurangi latensi dan beban jaringan.
19. *Edge Device Exploitation* adalah pemanfaatan celah keamanan (*vulnerability*) yang ada pada perangkat yang berada di tepi jaringan (*edge devices*), seperti *gateway* atau perangkat komputasi tepi, untuk mendapatkan akses ke jaringan yang lebih luas.
20. *Fault Management* adalah bagian dari manajemen sistem jaringan yang berperan dalam deteksi kegagalan dan pemulihan gangguan pada jaringan, misalnya melalui penerapan *auto-failover* ke *gateway* cadangan.
21. *Firmware* adalah jenis perangkat lunak permanen yang tertanam langsung pada perangkat keras (chip) perangkat. Fungsinya adalah untuk memberikan instruksi dasar tingkat rendah tentang bagaimana perangkat harus beroperasi dan mengelola dirinya sendiri.
22. *Firmware Update* (OTA) adalah proses pembaruan *firmware* setiap perangkat IoT yang dikelola secara aman, dan dapat dilakukan secara *Over-The-Air* (OTA) atau nirkabel.

23. *General Data Protection Regulation* (GDPR) adalah peraturan Uni Eropa yang mengatur perlindungan data dan privasi individu, memberikan kendali kepada penduduk Uni Eropa atas data pribadi.
24. *Health Monitoring* adalah proses pemantauan terus-menerus terhadap kondisi fisik, kinerja (*performance*), dan keamanan perangkat IoT untuk memastikan ketersediaan (*availability*) dan kepatuhan keamanan.
25. HTTPS (*HyperText Transfer Protocol Secure*) adalah versi aman dari HTTP, protokol standar yang digunakan *browser* untuk mengakses situs web. HTTPS mengenkripsi komunikasi antara perangkat (atau *client*) dan *server* menggunakan SSL/TLS. Dalam IoT, ini digunakan untuk komunikasi data yang membutuhkan tingkat keamanan tinggi dan pertukaran data yang lebih besar (misalnya, *firmware update* atau komunikasi *gateway* ke *cloud*).
26. *Incident Response Plan* dalah dokumen terperinci dan terstruktur yang berisi langkah-langkah yang harus diikuti oleh tim IT dan keamanan sebuah organisasi ketika terjadi insiden keamanan siber (seperti serangan *malware* atau pelanggaran data). Rencana ini mencakup tahapan mulai dari persiapan, deteksi, penahanan, pemulihan, hingga pembelajaran (*lessons learned*).
27. *Input Validation* adalah proses pemeriksaan (validasi) dan pembersihan semua data yang dimasukkan oleh pengguna atau dari sumber eksternal sebelum data tersebut diproses oleh aplikasi. Tujuannya adalah untuk mencegah *bug* atau serangan yang memanfaatkan input yang tidak terduga atau berbahaya (misalnya *SQL Injection*).
28. *Insecure Authentication* adalah mekanisme atau proses verifikasi identitas (seperti *username* dan *password*) yang lemah, mudah dibobol, atau gagal melindungi kredensial, sehingga memungkinkan penyerang meniru identitas pengguna atau perangkat yang sah.
29. Integrasi *Handshake* (API) adalah metode integrasi di mana pabrikan mengembangkan *Application Programming Interface* (API) agar dua atau beberapa sistem yang berbeda dapat saling terhubung.
30. *Integrity Checks* adalah proses yang dilakukan untuk memastikan data atau *file* belum diubah secara tidak sah selama transmisi atau penyimpanan.
31. *Internet of Things* (IoT) adalah perangkat elektronik yang dilengkapi dengan perangkat lunak, sensor, aktuator, dan konektivitas internet sehingga mampu melakukan pengiriman atau pertukaran data melalui akses internet.
32. Interoperabilitas adalah Kemampuan perangkat IoT untuk dapat bekerja dengan berbagai *platform* dan protokol (misalnya MQTT, CoAP, HTTPS, LoRaWAN, dll.).
33. *Jitter* adalah variasi *latency* antar paket dalam konteks *Quality of Service* (QoS).
34. Kecerdasan Buatan (*Artificial Intelligence*-AI) adalah teknologi kecerdasan buatan pada mesin yang memiliki fungsi kognitif untuk melakukan pembelajaran dan pemecahan masalah sebagaimana halnya dilakukan oleh manusia.

35. Kecerdasan Buatan Agentik atau AI Agentik adalah kecerdasan buatan yang bisa bertindak sendiri untuk mencapai tujuan, seperti asisten digital yang mandiri atau *autonomous driving*. kecerdasan buatan Agentik menerima tugas, merencanakan langkah-langkah, dan melaksanakannya tanpa perlu diarahkan secara terus-menerus.
36. Kecerdasan Buatan Generatif atau AI Generatif adalah adalah kecerdasan buatan yang menciptakan sesuatu yang baru, seperti teks, gambar, musik, atau kode.
37. Kecerdasan Buatan Prediktif atau AI Prediktif adalah kecerdasan buatan yang memprediksi apa yang akan terjadi berdasarkan data masa lalu, belajar dari pola-pola sebelumnya, dan memperkirakan kemungkinan kejadian di masa depan.
38. *Key Performance Indicators* (KPIs) adalah metrik kinerja utama yang menampilkan metrik kinerja utama (misalnya tingkat konsumsi energi pada IoT).
39. *Latency* adalah waktu pengiriman data *end-to-end* dalam konteks *Quality of Service* (QoS) , atau waktu respons perangkat.
40. LoRaWAN (*Long Range Wide Area Network)* adalah sebuah spesifikasi protokol jaringan dan sistem arsitektur yang dirancang untuk komunikasi nirkabel jarak jauh (*long-range*) dengan konsumsi daya yang sangat rendah (*low-power*). Teknologi ini memungkinkan perangkat bertenaga baterai mengirim data dalam jarak hingga kilometer, menjadikannya pilihan utama untuk aplikasi Smart City dan sensor pertanian yang tersebar luas.
41. *Low-power mode* adalah mode penggunaan daya yang dioptimasi untuk perangkat yang dioperasikan dengan baterai (*battery-operated*).
42. *Machine Learning* (ML) atau mesin pembelajaran adalah teknologi digunakan untuk prediksi, deteksi anomali, dan pengambilan keputusan otomatis dalam konteks Analitik Data dan kecerdasan buatan.
43. *Malware* atau *Malicious Software* adalah rogram atau kode jahat yang dirancang untuk menyusup, merusak, atau mendapatkan akses tidak sah ke sistem komputer, *server*, atau jaringan (termasuk *virus*, *ransomware*, *spyware*).
44. *Man-in-the-Middle* (MitM) adalah serangan di mana penyerang diam-diam mencegat dan berpotensi mengubah komunikasi antara dua pihak yang sedang berkomunikasi (misalnya antara sensor dan *server*) tanpa diketahui oleh kedua pihak tersebut.
45. *Middleware* adalah perangkat integrasi yang berfungsi sebagai jembatan antara perangkat IoT dan aplikasi yang berbeda, memungkinkan komunikasi antara *platform* perangkat keras dan perangkat lunak yang beragam.
46. *Mobile internet* adalah akses internet yang menggunakan gawai personal.
47. MQTT (*Message Queuing Telemetry Transport*) adalah protokol *messaging* yang sangat ringan, dirancang khusus untuk perangkat dengan keterbatasan sumber daya (*low bandwidth*) dan daya. Ini menggunakan pola pub/sub (publisher/subscriber), di mana sensor (*publisher*) mengirim data ke *broker* sentral, dan aplikasi (*subscriber*) mengambil data dari *broker* tersebut. Sangat ideal untuk komunikasi IoT.

48. *Network Layer* atau *transport layer* atau *communication layer*, yang bertanggung jawab dalam transmisi data dari dan ke *application layer*.
49. *Network Segmentation* adalah praktik membagi jaringan komputer menjadi segmen-segmen atau sub-jaringan yang lebih kecil dan terisolasi. Tujuannya adalah untuk membatasi pergerakan potensi ancaman (seperti *malware*) dan mencegahnya menyebar ke seluruh jaringan jika satu segmen terkompromi.
50. *NIST CSF* adalah kerangka kerja sukarela yang dikembangkan oleh *National Institute of Standards and Technology* AS untuk membantu organisasi dari semua ukuran dalam mengelola dan mengurangi risiko keamanan siber.
51. *Packet Loss* adalah persentase paket hilang dalam transit (kritis untuk aplikasi *real-time*).
52. *Perception Layer* atau *sensor layer* adalah perangkat *IoT endpoint* bertanggung jawab dalam penginderaan (sensor) dan juga dapat dilengkapi dengan *actuator*.
53. *Physical Tampering* adalah upaya merusak atau memodifikasi secara fisik (membongkar, memutus kabel, memanipulasi komponen) suatu perangkat keras (seperti sensor atau *gateway*) dengan tujuan agar perangkat berhenti berfungsi atau mengompromikan keamanannya.
54. *Predictive Maintenance* adalah deteksi dini kegagalan yang dapat dilakukan dengan penerapan *machine learning* untuk mendeteksi kegagalan dari pola historis dan digunakan untuk pengelolaan pemeliharaan.
55. *Privacy Violations* adalah pelanggaran terhadap hak individu untuk mengontrol bagaimana data pribadi mereka dikumpulkan, disimpan, dan digunakan. Ini terjadi ketika data dikumpulkan atau diolah tanpa persetujuan atau di luar tujuan yang ditentukan.
56. *Protocol Vulnerabilities* (MQTT/CoAP) adalah kelemahan, cacat, atau *bug* dalam desain atau implementasi protokol komunikasi standar (seperti MQTT atau CoAP) yang dapat dimanfaatkan oleh penyerang untuk mengganggu komunikasi atau mencuri data.
57. *Quality of Service* (QoS) adalah serangkaian teknik untuk mengelola prioritas trafik jaringan untuk *data delivery* yang andal, latensi rendah untuk aplikasi *real-time*, dan pemanfaatan *bandwidth* yang optimal.
58. RBAC (*Role-Based Access Control*) adalam mekanisme pengendalian keamanan pada *Application Layer* untuk otentikasi yang berbasis peran atau kewenangan.
59. *Real-time* atau waktu-nyata adalah istilah yang mengacu pada pengumpulan, analisis data , dan pemantauan data yang terjadi pada saat itu juga.
60. *Secure Boot* adalah fitur keamanan pada *firmware* (BIOS/UEFI) yang memastikan bahwa hanya perangkat lunak yang ditandatangani secara digital dan tepercaya (seperti sistem operasi) yang dapat dimuat saat komputer dinyalakan. Ini mencegah malware mengambil alih proses *boot* awal
61. *Security Analytics* adalah proses pengumpulan, agregasi, dan analisis data keamanan dalam jumlah besar (*log* sistem, *event* jaringan) menggunakan

*tool* dan teknik canggih (seperti ML dan AI) untuk mengidentifikasi ancaman, tren serangan, dan pola risiko secara lebih efektif.

62. *SHA-256* adalah fungsi *hashing* kriptografi yang mengambil data (apapun ukurannya) dan menghasilkan *string* karakter unik dengan panjang tetap (256 *bit*). Perubahan sekecil apa pun pada data akan menghasilkan *hash* yang sangat berbeda.
63. Skalabilitas adalah dukungan pada perangkat IoT untuk penambahan perangkat baru dan kompatibilitas dengan teknologi masa depan.
64. SSL/TLS (*Secure Sockets Layer / Transport Layer Security*) adalah kriptografi standar yang digunakan untuk mengamankan komunikasi data di internet (termasuk yang digunakan oleh HTTPS), yang merupakan lapisan keamanan yang memastikan bahwa data yang dikirim antara dua titik (misalnya sensor dan *server*) tetap rahasia dan tidak dapat diotak-atik.
65. *Support Layer* atau *gateway layer* atau *edge layer* adalah lapisan yang bertanggung jawab untuk memastikan data terotentikasi, terlindungi dengan baik, dan mengirimkan data ke *network layer*.
66. *Throughput* adalah jumlah data yang sukses dikirim per detik.
67. TLS/DTLS adalah protokol kriptografi standar industri yang digunakan untuk mengamankan komunikasi melalui jaringan komputer. Ini memastikan bahwa data yang dikirim antara dua aplikasi (misalnya *web browser* dan *server*) bersifat pribadi (*confidential*) dan integritasnya terjaga (*unaltered*). TLS adalah penerus dari SSL. DTLS adalah varian dari TLS yang dirancang untuk mengamankan komunikasi yang menggunakan protokol UDP (User Datagram Protocol), yang lebih cepat tetapi tidak menjamin pengiriman paket. DTLS penting dalam IoT, terutama untuk protokol ringan seperti CoAP.
68. *Trusted Platform Module (TPM)* adalah adalah sebuah chip kriptografi khusus yang tertanam pada *motherboard* komputer. Fungsinya adalah untuk menyimpan kunci enkripsi, sertifikat digital, dan *hash* pengukuran integritas secara aman, sehingga meningkatkan keamanan perangkat keras secara keseluruhan.
69. *Unauthorized Access* adalah upaya atau tindakan yang berhasil masuk atau mengakses sistem, data, atau sumber daya jaringan tanpa izin atau kredensial yang sah dari pemilik sistem.
70. *User-Centric* adalah prinsip di mana perangkat IoT harus memiliki antarmuka yang mudah digunakan dan kemampuan personalisasi.
71. *Zero-Touch Deployment* adalah metode otomatisasi yang memungkinkan perangkat keras atau perangkat lunak baru (seperti perangkat jaringan, server, komputer pengguna, atau perangkat IoT) dikonfigurasi, *provisioning*, dan disiapkan agar siap digunakan sepenuhnya tanpa memerlukan intervensi, atau konfigurasi manual oleh teknisi di lokasi pemasangan.

B. PENDAHULUAN

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) telah menyertakan Rencana Induk SPBE nasional pada lampirannya. Rencana induk SPBE nasional menekankan pemanfaatan

TIK yang efektif dan efisien melalui integrasi infrastruktur, sistem aplikasi, keamanan informasi, dan layanan TIK serta adopsi yang selektif yang disesuaikan dengan kondisi lingkungan internal dan eksternal Instansi Pusat dan Pemerintah Daerah.

Diantara teknologi masa depan yang diharapkan mendorong perubahan SPBE adalah sebagai berikut:

1. *Mobile internet,* merupakan akses internet yang menggunakan gawai personal.
2. *Cloud computing,* merupakan teknologi layanan berbagi pakai yang dapat diakses melalui internet untuk memberikan layanan data, aplikasi, dan infrastruktur kepada pengguna.
3. *Internet of Things* (IoT), merupakan perangkat elektronik yang dilengkapi dengan perangkat lunak, sensor, aktuator, dan konektivitas internet sehingga mampu melakukan pengiriman atau pertukaran data melalui akses internet.
4. *Big Data Analgtics,* merupakan teknologi analisis terhadap data yang berukuran sangat besar, tidak terstruktur, dan tidak diketahui pola, korelasi ataupun relasi antar data.
5. *Artificial Intelligence* (kecerdasan buatan), merupakan teknologi kecerdasan buatan pada mesin yang memiliki fungsi kognitif untuk melakukan pembelajaran dan pemecahan masalah sebagaimana halnya dilakukan oleh manusia.

Dalam rangka mendukung pemerintahan digital dan sejalan dengan perkembangan kebutuhan layanan administrasi pemerintahan dan layanan publik pada bidang infrastruktur pekerjaan umum, perlu ditetapkan standar penerapan teknologi terkait.

## C. RUANG LINGKUP DAN BATASAN

### 1. Ruang Lingkup

Pedoman ini berlaku bagi seluruh unit kerja di lingkungan Kementerian Pekerjaan Umum yang mengembangkan, mengoperasikan, dan/atau memanfaatkan teknologi IoT dan kecerdasan buatan dalam layanan SPBE.

### 2. Batasan

Pengembangan, pengoperasian, dan/atau pemanfaatan teknologi IoT dan kecerdasan buatan harus mematuhi seluruh ketentuan pada Pedoman Manajemen Keamanan Informasi dan tidak menggunakan data rahasia dan/atau data pribadi. Penggunaan data rahasia dan/atau data pribadi pada IoT dan/atau kecerdasan buatan pelru diatur pada ketentuan lain yang lebih spesifik.

D. PEDOMAN PENERAPAN *INTERNET OF THINGS* (IoT)

IoT dalam infrastruktur bidang Pekerjaan Umum mengacu pada penggunaan perangkat, sensor, dan perangkat lunak yang saling terhubung untuk memantau, mengelola, dan mengoptimalkan berbagai aspek infrastruktur publik seperti gedung, jembatan, sistem transportasi, dan utilitas lain terkait. IoT yang dimaksud termasuk yang menjadi bagian dari sistem IioT (*Industrial Internet of Things*), OT (*Operation Technology*), IACS (*Industrial Automation & Control Systems*), BACS (*Building Automation & Control Systems*), SCADA (*Supervisory Control and Data Acquistion*), dan sistem serupa yang digunakan dalam bidang infrastruktur pekerjaan umum.

IoT memungkinkan pengumpulan dan analisis data secara *real-time*, yang mengarah pada peningkatan efisiensi, pemeliharaan, keamanan, dan keselamatan pengelolaan infrastruktur bidang Pekerjaan Umum.

Standar ini dimaksudkan sebagai sebagai acuan dalam implementasi adopsi teknologi, sehingga aspek-aspek integrasi dan keamanan informasi SPBE dapat dicapai secara efektif dan efisien untuk menghasilkan layanan berkinerja tinggi.

1. Prinsip-prinsip Penerapan IoT

Prinsip IoT merupakan asas yang menjadi pertimbangan dalam penerapan IoT yang dikelola secara terintegrasi. Prinsip IoT memuat keseimbangan antara aspek manusia, lingkungan, dan teknologi, baik yang dinyatakan secara eksplisit maupun implisit. Prinsip IoT meliputi:

a. Otomatisasi

Perangkat IoT harus mampu beroperasi secara mandiri berdasarkan data sensor dan aturan yang ditetapkan.

b. Keterhubungan

Perangkat IoT harus terintegrasi melalui protokol standar untuk komunikasi antar-perangkat (*device-to-device*) dan dengan sistem pusat (*cloud/server*).

c. Manajemen Energi

Perangkat IoT harus menerapkan optimasi penggunaan daya, termasuk pengutamaan penggunaan sumber energi terbarukan dan *mode low-power* untuk perangkat *battery-operated*.

d. Keamanan Siber

Perangkat IoT harus menerapkan prinsip-prinsip keamanan siber termasuk namun tidak terbatas pada: enkripsi data, autentikasi perangkat, dan perlindungan dari serangan siber.

e. Analitik Data & Kecerdasan Buatan

Perangkat IoT harus mendukung proses pengumpulan data yang efektif untuk analitik data dan kecerdasan buatan melalui penggunaan *machine learning* untuk prediksi, deteksi anomali, dan pengambilan keputusan otomatis.

*f. User-Centric*

Perangkat IoT harus memiliki antarmuka yang mudah digunakan dan kemampuan personalisasi.

g. *Fleksibilitas* & Skalabilitas

Perangkat IoT harus memiliki dukungan untuk penambahan perangkat baru dan kompatibilitas dengan teknologi masa depan.

h. *Pemantauan* & Pemeliharaan

Perangkat IoT harus mampu melakukan pemantauan *real-time* dan peringatan (*alert*) untuk deteksi dini masalah.

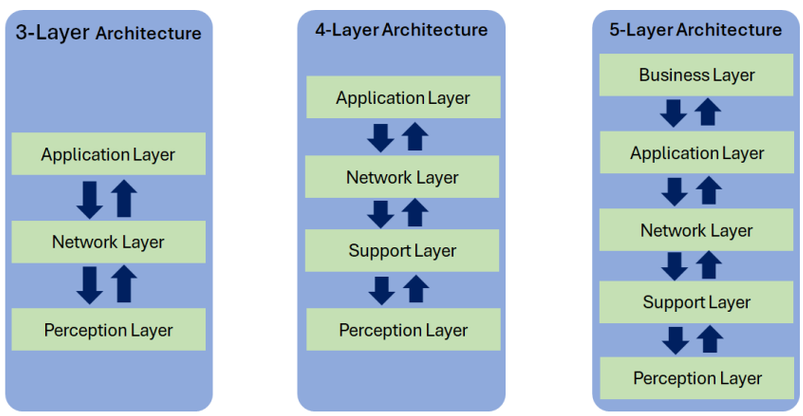
i. *Interoperabilitas*

Perangkat IoT harus memiliki kemampuan interoperabilitas yaitu dapat bekerja dengan berbagai *platform* dan protokol (misalnya MQTT, CoAP, HTTPS, LoRaWAN, dll.).

2. Arsitektur Sistem IoT

Arsitektur Sistem IoT merupakan kerangka kerja atau struktur yang mendefinisikan bagaimana perangkat IoT, jaringan, dan sistem terhubung dan berinteraksi untuk mencapai tujuan tertentu. Arsitektur Sistem IoT mengatur berbagai komponen, seperti sensor, jaringan, dan *platform cloud*, bekerja sama dalam sebuah ekosistem IoT.

Arsitektur IoT dapat menggunakan *3-layer*, *4-layer*, dan *5 layer architecture*.




*a. Perception Layer*

Lapisan ini juga disebut sebagai *sensor layer*, dimana perangkat *IoT endpoint* bertanggung jawab dalam penginderaan sesuai dengan

kebutuhan penerapannya. Penginderaan dapat terkait dengan lokasi, perubahan lingkungan, suhu, tekanan, gerakan, vibrasi, dan sebagainya. Pada perangkat tertentu, *IoT endpoint* juga dilengkapi dengan *actuator* yang memberikan respon sesuai desain penerapannya (misalnya memberikan peringatan, menyambungkan atau memutuskan arus listrik, membuka atau menutup *valve*, dan sebagainya).

b. *Support Layer*

Lapisan ini juga disebut *gateway layer* atau *edge layer.* Lapisan ini bertanggung jawab untuk memastikan bahwa data dikirim dari perangkat atau pengguna ~~yang~~ terotentikasi dan terlindungi dengan baik, serta mengirimkan data ke *network layer* baik melalui media kabel maupun nirkabel.

c. *Network Layer*

Lapisan ini juga disebut *transport layer* atau *communication layer* yang bertanggung jawab dalam transmisi data dari dan ke *application layer*. Lapisan ini dapat menggunakan media kabel maupun nirkabel.

d. *Application Layer*

Lapisan ini bertanggung jawab dalam pemrosesan dan menampilkan data kepada pengguna. Lapisan ini juga bertanggung jawab atas berbagai aplikasi ke berbagai pengguna sesuai dengan rancangan dan tujuan penerapannya. Beberapa aplikasi IoT yang dimaksud antara lain rumah pintar atau bangunan cerdas (*smart home* atau *smart building*), transportasi cerdas (*smart transportation*), kota cerdas (*smart city*), pertanian cerdas (*smart farming*), dan sebagainya.

e. *Business Layer*

Lapisan *business layer* berperan untuk mengintegrasikan aplikasi IoT dengan kebutuhan strategi organisasi. Lapisan ini bertanggung jawab dalam mengelola dan mengendalikan aplikasi-aplikasi IoT, pengguna, dan proses pengelolaan data dan informasi untuk mencapai tujuan bisnis atau organisasi.

3. Kriteria

Penerapan IoT mengacu pada standar teknis dan standar keamanan sebagai berikut:

a. Standar IoT

1) ISO/IEC 30141:2024, *Internet of Things (IoT) — Reference architecture*

2) SNI ISO/IEC 30162:2022, Internet untuk Segala (IoT) — persyaratan kompatibilitas dan model pada perangkat dalam sistem IoT untuk industri

3) SNI ISO/IEC TR 30164:2020, Internet untuk Segala (IoT) - *Edge computing*

4) SNI ISO/IEC 30165:2021, Internet untuk Segala (IoT) — Kerangka kerja IoT waktu nyata, 2. Internet untuk Segala (IoT) - *Edge computing*

5) SNI ISO/IEC 21823-1:2019 Internet untuk Segala (IoT) – Interoperabilitas untuk sistem Internet untuk Segala – Bagian 1:Kerangka kerja

6) ISO/IEC 21823-2:2020, *Internet of things (IoT) — Interoperability for IoT systems Part 2: Transport interoperability*

7) SNI ISO/IEC 30162:2022, Internet untuk Segala (IoT) — Persyaratan kompatibilitas dan model pada perangkat dalam sistem IoT untuk industri

8) SNI ISO/IEC 21481:2021, Telekomunikasi dan pertukaran informasi antara sistem — Antarmuka dan protokol 2 komunikasi medan dekat (Near field communication interface and protocol 2/NFCIP-2)

b. Standar Keamanan

1) ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*

2) ISO/IEC 27402:2023 — *IoT security and privacy — Device baseline requirements.*

3) ISO/IEC 27403:2024 — *IoT security and privacy — Guidelines for IoT-domotics.*

4) ISO/IEC 27404 FDIS (2025) — *IoT security and privacyy — Cybersecurity labelling framework for consumer IoT.*

5) SNI IEC TS 62443-1-1:2009, Jaringan komunikasi industri – Keamanan jaringan dan sistem – Bagian 1-1: Terminologi, konsep, dan model

6) SNI IEC TR 62443-2-3:2015, Keamanan automasi industri dan sistem kontrol — Bagian 2-3: Manajemen patch di lingkungan lACS

7) SNI IEC 62443-2-4:2015, Keamanan automasi industri dan sistem kontrol — Bagian 2-4: Persyaratan program keamanan untuk penyedia layanan IACS

8) SNI IEC TR 62443-3-1:2009, Jaringan komunikasi industri — Keamanan jaringan dan sistem — Bagian 3-1: Teknologi keamanan automasi industri dan sistem kontrol

9) SNI IEC 62443-3-2:2020, Keamanan automasi industri dan sistem kontrol — Bagian 3-2: Asesmen risiko keamanan untuk desain sistem

10) SNI IEC 62443-3-3:2013 Jaringan komunikasi industri — Keamanan jaringan dan sistem — Bagian 3-3: Persyaratan keamanan sistem dan level keamanan

11) SNI IEC 62443-4-1:2018, Keamanan automasi industri dan sistem kontrol — Bagian 4-1: Persyaratan siklus hidup pengembangan produk yang aman

12) SNI IEC 62443-4-2:2019, Keamanan automasi industri dan sistem kontrol — Bagian 4-2: Persyaratan keamanan teknis untuk komponen IACS

4. Manajemen Sistem IoT

Manajemen Sistem IoT harus didukung dengan *dashboard* yang menjadi antar-muka untuk mendukung pengelolaan operasional maupun memperoleh data & informasi guna mendukung berbagai keputusan organisasi yang relevan.

Ketentuan implementasi *dashboard* manajemen sistem IoT mencakup:

a. Ringkasan Kinerja dan Status Keseluruhan

Kemampuan menampilkan informasi ringkasan kinerja dan status keseluruhan diharapkan dapat memberikan gambaran global mengenai sistem IoT, antara lain:

1) Jumlah perangkat terhubung, misalnya mengenai total sensor, aktuator, dan gateway yang aktif.

2) Status sistem secara global, misalnya Indikator kesehatan sistem keseluruhan (dapat direpresentasikan dengan warna tertentu misalnya hijau = normal, kuning = peringatan, merah = kritis).

3) Peta geolokasi atau posisi perangkat dalam sistem sebagai bentuk visualisasi yang menunjukkan lokasi semua atau perangkat-perangkat kritis secara geografis atau pada sistem, dimana titik pada lokasi dapat berubah warna berdasarkan statusnya.

*Key performance indicators* (KPIs yang menampilkan metrik kinerja utama yang dihasilkan dari data IoT misalnya: tingkat konsumsi energi untuk gedung, rata-rata penggunaan air bersih, rata-rata tinggi muka air pada bendungan selama kurun waktu tertentu, dan sebagainya.

b. Pemantauan Data *Real-Time* dan Historis

Pemantauan data *real-time* dan historis diharapkan dapat menampilkan data yang dikumpulkan dari perangkat.

1) Grafik *Time-series*, yang menampilkan perubahan suatu variabel (suhu, kelembaban, tekanan, konsumsi daya) terhadap waktu

(detik, menit, jam, hari) yang sangat penting dalam analisis tren atas data.

2) Data Pengukuran, yang merupakan visualisasi sederhana yang menunjukkan nilai saat ini dan zona bahayanya (misalnya, pengukuran suhu yang menunjukkan apakah dalam batas normal).

3) Visualisasi numerik *real-time*, yang merupakan nilai terbaru dari sensor tertentu yang diperbarui secara *live*.

c. Pengelolaan dan Pemantauan Status Perangkat

Pengelolaan dan pemantauan status perangkat merupakan bagian khusus untuk mengelola dan memantau kondisi dari setiap perangkat IoT, antara lain:

1) Daftar perangkat yang dapat berupa tabel yang menampilkan semua perangkat dengan detail seperti nama, ID, status (*online/offline*), *firmware version*, dan waktu aktivitas terakhir (*last seen*).

2) Rincian konfigurasi perangkat yang mampu menampilkan informasi detil pada suatu perangkat dan ftiur yang dapat digunakan untuk mengubah konfigurasinya (misalnya, mengubah interval pengiriman data).

3) Status konektivitas yang menampilkan status koneksi perangkat IoT (misalnya kekuatan sinyal atau kualitas koneksi).

4) Pengelolaan *firmware* secara OTA (Over-The-Air) termasuk notifikasi jika terdapat *update firmware* dan kemampuan untuk melalukan *update* ke perangkat tertentu atau kelompok perangkat.

5) Daftar alarm aktif yang dapat berupa tabel yang menampilkan alarm yang sedang berlangsung, dilengkapi dengan tingkat keparahan (*Severity: Critical, Warning, Info*), waktu kejadian, dan perangkat sumber.

6) Visualisasi alarm yang dapat menggunakan perubahan warna (merah berkedip untuk kritis), *badge*, atau *pop-up* untuk menarik perhatian ke alarm atas kejadian yang dianggap penting.

7) Log historis alarm yang menyimpan riwayat semua alarm yang telah terjadi, disertai dengan tindakan yang telah diambil dan personil yang menanganinya.

d. Kontrol dan Automasi

Dashboard tidak hanya untuk dapat digunakan untuk mengelola dan memantau perangkat IoT, tetapi juga dapat digunakan untuk melakukan tindakan tertentu.

1) Tombol kontrol virtual yang dapat berupa tombol *on/off*, *slider*, atau *toggle* untuk mengendalikan aktuator dari jarak jauh misalnya: menyalakan lampu, mengunci pintu, atau mengatur *setpoint* suhu, dan sebagainya.

2) Status perintah yang memberikan fitur konfirmasi bahwa perintah telah dikirim dan dijalankan oleh perangkat.

3) Panel automasi atau *Rules Engine* yang memberikan tampilan sederhana dari aturan-aturan yang telah dibuat (misalnya *if - then rules* pada pengaturan "JIKA suhu > 30°C MAKA nyalakan AC", dan sebagainya)

e. Fitur Analitik dan Pelaporan

Fitur analitik dan pelaporan memiliki kemampuan mengubah data mentah menjadi informasi yang dapat ditindaklanjuti, misalnya berupa:

1) Laporan yang Dijadwalkan, yaitu fitur untuk menghasilkan laporan periodik (harian, mingguan, bulanan) dalam format PDF atau CSV, misalnya laporan konsumsi energi bulanan.

2) Visualisasi Data misalnya berupa *heatmaps* (untuk melihat kepadatan *event*), grafik batang/perbandingan, analisis statistik sederhana (rata-rata, maks/min, total), dan sebagainya.

f. Aspek Keamanan dan Audit

Dasboard harus memiliki kemampuan mengumpulkan data dan informasi untuk mendukung aspek keamanan dan audit, diantaranya:

1) Log aktivitas pengguna yang mencatat siapa saja yang login, kapan, dan tindakan apa yang dilakukan (misalnya, mengubah konfigurasi atau mengirim perintah).

2) Pemantauan ancaman keamanan, melalui pemantauan atas percobaan akses yang tidak sah atau aktivitas mencurigakan dari perangkat.

Adapun aspek-aspek penting dalam Manajemen Sistem IoT mencakup pengeloaan atas aspek-aspek:

a. *Device Management* (Manajemen Perangkat)

Manajemen perangkat mencakup aktivitas-aktivitas:

1) Identifikasi

   Setiap perangkat IoT harus dilakukan identifikasi dan memiliki penamaaan (*naming*) dan pengalamatan (*addressing*) yang dikelola dengan baik.

   Penamaan dapat menggunakan nama yang disepakati berdasarkan rencana yang ditetapkan (misalnya dengan menggunakan kode produk, atau penomoran menggunakan *Ucode* atau *Unique Code System* dengan pengaturan tertentu).

   Pengalamatan pada umumnya menggunakan *internet protocol* (IP) versi 4 atau IP versi 6.

2) Registrasi

   Setiap perangkat IoT harus diregistrasikan ke sistem IoT untuk memastikan perangkat IoT telah:

   a) Diregistrasi dengan kode unik;

   b) Dapat diotentikasi dengan baik; dan

   c) Dilakukan enkripsi.

3) Konfigurasi Perangkat

   Konfigurasi perangkat adalah proses mengatur parameter perangkat (seperti interval pengiriman data, *threshold sensor*, atau *firmware*) melalui *platform cloud*, jaringan lokal, *bluetooth*, *peer-to-peer network*, atau akses fisik perangkat.

   Pengelolaan konfigurasi direkomendasikan dapat dilakukan secara terpusat baik dengan menggunakan layanan *cloud* atau server & jaringan lokal (*local server/edge gateway*).

4) *Firmware update*

   Proses pembaruan *firmware* setiap perangkat IoT harus dikelola secara aman. Pembaruan *firmware* dapat dilakukan secara OTA (*Over-The-Air*).

5) *Health monitoring*

   Setiap perangkat IoT harus dapat dipantau kesehatannya untuk memastikan dapat beroperasi dengan baik. Proses pemantauan terus-menerus terhadap kondisi fisik, kinerja, dan keamanan perangkat IoT untuk memastikan:

   a) Ketersediaan (*availability*) perangkat, antara lain terkait dengan pemantauan kondisi fisik (suhu, kelembaban, daya baterai, dan sebagainya).

   b) Kinerja optimal (*performance*), antara lain terkait dengan *CPU/Memory Usage* pada perangkat *edge*, *uptime/downtime*

waktu operasional, dan *latency* dan *packet* loss komunikasi data.

c) Deteksi dini kegagalan (*predictive maintenance*), antara lain terkait dengan deteksi terhadap anomali perangkat. *Predictive maintenance* lebih jauh dapat dilakukan dengan penerapan *machine learning* untuk mendeteksi kegagalan dari pola historis.

d) Kepatuhan keamanan (*security compliance*) antara lain terkait dengan anomali trafik data, kegagalan otentikasi, dan pemantauan versi *firmware*.

Pemantauan kesehatan perangkat dapat dilakukan secara aktif *(active monitoring*, misalnya perangkat mengirim "ping" secara teratur ke server, atau pengiriman data status perangkat melalui REST API). Pemantauan secara pasif dapat dilakukan misalnya dengan *parsing log* perangkat untuk dilakukan analisis.

Log harus disimpan dan dilakukan analisis secara rutin. Data log harus dikumpulkan secara langsung dari sumber data (*IoT devices*).

Retensi penyimpanan log dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan dan/atau kebijakan teknis yang relevan. Evaluasi dan penyimpanan log ini selanjutnya digunakan sebagai penunjang pada kegiatan:

a) Pemeliharaan & peningkatan kinerja

b) Memenuhi kebutuhan audit teknis dan audit keamanan informasi

c) Evaluasi nilai manfaat atau *value* atas penerapan IoT.

b. *Network Management (Manajemen Jaringan)*

Manajemen jaringan bertanggung jawab dalam pengelolaan dan pemantauan infrastruktur jaringan pada lingkungan sistem IoT pada setiap lapisan (layer) secara terpadu. Manajemen jaringan berperan dalam:

1) *Provisioning* & Konfigurasi

Pengelolaan *provisioning* & konfigurasi misalnya penerapan alokasi IP statik, atau *Zero-Touch Deployment* dimana perangkat terkonfigurasi secara otomatis saat terhubung ke jaringan.

2) *Performance Monitoring*

Pemantauan kinerja jaringan antara lain terkait dengan *latency, jitter, packet loss,* dan *bandwidth pada* jaringan.

3) *Fault Management*

Berperan dalam deteksi kegagalan dan pemulihan gangguan pada jaringan, misalnya melalui penerapan *auto-failover* ke

*gateway* cadangan jika *gateway* utama *down*. *Fault management* juga digunakan dalam analisis pola kegagalan untuk perbaikan berkelanjutan.

4) *Security Management*

Melalui manajemen jaringan, aspek-aspek keamanan dapat dikelola penerapannya antara lain terkait dengan penerapan enkripsi, deteksi & perlindungan dari penyusupan (*intrusion detection & intrusion protection*), serta pemisahan segmentasi jaringan misalnya pemisahan segmen jaringan IoT dari segmen jaringan organisasi.

5) *Quality of Service* (QoS)

*Quality of Service* adalah serangkaian teknik untuk mengelola prioritas trafik jaringan *data delivery* yang andal, latensi rendah untuk aplikasi *real-time*, pemanfaatan *bandwidth* yang optimal, dan menghindari *packet loss*.

Parameter-parameter QoS antara lain

a) *Latency*, atau waktu pengiriman data *end-to-end*

b) *Jitter*, atau variasi *latency* antar paket

c) *Packet Loss*, atau persentase paket hilang dalam transit

d) *Throughput*, atau jumlah data yang sukses dikirim per detik

e) *Reliability*, atau keandalan pengiriman data.

Kriteria pada setiap parameter dapat berbeda, sesuai dengan kebutuhan dan tujuan penerapan dan pada umumnya ditetapkan pada tahap perencanaan.

c. *Data Management*

Data management pada Sistem IoT bertanggung jawab dalam mengumpulkan, menyimpan, memproses, menganalisis, dan mengamankan data yang dihasilkan oleh perangkat IoT untuk menghasilkan informasi yang dapat ditindaklanjuti.

1) Prinsip-prinsip Manajemen Data

Manajemen data dalam sistem IoT harus memperhatikan prinsip-prinsip manajemen data sebagai berikut:

a) Interoperabilitas

Data dari berbagai sumber dapat dipertukarkan dengan baik untuk memastikan keterpaduan pada penerapan sistem IoT.

b) Efisiensi

Penerapan standar data yang mendukung efisiensi proses pengelolaan data dalam hal utilisasi sumber daya, konsumsi *bandwidth*, dan meningkatkan kinerja secara keseluruhan.

c) Tepat Waktu (*Timely*)

Data yang dihasilkan, diolah, dan dikirimkan secara tepat waktu sesuai desain penerapan IoT dan tujuan penggunaan data serta kebutuhan layanan. Pihak Ketiga yang terlibat dalam penerapan IoT wajib memenuhi tingkat layanan sesuai dengan kesepakatan.

d) Akuntabilitas

Pengelolaan data memiliki kejelasan fungsi dan pertanggungjawaban data.

e) Skalabilitas

Pengelolaan data mendukung aspek skalabilitas yang memudahkan pengembangan sistem IoT, penambahan atau pengurangan perangkat baru dan integrasinya tanpa perubahan arsitektur yang signifikan.

f) Keamanan

Proses pengelolaan data memperhatikan aspek-aspek keamanan informasi terkait dengan kerahasian (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authenticity*), serta kenirsangkalan (*non repudiation*).

2) Standar Data

Proses pengelolaan dan pengolahan data menggunakan standar umum yang digunakan industri dan disesuaikan dengan kebutuhan dan desain sistem IoT, antara lain sebagai berikut:

| *Layer* | Fungsi Utama | Contoh Standar Format Data | Contoh Penggunaan Protocol |
|---|---|---|---|
| *Perception/ Device Layer* | Pengumpulan data dari sensor/aktuator | – JSON<br>– XML<br>– CBOR<br>– Protocol Buffers (Protobuf)<br>– Binary/ Hex<br>– dan lain-lain | – MQTT (JSON)<br>– CoAP (CBOR)<br>– LoRaWAN (Binary)<br>– dan lain-lain |
| *Support Layer* | Preprocessing & agregasi data di edge | – Avro<br>– Parquet<br>– CSV/TSV<br>– JSON<br>– dan lain-lain | – Apache Kafka (Avro)<br>– Edge Analytics (Parquet)<br>– dan lain-lain |
| *Network Layer* | Transmisi data ke cloud/server | – JSON<br>– CBOR | – MQTT/HTTP (JSON) |

| *Layer* | Fungsi Utama | Contoh Standar Format Data | Contoh Penggunaan Protocol |
|---|---|---|---|
| | | – Binary<br>– XML<br>– dan lain-lain | – CoAP (CBOR)<br>– LoRaWAN (Binary)<br>– dan lain-lain |
| *Application Layer* | Analisis & visualisasi data | – JSON<br>– XML<br>– GraphQL<br>– REST API Responses<br>– NoSQL Database (JSON, BSON)<br>– SQL Database (ProsgreSQL, MySQL, MSSQL, dsb.)<br>– Time-series database (InfluxDB, TimescaleDB)<br>– dan lain-lain | – REST/ GraphQL (JSON)<br>– WebSocket (Binary/ JSON)<br>– dan lain-lain |
| *Business Layer* | Integrasi dengan bisnis & keputusan | – JSON<br>– XML<br>– SQL/NoSQL Records<br>– Dashboard Formats<br>– dan lain-lain | – ERP/CRM (XML/JSON)<br>– Power BI (Parquet/CSV)<br>– dan lain-lain |

3) Kesesuaian dan Kepatuhan

Proses manajemen data memperhatikan dan mematuhi aspek-aspek kesesuaian (*conformance*) dan kepatuhan (*compliance*) terhadap peraturan perundang-undangan dan kebijakan serta petunjuk teknis internal yang relevan, terkait dengan Satu Data Indonesia, Perlindungan Data Pribadi, dan Keamanan Informasi SPBE.

d. *Security Management*

Manajemen keamanan dalam sistem IoT semakin krusial, seiring dengan peningkatan risiko keamanan informasi baik keamanan fisik maupun keamanan siber. Penerapan manajemen keamanan informasi sistem IoT dilaksanakan secara terpadu, sesuai dengan pedoman manajemen keamanan informasi SPBE.

Penerapan manajemen keamanan sistem IoT sekurang-kurangnya mencakup:

1) Peran & Tanggung Jawab

Terdapat kejelasan tujuan, peran dan tanggung jawab, serta adopsi standar yang digunakan dalam penerapan manajemen keamanan sistem IoT.

2) Risiko Keamanan Informasi

Terdapat proses identifikasi, analisis, dan rencana mitigasi risiko pada penerapan IoT. Proses manajemen risiko dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan dan kebijakan Kementerian.

3) Kontrol Keamanan

Terdapat kontrol keamanan yang diterapkan pada setiap risiko keamanan yang telah diidentifikasi. Berikut contoh potensi risiko dan kontrol keamanan pada sistem IoT.

| Layer | Potensi Risiko | Pengendalian (*Control*) Keamanan |
|---|---|---|
| *Perception/Device Layer* (Sensor, Aktuator, RFID) | – *Physical tampering*<br>– *Unauthorized access*<br>– *Malware* pada *firmware* | – *Secure Boot & TPM (Trusted Platform Module)*<br>– Enkripsi Data *(AES-128/256)*<br>– Autentikasi Perangkat *(Certificate-based)*<br>– Deteksi *Tampering* Fisik |
| *Support Layer (Gateway, Edge Computing)* | – *Man-in-the-Middle (MitM)*<br>– *Data corruption*<br>– *Edge device exploitation* | – *Firewall/IDS-IPS* Khusus IoT<br>– *Integrity Checks (SHA-256, Digital Signature)*<br>– *Enkripsi End-to-End* (sebelum transmisi cloud) |
| *Network Layer* (Wi-Fi, LoRaWAN, 5G, dll.) | – *Eavesdropping*<br>– *DDoS*<br>– *Protocol vulnerabilities (MQTT/CoAP)* | – *TLS/DTLS* untuk enkripsi<br>– *Network Segmentation*<br>– *Anomaly Detection (kecerdasan buatan/ML)*<br>– *Secure Protocols (MQTT-SN, CoAP+DTLS)* |
| *Application Layer (Dashboard, API, Analytics)* | – *API abuse*<br>– *Data leakage*<br>– *Insecure authentication* | – *RBAC (Role-Based Access Control)*<br>– *OAuth2.0 & API Gateways*<br>– *Data Anonymization*<br>– *Input Validation* |
| *Business Layer* (Pendukung Kebijakan, Monetisasi, *Compliance*) | – *Privacy violations*<br>– *Business logic attacks* | – *Compliance Framework (GDPR, NIST CSF)*<br>– *Security Analytics*<br>– *Incident Response Plan* |

4) Prosedur Keamanan

Terdapat prosedur operasional pengelolaan keamanan sistem IoT. Prosedur dapat ditetapkan sesuai dengan analisis risiko dan mitigasinya, serta kebutuhan pengendalian keamanan sistem IoT. Prosedur keamanan sistem IoT dapat mencakup antara lain:

a) Prosedur Pengelolaan *Update* & *Patch*

b) Prosedur Pengelolaan Otentikasi

c) Prosedur Pengelolaan Enkripsi dan Manajemen Kunci

d) Prosedur Tanggap Insiden Keamanan IoT

e. *Performance Monitoring & Optimization*

Pemantauan dan optimisasi sistem IoT bertujuan memastikan sistem IoT berjalan efisien, stabil, dan sesuai SLA (*Service Level Agreement*), serta mengidentifikasi peluang peningkatan kinerja secara berkelanjutan.

1) Aspek Pemantauan

Pemantauan dapat dilakukan sesuai dengan kebutuhan *(requirement)* layanan. Aspek-aspek yang dapat dilakukan pemantauan antara lain terkait dengan:

a) *Device performance*

(1) *Resource Utilization*, yaitu tingkat utilisasi CPU, RAM, dan daya pada perangkat *edge/gateway*.

(2) *Uptime/Downtime*, yaitu ketersediaan perangkat (misalnya sensor mati atau hidup).

(3) *Latency*, yaitu waktu respons perangkat (misalnya *delay* pada sensor suhu).

b) *Network performance*

(1) *Throughput,* yaitu volume data yang berhasil ditransfer per satuan waktu.

(2) *Packet Loss,* yaitu persentase data hilang dalam transmisi (kritis untuk aplikasi *real-time).*

(3) *Jitter & Latency,* yaitu variasi *delay* jaringan.

c) *Cloud/Backend Performance*

(1) *Database Query Time,* yaitu kecepatan akses data historis.

(2) *API Response Time,* yaitu *latency* pada permintaan data dari *dashboard* ke *backend.*

(3) *Scalability,* yaitu kemampuan mengakomodasi penambahan/pengurangan perangkat IoT dalam jumlah tertentu.

d) *Application Performance*

(4) *User Experience,* misalnya *load time* pada *dashboard* atau aplikasi *mobile.*

(5) *Error Rates* yaitu frekuensi kegagalan aplikasi dalam memproses *request.*

2) Optimisasi

Optimisasi pada sistem IoT antara lain bertujuan untuk meningkatkan efisiensi energi, *latency*, *bandwidth*, skalabilitas, dan keandalan sistem.

a) Efisiensi energi

Efisiensi dilakukan pengukuran dengan KPI tertentu pada setiap penerapan IoT (KPI merujuk pada BGC misalnya 25% untuk listrik, 10% air).

Efisiensi energi dapat dilakukan antara lain dengan cara:

(1) *Sleep schedulling*, dimana perangkat IoT (seperti sensor) diatur untuk aktif hanya saat diperlukan.

(2) *energy harvesting*, dengan memanfaatkan sumber energi alternatif untuk perangkat *low-power* (misalnya menggunakan tenaga surya, vibrasi, atau angin).

(3) *Dynamic Voltage Scaling* (DVS), misalnya menyesuaikan tegangan CPU sesuai beban kerja.

(4) Penggunaan komputasi hemat daya misalnya penggunaan mikroprosesor ARM Cortex-M atau RISC-V yang dirancang untuk IoT.

b) Reduksi *latency* dan optimisasi *bandwidth*

Reduksi *latency* dan optimisasi *bandwidth* dapat dilakukan antara lain dengan cara:

(1) Optimisasi Jaringan

Optimisasi jaringan dapat dilakukan antara lain dengan:

(a) *Edge computing*, dengan mengoptimalkan pengolahan data sedekat mungkin dengan sensor misalnya pada kamera keamanan dengan *on device AI.*

(b) Penggunaan protokol ringan dan *low latency*, misalnya MQTT dengan QoS atau penggunaan *web socke*I untuk komunikasi *full duplex real time*.

(c) Jaringan *dedicated* melalui *network slicing* dengan mengalokasikan bandwidth khusus untuk kebutuhan aplikasi yang bersifat *latency critical*.

(2) Optimisasi Arsitektur

(a) Strategi *cache* data hirarkis, misalnya L1 *Cache* pada level perangkat, L2 *Cache* pada layer *edge/gateway*, dan L3 *Cache* pada *cloud* CDN.

(b) *Load balancing*, misalnya melalui penerapan DNS-*based Load Balancer* untuk mengarahkan *traffic* ke server terdekat.

(c) *Time Sensitive networking*, misalnya penerapan standar IEEE 802.1 untuk menjamin *latency* deterministik di jaringan.

(3) Optimisasi Algoritma dan Data

(a) Penerapan *adaptive sampling rate*, dengan menyesuaikan frekuensi pengiriman data sesuai dengan kebutuhan.

(b) *Pre-processing* data pada *edge*, misalnya penerapan *filtering noise sensor* di tingkat *edge/gateway*.

(c) Penerapan ML ringan *(tiny-ML)*, misalnya *penerapan Tensor-Flow Lite* pada *micro-controller* pada deteksi anomali yang dilakukan pada tingkat *device.*

c) Skalabilitas

Penerapan arsitektur modular dan bertingkat pada umumnya lebih memudahkan dalam pengelolaan skalabilitas dan optimisasi sistem IoT.

5. Integrasi Sistem

Integrasi sistem *(system integration)* dalam konteks IoT merujuk pada proses menghubungkan sistem, data, aplikasi, dan Proses Bisnis secara otomatis untuk menciptakan aliran data dan informasi secara efisien dalam rangka penciptaan nilai manfaat *(value)* bagi organisasi serta mendukung pengambilan keputusan yang lebih baik.

Integrasi sistem IoT memiliki tantangan yang cukup besar antara lain disebabkan oleh:

a. Tantangan teknologi berupa keragaman perangkat dan standar teknis, fragmentasi protokol komunikasi, serta perbedaan format data dan semantik.

b. Tantangan keamanan dalam memastikan keamanan pertukaran data dan risiko-risiko *privacy*.

c. Isu-isu skalabilitas dan keragaman perangkat yang berbeda pada solusi yang berbeda.

Integrasi sistem IoT harus dirancang sejak tahap perencanaan melalui pemahaman terhadap:

d. Proses Bisnis (misalnya Proses Bisnis Bangunan Gedung Cerdas, Proses Bisnis Transportasi Cerdas, Proses Bisnis Kota Cerdas, dan sebagainya).

e. elemen-elemen sistem IoT serta standar terkait

f. spesifikasi teknis dan fungsi operasional integrasi sistem dan komponen-komponennya

g. aspek-aspek keamanan *(security requirement)* sesuai dengan peraturan perundang-undangan dan kebijakan internal.

h. Aspek-aspek kepatuhan dan kesesuaian dengan standar teknis, *privacy*, dan peraturan lain sesuai dengan sektor infrastruktur bidang pekerjaan umum yang relevan.

Integrasi sistem IoT dapat dilakukan dengan menggunakan perangkat integrasi sebagai berikut:

a. *Middleware*

   *Middleware* berfungsi sebagai jembatan antara perangkat IoT dan aplikasi yang berbeda, yang memungkinkan komunikasi antara platform perangkat keras dan perangkat lunak yang beragam. *Middleware* menyediakan *platform* umum untuk pertukaran dan integrasi data.

   *Middleware* mungkin memiliki kekurangan dalam hal ketersediaan perangkat pengelolaan *(management tools)* dan kapabilitas analitik data yang terdapat pada *platform IoT* yang lengkap.

b. *Platform* IoT

   Solusi platform IoT umumnya disediakan oleh swasta, termasuk didalamnya solusi *middleware* yang mengintegrasikan data dari perangkat IoT ke aplikasi dan solusi analitik data.

c. Metode Integrasi

   Integrasi dapat diterapkan pada beberapa level, yaitu level fisik dan *High Level Interface* (HLI) pada jaringan dan aplikasi, dan menyatukan sistem secara fisik dan fungsional. Integrasi secara fisik merujuk pada pemasangan kabel, ruang peralatan dan dukungan infrastruktur,

sementara integrasi secara fungsional pada HLI mengacu pada kemampuan beberapa sistem untuk saling beroperasi menjadi suatu integrasi fungsionalitas.

Metode integrasi sistem antara lain:

1) Integrasi Standar Terbuka (*Open System Interconnection* (OSI))

   Salah satu pendekatan metode ini yaitu dengan memilih dua protokol utama yang dapat mencakup hampir semua kebutuhan sistem seperti misalnya BACnet IP dan Modbus IP, atau *Local operating network* (LonWorks) IP dan Modbus IP.

2) Integrasi *Handshake*

   Sistem ini memungkinkan penggunaan sistem, fasilitas, atau produk dari dua pabrikan yang berbeda. Pabrikan mengembangkan *Application Programming Interface* (API) agar dua atau beberapa sistem yang berbeda dapat saling terhubung. Protokol ini umumnya digunakan untuk mengintegrasikan sistem BGC dengan sistem kota cerdas atau sistem lain yang lebih besar.

3) Kerangka Referensi

   Kerangka referensi untuk integrasi sistem dapat merujuk pada model OSI yang dikembangkan oleh *International Standards Organization* (ISO) berupa tujuh lapisan jaringan komunikasi informasi terbuka yang setiap lapisannya memiliki peran untuk melakukan komunikasi secara menyeluruh pada jaringan.

   Kerangka referensi integrasi dapat mengacu pada arsitektur sistem IoT yang dipergunakan (3-*layer*, 4-*layer*, atau 5-*layer architecture*). Pada dasarnya, arsitektur sistem IoT dapat dipetakan pada model 7-layer OSI. Contoh pemetaan 4-layer architecture sistem IoT ke model OSI sebagai berikut:

| *Layer* IoT | *Layer* OSI | Fungsi Utama |
|---|---|---|
| *Perception* | *Physical Layer* | *Transmisi bit data melalui media (kabel, radio, cahaya)* |
| | *Datalink Layer* | *Framing, MAC Address, Error Detection* |
| *Support Layer & Network Layer* | *Network Layer* | *Routing & IP Address* |
| | *Transport Layer* | *End-to-end data transminission reliability* |
| | *Session Layer* | *Session management* |
| | *Presentation Layer* | *Encryption, compression, format data* |

| *Layer* IoT | *Layer* OSI | Fungsi Utama |
|---|---|---|
| *Application Layer* | *Application Layer* | *Process & present data to end-users.* |
| *Business Layer* | *Application Layer* | *Process & present data to end-users. Analitik Data* |

6. Aspek Pengelolaan IoT

   a. Unit Kerja

      1) Aspek Bisnis

         a) Memastikan perencanaan dan implementasi IoT sesuai dengan kebutuhan bisnis, selaras dengan tugas dan fungsi unit kerja, serta rencana strategis Kementerian. Aktivitas ini antara lain dapat diwujudkan dengan pemetaan IKU Unit Organisasi atau Unit Kerja dengan rencana penerapan IoT.

         b) Melakukan analisis perubahan Proses Bisnis dan melakukan pembaruan, termasuk:

            i. Menganalisis dan menyusun model Proses Bisnis sebelum dan sesudah penerapan IoT dalam perencanaannya sebagai bagian dari inovasi Proses Bisnis.

            ii. Menyampaikan perubahan alur Proses Bisnis kepada Biro Kepegawaian dan Organisasi.

         c) Memastikan kesesuaian penerapan IoT selaras dengan Arsitektur SPBE dan Peta Rencana SPBE, antara lain terkait dengan:

            i. Menyusun perubahan Proses Bisnis karena penerapan IoT.

            ii. Melakukan pembaruan Arsitektur SPBE dan Peta Rencana SPBE.

      2) Aspek Data

         a) Memastikan pengelolaan data IoT memenuhi Pedoman Manajemen Data, dimana data dapat dibagi-pakaikan sesuai dengan ketentuan peraturan perundang-undangan.

         b) Melaksanakan aspek-aspek pengelolaan data lainnya seperti pengendalian akses, pencadangan dan pengujian cadangan data, serta pengelolaan log akses.

         c) Berkoordinasi dengan Unit Datin sebagai Koordinator Produsen Data dalam penyelenggaraan pengelolaan data.

      3) Aspek Teknologi

         a) Bertanggung jawab dalam pengelolaan operasional dan pemeliharaan perangkat pada penerapan IoT, termasuk penyusunan dan pelaksanaan rencana pemeliharaan sistem IoT.

b) Memastikan keterpaduan pemanfaatan teknologi melalui penerapan infrastruktur berbagi-pakai.

4) Aspek Keamanan

a) Memastikan penerapan aspek keamanan informasi pada tahap perencanaan, pembangunan/ pengembangan, dan operasionalisasi sistem IoT di unit kerja masing-masing.

b) Berkoordinasi dengan Unit Datin dalam pelaksanaan aspek keamanan informasi termasuk pelaksanaan uji kerentanan dan/atau uji penetrasi serta audit keamanan informasi.

b. Unit Datin

1) Aspek Data

a) Bertanggung jawab sebagai Koordinator Produsen Data pada unit organisasi terkait sebagaimana ketentuan pada Manajemen Data.

b) Memastikan penerapan prinsip manajemen data yaitu akurasi, mutakhir, terintegrasi, dapat diakses secara aman melalui pengelolaan siklus hidup data, serta memenuhi prinsip-prinsip Satu Data Indonesia.

2) Aspek Teknologi

a) Melakukan koordinasi dengan Unit Kerja terkait dengan perencanaan dan pembangunan/ pengembangan IoT untuk memastikan penerapan teknologi yang sesuai dengan kriteria dan standar yang ditetapkan.

b) Melakukan pemantauan dan evaluasi operasional IoT baik secara *adhoc* maupun periodik.

3) Aspek Keamanan

a) Melaksanakan penerapan manajemen keamanan informasi dalam siklus hidup IoT di Unit Organisasi masing-masing.

b) Mengoordinasikan dan mendokumentasikan pelaksanaan uji kerentanan dan/atau uji penetrasi pada sistem IoT.

c) Berkoordinasi dengan Pusdatin dalam penerapan keamanan informasi sistem IoT.

c. Pusdatin

1) Aspek Data

a) Bertanggung jawab sebagai Walidata Kementerian sebagaimana ketentuan pada Manajemen Data.

b) Melakukan pembinaan pengelolaan data untuk meningkatkan efisiensi, transparansi, dan akuntabilitas data.

2) Aspek Teknologi

a) Merumuskan dan menetapkan prinsip-prinsip dan standar teknologi IoT di lingkungan Kementerian.

b) Melakukan sosialisasi dan pengawasan penerapan prinsip-prinsip dan standar teknologi IoT di lingkungan Kementerian.

c) Memastikan integrasi penerapan sistem IoT.

3) Aspek Keamanan

a) Mengoordinasikan penerapan manajemen keamanan informasi pada penerapan IoT di lingkungan Kementerian.

b) Mengoordinasikan penanganan insiden keamanan informasi penerapan IoT di lingkungan Kementerian

c) Berkoordinasi dengan pihak-pihak terkait dalam pengelolaan keamaanan informasi dan penanganan insiden keamanan informasi.

d) Mengoordinasikan penyiapan data dan informasi yang diperlukan dalam mendukung pelaksanaan audit keamanan informasi.

e) Melakukan pembinaan penerapan keamanan informasi baik kepada pengelola sistem maupun pengguna akhir.

7. Evaluasi Penerapan IoT

Evaluasi terhadap penerapan IoT dilaksanakan secara periodik, sekurang-kurangnya satu kali dalam setahun. Pelaksanaan evaluasi penerapan IoT dikoordinasikan dengan Unit Datin dan Pusdatin.

8. Standar Industri

IoT sering kali berkembang pada masing-masing sektor industri, sehingga terdapat standar yang berbeda pada sektor industri tertentu. Selain standar yang pada sistem IoT di atas, beberapa standar dapat menjadi acuan sesuai dengan penerapan pada sektor masing-masing. Standar tersebut diantaranya:

a. Standar penerapan (*buiding management system* - BMS) pada Bangunan Gedung Cerdas:

1) ANSI/ASHRAE 135-2020, BACnet - A Data Communication Protocol for Building Automation and Control Networks atau perubahannya;

2) ISO 16484-1, Building Automation and Control Systems (BACS) - Part 1: Project Specification and Implementation atau perubahannya;

3) ISO 16484-2, Building Automation and Control Systems (BACS) -Part 2: Hardware atau perubahannya;

4) ISO 16484-3, Building Automation and Control Systems (BACS) - Part 3: Functions atau perubahannya;

5) ISO 16484-5, Building Automation and Control Systems (BACS) - Part 5: Data communication protocol atau perubahannya;

6) ISO 16484-6, Building Automation and Control Systems (BACS) - Part 6: Data communication conformance testing atau perubahannya;

7) IEC EN 61131-2, Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests atau perubahannya;

8) EN 61326, Electrical equipment for measurement, control, and laboratory use – EMC requirements atau perubahannya; dan

9) UL 916, UL Standard for Safety Energy Management Equipment atau perubahannya.

b. Standar dan acuan penerapan sistem alarm kebencanaan dan pemberitahuan massal

1) Peraturan perundang-undangan mengenai Persyaratan Teknis Sistem Proteksi Kebakaran pada Bangunan Gedung dan Lingkungan;

2) Peraturan perundang-undangan mengenai Pedoman Sistem Informasi dan Komunikasi Penanggulangan Bencana;

3) SNI 03-3985-2000 Tata cara perencanaan pemasangan dan pengujian sistem deteksi dan alarm kebakaran untuk pencegahan bahaya kebakaran pada Bangunan Gedung atau perubahannya;

4) SNI 03-6574-2001 Tata cara perancangan pencahayaan darurat, tanda arah, dan sistem peringatan bahaya pada Bangunan Gedung atau perubahannya;

5) NFPA 72-2022 National Fire Alarm and Signaling Code atau perubahannya;

6) NFPA 101-2021 Life Safety Code atau perubahannya;

7) UL 268 7th Edition Smoke Detector Standard atau perubahannya;

8) EN 54 Series on Fire Detection and Fire Alarm Systems atau perubahannya;

9) ISO 7240 Fire Detection and Alarm Systems atau perubahannya;

10) ISO 22322:2022 Security and resilience - Emergency management - Guidelines for public warning atau perubahannya;

11) ISO 22324:2022 Security and resilience - Emergency management - Guidelines for colour-coded alert atau perubahannya;

12) ISO 22325:2016 Security and resilience - Emergency management - Guidelines for capability assessment atau perubahannya;

13) ISO 22329:2021 Security and resilience - Emergency management - Guidelines for the use of social media in emergencies atau perubahannya;

14) ISO 8201:2017 Alarm systems - Audible emergency evacuation signal - Requirements atau perubahannya;

15) SNI ISO 22320:2012 Keamanan masyarakat - Manajemen kedaruratan - Persyaratan untuk penanganan insiden atau perubahannya; dan

16) SNI ISO/IEC 27037:2014 Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital atau perubahannya.

c. Standar dan acuan penerapan sistem kamera pengawas

1) ISO 22311:2012 Societal security — Video-surveillance — Export interoperability atau perubahannya;

2) ISO 30137 Information technology - Use of biometrics in video surveillance systems atau perubahannya;

3) SNI ISO/IEC 27037:2014 Teknologi Informasi – Teknik Keamanan – Pedoman Identifikasi, pengumpulan, akuisisi, dan preservasi bukti digital atau perubahannya; dan

4) IEEE 2410-2020 Standard for Biometrics Open Protocol Extended Frameworks (OPEN) atau perubahannya.

d. Standar dan Acuan Sistem Akses

1) ISO/IEC 27001 Sistem Manajemen Keamanan Informasi, atau perubahannya;

2) FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors atau perubahannya;

3) UL 294 UL Standard for Safety Access Control System Units atau perubahannya;

4) ANSI/BHMA A156.25 Electrified Looking Devices atau perubahannya;

5) IEC 60839-11-1:2013 Alarm and electronic security systems - Part 11-1: Electronic access control systems - System an components requirements atau perubahannya;

6) IEC 60839-11-2:2014 Alarm and electronic security systems - Part 11-2: Electronic access control systems - Application guidelines atau perubahannya;

7) ISO/IEC 19794-6:2019 Information technology - Biometric data interchange formats - Part 6: Iris image data atau perubahannya;

8) ISO/IEC 19794-5:2011 Information technology - Biometric data interchange formats - Part 5: Face image data atau perubahannya;

9) IEEE 2410-2020 Standard for Biometrics Open Protocol Extended Frameworks (OPEN) atau perubahannya; dan

10) ISO 14762 Information technology — Functional safety requirements for Home and Building Electronic Systems (HBES) atau perubahannya.

e. Standar dan acuan penerapan sistem audio visual

1) Peraturan perundang-undangan mengenai Pemberlakuan Standar Nasional Indonesia Audio Video dan Elektronika Sejenis secara Wajib;

2) SNI 04-2233-1991 Penguat audio Hi Fi, Persyaratan unjuk kerja minimum atau perubahannya;

3) SNI 04-2234-1991 Sistem dan peralatan audio Hi Fi, Persyaratan umum atau perubahannya;

4) SNI 04-6709.1-2002 Peralatan dan sistem audio visual, video dan televisi - Bagian 1: Umum atau perubahannya;

5) SNI 04-6714.1-2002 Peralatan tata suara - Bagian 1: Umum atau perubahannya;

6) SNI 04-6253-2003 Peralatan audio, video dan elektronika– sejenis - Persyaratan keselamatan atau perubahannya;

7) SNI 04-6709.2-2004 Peralatan dan sistem audiovisual, videodan televisi - Bagian 2: Definisi istilah umum atau perubahannya;

8) SNI 04-6709.10-2004 Peralatan dan sistem audiovisual, video dan televisi - Bagian 10: Sistem kaset audio atau perubahannya;

9) SNI IEC 61883-1:2009 Perlengkapan video/audio konsumen - antarmuka digital Bagian 1: Umum atau perubahannya; dan

10) SNI IEC 62368-1:2014 Peralatan audio/video, teknologi informasi dan komunikasi – Bagian 1: Persyaratan keselamatan atau perubahannya.

f. Standar acuan sistem pencahayaan

1) SNI 6197:2020 Konservasi energi sistem pencahayaan atau perubahannya;

2) SNI 03-6575-2001 Tata cara perancangan sistem pencahayaan buatan pada Bangunan Gedung atau perubahannya;

3) SNI 03-2396-2001 Tata cara perancangan sistem pencahayaan alami pada Bangunan Gedung atau perubahannya;

4) SNI IEC 60929:2009 Balast elektronik bertegangan a.b. - Untuk lampu fluoresen tabung - Persyaratan kinerja atau perubahannya; dan

5) ISO/CIE 20086:2019 *Light and lighting — Energy performance of lighting in buildings* atau perubahannya.

g. Standar acuan penerapan sistem penyediaan air minum

1) Peraturan perundang-undangan mengenai Penilaian Kinerja Bangunan Gedung Hijau.

2) Peraturan perundang-undangan mengenai Kesehatan Lingkungan;

3) ISA 112 SCADA System atau perubahannya;

4) ISA 18.2 Management of Alarm Systems for the Process Industries atau perubahannya;

5) Peraturan terakhir dari "Peralatan listrik dan bangunan" yang diterbitkan IEE dan NEC (IEC 61158/Modbus TCP Slave) atau perubahannya;

h. Standar acuan penerapan sistem pengelolaan air limbah

1) ISA 112 SCADA System atau perubahannya;

2) ISA 18.2 *Management of Alarm Systems for the Process Industries* atau perubahannya;

3) Peraturan terakhir dari "Peralatan listrik dan bangunan" yang diterbitkan IEEE dan NEC (IEC 61158/Modbus TCP Slave) atau perubahannya.

E. PEDOMAN PENERAPAN KECERDASAN BUATAN (*ARTIFICIAL INTELLIGENCE*)

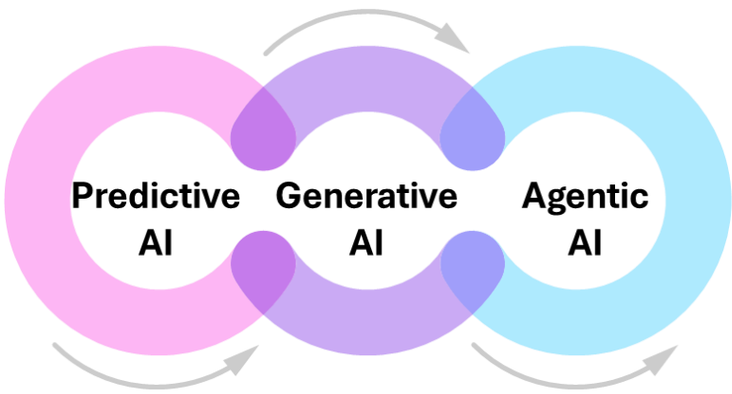
Penerapan kecerdasan buatan telah merambah berbagai bidang termasuk sektor publik, dalam hal ini penyelenggaraan administrasi pemerintahan maupun layanan publik. Penerapan kecerdasan buatan memiliki potensi besar untuk meningkatkan efisiensi, transparansi, dan kualitas pada penyelenggaraan administrasi pemerintahan maupun layanan publik.

Saat ini, kecerdasan buatan diterapkan dengan 3 (tiga) model penggunaan, yaitu:

1. Kecerdasan Buatan Prediktif adalah kecerdasan buatan yang memprediksi apa yang akan terjadi berdasarkan data masa lalu, belajar dari pola-pola sebelumnya, dan memperkirakan kemungkinan kejadian di masa depan. Penggunaan Kecerdasan Buatan Prediktif misalnya pada deteksi penyimpangan pra audit, prakiraan kejadian bencana, prakiraan kebutuhan anggaran, sistem pendukung kebijakan, dan sebagainya.

2. Kecerdasan Buatan Generatif adalah adalah kecerdasan buatan yang menciptakan sesuatu yang baru, seperti teks, gambar, musik, atau kode. Penggunaan Kecerdasan Buatan Generatif ini misalnya pada pembuatan transkripsi dan rangkuman hasil rapat, otomasi penyusunan laporan berdasarkan data akumulatif maupun waktu-nyata, inisiasi perancangan draft peraturan, *chatbot*, dan sebagainya.
3. Kecerdasan Buatan Agentik adalah kecerdasan buatan yang bisa bertindak sendiri untuk mencapai tujuan, seperti asisten digital yang mandiri atau *autonomous driving*. kecerdasan buatan Agentik menerima tugas, merencanakan langkah-langkah, dan melaksanakannya tanpa perlu diarahkan secara terus-menerus. Penggunaan Kecerdasan Buatan Agentik misalnya pada penanganan permintaan layanan sesuai dengan aturan tertentu, penggunaan pada kendaraan otonom, verifikasi dan validasi dokumen, pemantauan kemajuan proyek, dan sebagainya.

Berikut gambaran ketiga model kecerdasan artifsial yang umum digunakan saat ini.




Pemanfaatan kecerdasan buatan di Kementerian sebagai bagian dari penyelenggaraan SPBE memiliki peluang dan tantangan yang cukup besar dan kompleks. Untuk itu diperlukan panduan dasar dalam penerapannya.

1. Prinsip-prinsip Penerapan Kecerdasan Buatan

   Dalam rangka mitigasi risiko dan mengoptimalkan pemanfaatan kecerdasan buatan, diperlukan kerangka perilaku (*code of conduct*) yang dapat menjadi panduan untuk memastikan aplikasi berbasis kecerdasan buatan yang dimanfaatkan telah memenuhi prinsip-prinsip yang berlaku secara global. Penerapan kecerdasan buatan mengacu pada prinsip-prinsip sebagai berikut:

   a. Proporsionalitas dan Tidak Merusak (*Proportionality and Do Not Harm*)

      Penggunaan sistem kecerdasan buatan harus selalu proporsional dengan tujuan yang ingin dicapai. Prinsip ini menekankan pentingnya melakukan penilaian risiko secara menyeluruh untuk

memastikan bahwa kecerdasan buatan tidak menimbulkan kerugian—baik terhadap individu, kelompok, maupun lingkungan.

b. Keselamatan dan Keamanan (*Safety & Security*)

Penerapan kecerdasan buatan harus memperhatikan aspek keselamatan dan keamanan sepanjang siklus hidupnya. Langkah-langkah keamanan yang dapat diambil meliputi penerapan enkripsi data, pencegahan akses tidak sah, pengujian keamanan berkala, serta pengembangan sistem kecerdasan buatan yang dapat mendeteksi dan merespons ancaman secara otomatis. kecerdasan buatan yang aman dan terlindungi dimungkinkan melalui pengembangan kerangka kerja akses data berkelanjutan dan melindungi privasi yang mendorong pelatihan dan validasi model kecerdasan buatan yang lebih baik dengan memanfaatkan data berkualitas.

c. Keadilan dan Non-Diskriminasi (*Fairness and Non-discrimination*)

Sistem kecerdasan buatan harus dipastikan tidak mendorong terjadinya bias atau diskriminasi terhadap kelompok tertentu (ras, warna kulit, asal-usul, jenis kelamin, usia, bahasa, agama, pandangan politik, kebangsaan, etnisitas, status sosial, kondisi ekonomi atau sosial, atau disabilitas atau alasan lainnya), serta mendukung perwujudan keadilan sosial. Pendekatan inklusif sangat diperlukan agar semua kelompok, terutama yang rentan, mendapatkan manfaat yang sama dari teknologi kecerdasan buatan. Siklus hidup kecerdasan buatan harus dapat berkontribusi pada tatanan dunia yang lebih adil dalam hal informasi, komunikasi, budaya, pendidikan, penelitian, serta stabilitas sosial-ekonomi dan politik.

d. Keberlanjutan (*Sustainability*)

kecerdasan buatan dikembangkan dan digunakan dengan mempertimbangkan dampaknya terhadap lingkungan dan keberlanjutan sosial, antara lain mencakup upaya untuk mengurangi jejak karbon dalam pengoperasian kecerdasan buatan, misalnya melalui penggunaan sumber energi terbarukan dalam Pusat Data dan optimalisasi penggunaan daya. kecerdasan buatan dapat dimanfaatkan untuk mendukung keberlanjutan, misalnya dalam pengelolaan sumber daya alam, pemantauan perubahan iklim, serta optimalisasi rantai pasokan agar lebih ramah lingkungan.

e. Privasi dan Perlindungan Data (*Right to Privacy, and Data Protection*)

Penerapan kecerdasan buatan menerapkan kerangka kerja perlindungan data dan data pribadi, yang mengacu pada prinsip dan standar perlindungan data terkait dengan pengumpulan, penggunaan, dan pengungkapan serta pemrosesan data pribadi melalui proses persetujuan yang sah.

Penerapan kecerdasan buatan harus memastikan aspek pertanggungjawaban atas desain dan implementasi sistem kecerdasan buatan untuk memastikan bahwa informasi pribadi dilindungi sepanjang siklus hidup sistem kecerdasan buatan.

f. Pengawasan dan Penentuan oleh Manusia (*Human oversight and determination*)

Penerapan kecerdasan buatan harus memungkinkan pengawasan tidak hanya oleh individual, tetapi juga pengawasan publik yang inklusif. kecerdasan buatan mungkin dapat diandalkan dalam pengambilan keputusan tetapi tidak dapat menggantikan pertanggungjawaban manusia. Sebagai aturan dasar, keputusan yang menyangkut nyawa tidak boleh diserahkan kepada sistem kecerdasan buatan.

g. Transparansi dan Keterbukaan (*Transparency and Explainability*)

Sistem kecerdasan buatan harus dapat dijelaskan dan dipahami oleh pengguna serta pemangku kepentingan. Pengguna dapat mengetahui bagaimana kecerdasan buatan bekerja dan bagaimana keputusan dibuat.

Transparansi dan kejelasan sistem kecerdasan buatan menjadi prasyarat penting untuk memastikan penghormatan, perlindungan, dan promosi hak asasi manusia, kebebasan fundamental, dan prinsip-prinsip etika. Transparansi diperlukan agar pertanggungjawaban yang relevan dapat bekerja secara efektif.

h. Tanggung Jawab dan Akuntabilitas (*Responsibility and accountability*)

Setiap pihak yang mengembangkan, menerapkan, dan menggunakan kecerdasan buatan harus bertanggung jawab atas dampak yang ditimbulkan. Hal ini dapat diwujudkan melalui regulasi yang mewajibkan perusahaan teknologi untuk melakukan audit algoritma secara berkala guna memastikan tidak ada bias atau dampak negatif yang tidak terduga.

i. Kesadaran dan Literasi *(Awareness and Literacy)*

Kesadaran dan pemahaman publik terhadap teknologi kecerdasan buatan dan nilai data harus ditingkatkan melalui pendidikan yang terbuka dan mudah diakses, keterlibatan masyarakat, keterampilan digital dan pelatihan etika kecerdasan buatan, literasi dan pelatihan media dan informasi.

Penerapan kecerdasan buatan harus diikuti dengan edukasi dan peningkatan kesadaran, sehingga publik dapat mengambil keputusan yang tepat tentang penggunaan sistem kecerdasan buatan dan dilindungi dari pengaruh yang tidak semestinya.

j. Tata Kelola yang Adaptif, *Multi-Stakeholders* dan Kolaboratif (*Multi-stakeholder and adaptive governance and collaboration*)

Penerapan kecerdasan buatan diselenggarakan berlandaskan tata kelola yang adaptif dan melibatkan pemangku kepentingan yang relevan secara kolaboratif.

Partisipasi pemangku kepentingan pada seluruh siklus hidup sistem kecerdasan buatan diperlukan melalui pendekatan yang inklusif terhadap tata kelola kecerdasan buatan. Hal ini memungkinkan manfaat kecerdasan buatan terhadap semua pihak dan kontribusi pada pembangunan berkelanjutan. Para pemangku kepentingan termasuk tetapi tidak terbatas pada pemerintah, organisasi antarpemerintah, komunitas teknis, masyarakat sipil, peneliti dan akademisi, media, pendidikan, pembuat kebijakan, perusahaan sektor swasta, lembaga hak asasi manusia, atau kelompok lainnya.

2. Arsitektur Kecerdasan Buatan

Arsitektur Kecerdasan Buatan adalah kerangka kerja yang mendefinisikan struktur, komponen, dan alur kerja sistem kecerdasan buatan antara lain untuk memastikan:

a. Konsistensi desain antar-proyek kecerdasan buatan

b. Interoperabilitas dengan sistem yang telah ada

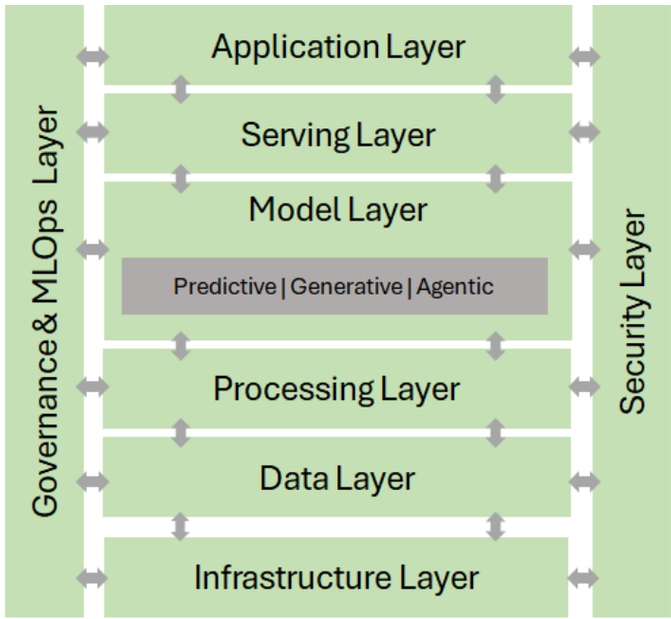
c. Kepatuhan terhadap regulasi dan etika

d. Skalabilitas untuk kebutuhan masa depan

Perancangan dan pembangunan model kecerdasan buatan merupakan tahap yang sangat penting dalam mengembangkan sistem kecerdasan buatan, di mana pilihan arsitektur secara signifikan memengaruhi kinerja dan skala sistem kecerdasan buatan. Sebagai inti dari sistem kecerdasan buatan, model merepresentasikan sebagian atau keseluruhan lingkungan eksternal yang menggambarkan struktur dan dinamika sistem tersebut (OECD, 2019).

Arsitektur kecerdasan buatan dapat direpresentasikan dengan berbagai pendekatan dan detil teknis yang bertingkat sesuai dengan kebutuhan dan tahapan pengembangan. Alur dasar sistem kecerdasan buatan umumnya serupa yaitu lapisan pada *data → processing → model → serving → application.* Setiap jenis kecerdasan buatan akan memiliki penekanan yang berbeda sesuai dengan model dan tujuan pengembangannya.

Secara umum arsitektur kecerdasan buatan digambarkan dengan komponen dan lapisan sebagai berikut:




3. *Application Layer*

   Merupakan lapisan yang menjadi antar-muka antara pengguna dan sistem kecerdasan buatan (UI/UX) dan pengelolaan sistem kecerdasan buatan termasuk integrasi sistem.

   Contoh lapisan ini adalah *chatbot*, *web* atau *mobile app*, dan *dashboard* analitik.

   a. *Serving Layer*

      Merupakan lapisan penghubung antara *application layer* dan *model layer* serta menyediakan model kecerdasan buatan dalam bentuk layanan untuk digunakan oleh aplikasi.

      Fungsi utama lapisan ini terkait dengan inference engine, yaitu:

      1) menjalankan model yang sudah dilatih (*pre-trained model*)
      2) melakukan optimasi kinerja, misalnya menyusun model dalam format yang lebih ringan dan cepat untuk dijalankan melalui *quantization* atau *pruning*)
      3) menyediakan antarmuka (API/REST) agar aplikasi lain (seperti chatbot atau dashboard publik) bisa mengakses model
      4) mengelola *monitoring & logging*, serta melacak performa, waktu respon, kesalahan, dan integritas model.

      Pada lapisan ini dapat terdiri dari beberapa komponen seperti:

      1) Model *Loader* yang berfungi memuat model dari *registry* (misal: MLflow, Hugging Face)

2) *Preprocessing Layer* yang berfungsi menyesuaikan input (misal: teks, data json) sehingga sesuai dengan format model
3) *Model Runtime* yatu *library* atau sistem yang menjalankan model (ONNX Runtime, TensorRT, TorchScript)
4) *Postprocessing Layer* yang berfungsi mengubah hasil model menjadi bentuk siap pakai (teks, label, probabilitas)
5) API Server yang menyediakan REST/gRPC API ke aplikasi *frontend*
6) *Metrics Collector* yang berfungsi melaporkan metrik ke sistem monitoring (Grafana, Prometheus)

b. *Model Layer*

Model layer merupakan inti dari sistem kecerdasan buatan. Pada layer ini, model dilatih berdasarkan data, diuji akurasinya, dan disiapkan untuk *deployment*. *Model layer* ini menangani:

1) Perancangan
2) Pelatihan (training)
3) Validasi
4) Penyimpanan *(registry)*, dan
5) Manajemen versi dari model kecerdasan buatan

Komponen pokok pada Model Layer dapat dilihat pada tabel berikut:

| Komponen | Fungsi | Contoh *Framework/ Tools* |
|---|---|---|
| *Data Input & Features* | menerima data yang sudah diproses (dari *Processing Layer*) | Scikit-learn (Preprocessing pipeline - scaling, encoding, imputation), Hugging Face Transformers (Tokenisasi dan input embedding untuk teks), TFX (TensorFlow Extended)- Feature store dan pipeline produksi |
| *Training Engine* | menjalankan proses pelatihan model menggunakan algoritma tertentu | TensorFlow, PyTorch, XGBoost, Scikit-learn |

| | | |
|---|---|---|
| *Experiment Tracking* | mencatat percobaan, parameter, dan hasil untuk perbandingan | MLflow, Weights & Biases, DVC |
| *Model Registry* | menyimpan versi model yang telah dilatih dan siap digunakan | MLflow Registry, SageMaker Model Hub |
| *Evaluation & Validation* | mengukur performa model terhadap data uji | Confusion matrix, ROC, AUC, MAE, bias/fairness metrics |
| *Model Versioning* | menyimpan versi model berdasarkan waktu, performa, atau *use case* | Mlflow, DVC (Data Version Control), SageMaker Model Registry, TensorFlow TFX + Model Analysis |

Model kecerdasan buatan yang dikelola dapat berupa Model Prediktif, Model Generatif, atau Model Agentik.

c. *Processing Layer*

Processing Layer bertanggung jawab atas proses transformasi data sumber menjadi data siap pakai untuk pelatihan dan inferensi model kecerdasan buatan.

Fungsi utama lapisan ini adalah:

1) Membersihkan data, misalnya dengan menghapus data duplikat, data rusak, atau nilai kosong.
2) Transformasi data melalui normalisasi, *encoding*, *scaling*, *log transform*, dan sebagainya.
3) *Feature engineering* yaitu membuat fitur baru dari data yang ada.
4) Integrasi data, dengan menggabungkan beberapa sumber data menjadi satu set.
5) Validasi data untuk memastikan konsistensi, akurasi, dan kelengkapan data.

*Framework* atau tools umum pada Processing Layer dapat dilihat pada tabel berikut:

| Kategori | Contoh *Tools* | Keterangan |
|---|---|---|
| Orkestrasi *pipeline* | Apache Airflow, Prefect, Luigi | Menjadwalkan dan mengatur proses ETL |
| Transformasi data | dbt (data build tool), Spark, Pandas, Dask | Transformasi skala besar atau lokal |

| | | |
|---|---|---|
| Stream processing | Apache Flink, Kafka Streams | Untuk data real-time seperti sensor atau antrian layanan |
| *Data cleaning* | Pandas, OpenRefine, Pyjanitor | Membersihkan dan menata data |
| Validasi data | Great Expectations, Deequ | Menetapkan aturan validasi & deteksi anomali data |
| *Feature Engineering* | Featuretools, Scikit-learn Pipeline, PyCaret | Otomatisasi dan modularisasi pembuatan fitur |
| *Monitoring pipeline* | Datafold, Monte Carlo, Soda | Observabilitas untuk kualitas & ketepatan data |

d. *Data Layer*

Data Layer adalah lapisan arsitektur kecerdasan buatan bertanggung jawab untuk:

1) Mengumpulkan data dari berbagai sumber
2) Menyimpan data dalam format yang efisien
3) Mengelola akses dan kualitas data
4) Mendistribusikan data ke lapisan-lapisan lain (seperti *processing* dan *modeling*).

Pada Data Layer dilakukan pengelolaan data sehingga dapat menjadi sumber daya yang tepercaya dan konsisten, tersimpan dalam format yang siap dianalisis, tersedia data yang aman & lengkap serta dapat dilacak ke sumbernya, dan mendukung integrasi data dari berbagai sumber.

Komponen proses dan fungsinya pada Data Layer ditabulasikan sebagai berikut:

| Komponen | Fungsi |
|---|---|
| *Data Sources* | Asal data: sistem administratif, sensor, aplikasi |
| *Data Ingestion* | Proses pengambilan data ke dalam sistem (*batch / real-time*) |
| *Storage* | Tempat menyimpan data (data lake, warehouse, database) |
| *Metadata & Catalog* | Sistem pengelolaan deskripsi data |
| *Data Lineage* | Pelacakan asal-usul dan transformasi data |
| *Access Control* | Mengatur siapa yang boleh melihat dan memodifikasi data |

| | |
|---|---|
| *Data Quality* | Validasi integritas, kelengkapan, dan akurasi data |

e. *Infrastructure Layer*

*Infrastructure Layer* merupakan fondasi fisik dan virtual yang menopang seluruh sistem kecerdasan buatan mulai dari penyimpanan data, pelatihan model, hingga *serving layer* dan *application layer*.

*Infrastructure Layer* adalah lapisan arsitektur kecerdasan buatan bertanggung jawab untuk:

1) Menyediakan prasarana komputasi, penyimpanan, jaringan, dan keamanan
2) Mendukung *scalability* (bisa berkembang sesuai beban kerja)
3) Menjamin *reliability* dan *availability* sistem
4) Menjadi dasar bagi *deployment* & operasi kecerdasan buatan secara berkelanjutan.

Komponen dan fungsi pada *Infrastructure Layer* ditabulasikan sebagai berikut:

| Komponen | Fungsi |
|---|---|
| *Compute* (Komputasi) | Menyediakan CPU, GPU, atau TPU untuk pelatihan & inferensi model |
| *Storage* (Penyimpanan) | Menyimpan data, model, log, serta metadata |
| *Network* (Jaringan) | Menjamin konektivitas antar sistem (cluster, cloud, API) |
| *Security* | Mengamankan akses, data, dan komunikasi antar komponen |
| *Containe*r & Orkestrasi | Menyediakan lingkungan isolasi dan otomatisasi deployment |
| *Cloud & On-Premises* | Infrastruktur dapat berbasis *cloud* publik, hybrid, atau lokal (private) |

f. *Security Layer*

*Security Layer* adalah lapisan lintas (*cross- layer*) yang menjamin bahwa seluruh sistem kecerdasan buatan — mulai dari data, pemrosesan, model, hingga aplikasi — aman dari ancaman, penyalahgunakan, atau kebocoran.

*Security Layer* adalah lapisan arsitektur kecerdasan buatan bertanggung jawab antara lain untuk:

1) Melindungi Data Sensitif
2) Mengontrol Akses ke data, model, dan sistem

3) Mendeteksi dan Merespon Ancaman secara real time
4) Menjaga Integritas dan Privasi Data
5) Memenuhi Regulasi (misalnya: UU PDP, ISO 27001, PP No. 71 Tahun 2019)

Area perlindungan pada *security layer* antara lain ditabulasikan sebagai berikut:

| Area | Perlindungan Keamanan |
|---|---|
| *Data Layer* | Enkripsi data saat penyimpanan (at rest) dan pengiriman (in transit) data |
| *Processing Layer* | Isolasi *pipeline* data dan audit proses manipulasi data |
| *Model Layer* | Perlindungan terhadap pencurian model (model theft) atau pencurian informasi dari model |
| *Inference / Serving* | Autentikasi API dan deteksi penyalahgunaan model kecerdasan buatan (misal *abuse chatbot*) |
| *Application Layer* | Perlindungan identitas pengguna, *rate-limiting,* dan *logging* aktivitas |

g. *Governance* & *MLOps Layer*

*Governance* & *MLOps Layer* dalam konteks dokumen ini menjalankan fungsi untuk mengatur *lifecycle model* kecerdasan buatan dan penerapan standar tata kelola (*auditing, versioning, reproducibility*) dalam pengembangan dan implementasinya, yang umumnya mengadopsi kerangka DevOps.

Fungsi-fungsi pokok lapisan ini ditabulasikan sebagai berikut:

| Fungsi Utama | Penjelasan |
|---|---|
| *Operationalization* | mengatur siklus hidup model dari *training* hingga *serving* |
| *Governance* | Memastikan kepatuhan pada kebijakan, hukum, standar, dan prinsip etika kecerdasan buatan |
| *Repeatability* | memastikan eksperimen bisa diulang & dilacak |
| *Auditability* | Memberikan kemampuan pelacakan siapa membuat model apa dan tujuannya |
| *Monitoring & Improvement* | memantau kinerja model dan memperbaruinya jika perlu |

Fungsi dan *tools* populer yang dapat dipergunakan pada *Governance & MLOps Layer* ditabulasikan sebagai berikut:

| Fungsi | *Tools* Populer |
|---|---|
| CI/CD MLOps | Kubeflow, MLflow, Metaflow, Airflow |
| Versioning | DVC, MLflow, Weights & Biases |
| Monitoring | Prometheus, Grafana, Arize, Fiddler |
| Governance | Apache Atlas, Collibra, Amundsen |
| Audit & Lineage | LakeFS, Sagemaker Audit Logs |
| Ethical kecerdasan buatan | IBM *Artificial intelligence* Explainability 360, Fairlearn |

4. Kriteria

Penerapan kecerdasan buatan mengacu pada standar teknis dan standar keamanan sebagai berikut:

a. Standar Penerapan Kecerdasan Buatan

1) ISO/IEC 38507:2022, Teknologi informasi — Tata kelola TI — Implikasi tata kelola penggunaan kecerdasan buatan oleh organisasi
2) SNI ISO/IEC 23053:2022, Kerangka kerja untuk Sistem Kecerdasaan Artifisial (KA) Menggunakan Pemelajaran Mesin (PM)
3) ISO/IEC 23894:2023 *Information technology — Artificial intelligence — Guidance on risk management*
4) ISO/IEC 42001:2023 *Information technology — Artificial intelligence — Management system*
5) ISO/IEC TR 24028:2020 *Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence.*

b. Standar Keamanan Kecerdasan Buatan

1) ISO/IEC 23894:2023 *Information technology — Artificial intelligence — Guidance on risk management*
2) ISO/IEC DIS 27090 (2025) *Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems.*
3) ISO/IEC DIS 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems
4) OWASP *Artificial Intelligence Security Verification Standard* (OWASP AISVS).

Penerapan kecerdasan buatan harus selalu memperhatikan dinamika peraturan perundang-undangan dan standar industri yang sedang berkembang. Penerapan standar di atas dapat disesuaikan dengan perkembangan terkini.

5. Manajemen Sistem Kecerdasan Buatan

Penerapan kecerdasan buatan harus diselenggarakan dalam konteks kebutuhan organisasi yang relevan, baik internal maupun eksternal. Konteks kebutuhan yang dimaksud perlu diidentifikasi untuk memastikan keselarasan antara rencana strategis organisasi dengan penerapan kecerdasan buatan. Identifikasi kebutuhan harus mencakup pemetaan kebutuhan pemangku kepentingan dan kepatuhan atas peraturan perundang-undangan terkait. Dengan demikian, ruang lingkup penerapan kecerdasan buatan memiliki definisi yang jelas.

Setiap penerapan kecerdasan buatan harus mendefinisikan organisasi pengelolaan yang mencerminkan bentuk pertanggungjawaban yang jelas dalam hal perencanaan, operasional, pengendalian, pemantauan dan evaluasi, serta peningkatan berkelanjutan. Hal ini diperlukan dalam memastikan penerapan kecerdasan buatan sejalan dengan prinsip-prinsip kecerdasan buatan yang telah disepakati secara global, keterpaduan pemanfaatan infrastruktur TIK, kepatuhan terhadap kebijakan dan peraturan perundang-undangan.

a. Aspek Perencanaan

Penerapan kecerdasan buatan harus direncanakan secara komprehensif untuk meminimalkan dampak negatif dan memaksimalkan manfaat kecerdasan buatan. Upaya ini dilakukan melalui serangkaian langkah-langkah identifikasi risiko, optimisasi peluang solusi, dan penetapan tujuan serta rencana pencapaiannya.

Risiko-risiko yang harus diidentifikasi antara lain terkait dengan bias algoritma, keamanan data, kesinambungan layanan, etika dan akuntabilitas, serta kepatuhan. Setiap risiko yang diidentifikasi harus dilakukan penilaian kemungkinan dan dampak serta dirumuskan rencana mitigasinya.

Tujuan penerapan kecerdasan buatan secara umum harus konsisten dengan kebijakan terkait kecerdasan buatan, dapat diukur, mempertimbangkan persyaratan yang berlaku, dapat dipantau, dan diperbarui dengan benar, serta didokumentasikan.

Rencana pencapaian tujuan penerapan kecerdasan buatan mendefinisikan langkah-langkah apa yang akan dilakukan, siapa saja yang terlibat, kebutuhan sumber daya, dan kriteria capaian yang dapat diukur.

b. Aspek Dukungan dan Sumber Daya

Penerapan kecerdasan buatan harus mengidentifikasi dan memastikan ketersediaan dukungan dan kebutuhan sumber daya, yang mencakup:

1) Sumber Daya

Penerapan kecerdasan buatan harus memastikan ketersediaan sumber daya dalam pembangunan dan pengembangan, implementasi dan operasional, pemeliharaan, serta peningkatan berkelanjutan.

2) Kompetensi

Penerapan kecerdasan buatan harus didukung dengan ketersediaan kompetensi sumber daya manusia yang mencukupi. Ketersediaan kompetensi dapat dilakukan melalui pendidikan, pelatihan, dan pengalaman.

3) Kesadaran

Setiap personil yang terlibat dalam penerapan kecerdasan buatan harus memiliki kesadaran *(awareness)* terkait dengan kebijakan mengenai kecerdasan buatan, peraturan perundang-undangan yang relevan, serta implikasi-implikasi yang mungkin terjadi atas ketaksesuaian penerapan kecerdasan buatan dengan persyaratan kebijakan, standar, dan peraturan perundang-undangan.

4) Komunikasi

Penerapan kecerdasan buatan harus menetapkan strategi dan mekanisme komunikasi dengan pihak-pihak internal maupun eksternal. Rencana komunikasi ini mencakup kebutuhan komunikasi yang relevan pada pemangku kepentingan yang sudah diidentifikasi.

5) Informasi yang didokumentasikan

Informasi yang diperlukan dalam penerapan kecerdasan buatan harus didokumentasikan sesuai dengan tata cara pengelolaaan dokumen baik pada proses pembuatan & pembaruan dokumentasi maupun pengendaliannya.

c. Aspek Operasional

Penerapan kecerdasan buatan harus didukung dengan rencana dan pengendalian operasional melalui penetapan kriteria setiap tahapan proses serta pengendalian proses sesuai dengan kriteria yang ditetapkan. Pengendalian operasional kecerdasan buatan selaras dengan rencana mitigasi risiko yang telah diidentifikasi, serta dilakukan pemantauan dan pengendalian dalam hal terjadi penyimpangan atas kriteria dari hasil yang diharapkan.

d. Aspek Pemantauan dan Evaluasi

Penerapan kecerdasan buatan harus menetapkan apa saja yang menjadi subjek pemantauan dan pengukuran kinerja, metode pemantauan dan pengukuran yang digunakan, serta kapan pelaksanaan dan evaluasi atas pemantauan dan pengukuran penerapan kecerdasan buatan.

Audit dapat menjadi bagian dari pemantauan dan evaluasi. Audit dapat dilaksanakan secara internal maupun eksternal sesuai dengan standar dan kriteria audit yang berlaku.

e. Aspek Peningkatan Berkelanjutan

Peningkatan berkelanjutan penerapan kecerdasan buatan dilaksanakan pada aspek-aspek kesesuaian, kecukupan, dan keefektifan penerapan kecerdasan buatan. Penilaian atau evaluasi terhadap ketaksesuaian penerapan kecerdasan buatan terhadap tujuan, perencanaan, prinsip-prinsip, kebijakan, dan peraturan perundang-undangan harus dilakukan secara periodik. Tindakan perbaikan atas ketaksesuaian yang

diidentifikasi harus direncanakan, diimplementasikan, dan dievaluasi keefektifannya.

6. Integrasi Kecerdasan Buatan

   Penerapan kecerdasan buatan harus mempertimbangkan sinergi pemanfaatan sumber daya secara optimal dan pengendalian risiko yang memadai. Untuk itu, penerapan kecerdasan buatan harus mengedepankan keterpaduan dengan mengintegrasikan pemanfaatan sumber daya, antara lain meliputi:

   a. Koordinasi dalam pengembangan
   b. Pemanfaatan *shared-infrastructure*
   c. Pemanfaatan data bersama
   d. Pengelolaan risiko
   e. Pengendalian keamanan yang lebih efektif

   Penerapan kecerdasan buatan harus dikoordinasikan dengan Unit Datin dan Pusdatin.

7. Aspek Pengelolaan Kecerdasan Buatan

   a. Unit Kerja

      1) Aspek Bisnis

         a) Mengidentifikasi peluang dan kebutuhan bisnis yang dapat dioptimalkan dengan solusi kecerdasan buatan, serta menyusun *business case* dan proposal inisiatif kecerdasan buatan.
         b) Menjadi pemilik (owner) dari model dan solusi kecerdasan buatan yang diimplementasikan, serta bertanggung jawab atas dampak dan *outcome*-nya terhadap pelayanan.
         c) Melakukan analisis perubahan Proses Bisnis dan menyusun SOP baru yang mengintegrasikan output kecerdasan buatan ke dalam alur kerja operasional, serta menyampaikan perubahan alur Proses Bisnis kepada Biro Kepegawaian dan Organisasi
         d) Menyediakan anggaran operasional untuk pemeliharaan dan pengembangan berkelanjutan solusi kecerdasan buatan di unitnya
         e) Memastikan perencanaan dan implementasi kecerdasan buatan sesuai dengan kebutuhan bisnis, selaras dengan tugas dan fungsi unit kerja, serta rencana strategis Kementerian. Aktivitas ini antara lain dapat diwujudkan dengan pemetaan IKU Unit Organisasi atau Unit Kerja dengan rencana penerapan kecerdasan buatan.
         f) Memastikan kesesuaian penerapan kecerdasan buatan selaras dengan Arsitektur SPBE dan Peta Rencana SPBE.

      2) Aspek Data

         a) Bertanggung jawab penuh sebagai Produsen Data atas ketersediaan, ketepatan waktu, akurasi, dan kelengkapan data (*data quality at source*).
         b) Melakukan validasi dan pembersihan data awal (*data cleansing at source*) sesuai dengan standar kualitas data yang ditetapkan.

c) Memastikan pengelolaan data kecerdasan buatan memenuhi Pedoman Manajemen Data, dimana data dapat dibagi-pakaikan sesuai dengan ketentuan peraturan perundang-undangan.

d) Melaksanakan aspek-aspek pengelolaan data lainnya seperti pengendalian akses, pencadangan dan pengujian cadangan data, serta pengelolaan log akses.

e) Berkoordinasi dengan Unit Datin sebagai Koordinator Produsen Data dalam penyelenggaraan pengelolaan data.

3) Aspek Teknologi

a) Melakukan pemantauan operasional harian performa model kecerdasan buatan (seperti model drift) dan melaporkan jika terjadi anomali atau penurunan akurasi.

b) Bertanggung jawab dalam penggunaan aplikasi kecerdasan buatan dan antarmuka pengguna (dashboard), termasuk pelatihan pengguna akhir.

c) Bertanggung jawab dalam pengelolaan operasional dan pemeliharaan pada penerapan kecerdasan buatan, termasuk penyusunan dan pelaksanaan rencana pemeliharaan sistem kecerdasan buatan.

d) Memastikan keterpaduan pemanfaatan teknologi melalui penerapan infrastruktur berbagi-pakai

4) Aspek Keamanan

a) Memastikan pengumpulan dan penggunaan data untuk kecerdasan buatan memenuhi aspek etika, regulasi, dan hukum (seperti perlindungan data pribadi) dalam domainnya.

b) Memastikan penerapan aspek keamanan informasi pada tahap perencanaan, pembangunan/ pengembangan, dan operasionalisasi sistem kecerdasan buatan di unit kerja masing-masing.

c) Melaporkan dugaan insiden keamanan informasi atau penyimpangan etika yang terkait dengan penggunaan kecerdasan buatan kepada Unit Datin.

d) Berkoordinasi dengan Unit Datin dalam pelaksanaan aspek keamanan informasi termasuk pelaksanaan uji kerentanan dan/atau uji penetrasi serta audit keamanan informasi.

b. Unit Datin

1) Aspek Data

a) Bertanggung jawab sebagai Koordinator Produsen Data pada unit organisasi terkait sebagaimana ketentuan pada Manajemen Data.

b) Memastikan penerapan prinsip manajemen data yaitu akurasi, mutakhir, terintegrasi, dapat diakses secara aman melalui pengelolaan siklus hidup data, serta memenuhi prinsip-prinsip Satu Data Indonesia.

c) Mengoordinasikan penerapan standar kualitas data, metadata, dan tata kelola data di unit Organisasi terkait.

d) Mengoordinasikan proses integrasi, transformasi, dan *enrichment* data dari berbagai Unit Kerja jika diperlukan.

e) Memantau kualitas dan kelancaran aliran data dan berkoordinasi dengan Unit Kerja untuk perbaikan.

2) Aspek Teknologi

a) Melakukan koordinasi dengan Unit Kerja terkait dengan perencanaan dan pembangunan/ pengembangan kecerdasan buatan untuk memastikan penerapan teknologi yang sesuai dengan kriteria dan standar yang ditetapkan.

b) Membantu Unit Kerja dalam menyusun spesifikasi teknis model kecerdasan buatan, seleksi *tools*/*platform*, dan melakukan pengawasan teknis selama pembangunan/pengembangan serta berkoordinasi dengan Pusdatin.

c) Melakukan pemantauan dan evaluasi operasional kecerdasan buatan baik secara *adhoc* maupun periodik.

3) Aspek Keamanan

a) Melaksanakan penerapan manajemen keamanan informasi dalam siklus hidup kecerdasan buatan di Unit Organisasi masing-masing.

b) Mengoordinasikan dan mendokumentasikan pelaksanaan uji kerentanan dan/atau uji penetrasi pada sistem kecerdasan buatan.

c) Mengoordinasikan pelaksanaan audit model kecerdasan buatan (*model audit*) dan *bias testing* untuk mendeteksi potensi bias yang tidak diinginkan.

d) Berkoordinasi dengan Pusdatin dalam penerapan keamanan informasi sistem kecerdasan buatan.

c. Pusdatin

1) Aspek Data

a) Bertanggung jawab sebagai Walidata Kementerian sebagaimana ketentuan pada Manajemen Data.

b) Melakukan pembinaan pengelolaan data untuk meningkatkan efisiensi, transparansi, dan akuntabilitas data.

2) Aspek Teknologi

a) Merumuskan dan menetapkan prinsip-prinsip dan standar teknologi kecerdasan buatan di lingkungan Kementerian.

b) Melakukan sosialisasi dan pengawasan penerapan prinsip-prinsip dan standar teknologi kecerdasan buatan di lingkungan Kementerian.

c) Memastikan integrasi penerapan sistem kecerdasan buatan.

3) Aspek Keamanan

a) Mengoordinasikan penerapan manajemen keamanan informasi pada penerapan kecerdasan buatan di lingkungan Kementerian.
b) Mengoordinasikan penanganan insiden keamanan informasi penerapan kecerdasan buatan di lingkungan Kementerian
c) Berkoordinasi dengan pihak-pihak terkait dalam pengelolaan keamaanan informasi dan penanganan insiden keamanan informasi.
d) Mengoordinasikan penyiapan data dan informasi yang diperlukan dalam mendukung pelaksanaan audit keamanan informasi.

MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA,

ttd.

DODY HANGGODO

LAMPIRAN II
PERATURAN MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2026
TENTANG
PENERAPAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

MANAJEMEN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

A. DAFTAR ISTILAH

Istilah yang dipergunakan pada lampiran Peraturan Menteri ini adalah sebagai berikut:

1. Aplikasi Layanan Publik adalah aplikasi yang digunakan dalam pelayanan publik baik masyarakat umum maupun dunia usaha.
2. Aplikasi Pendukung adalah aplikasi yang digunakan untuk mendukung operasional sebagai pelengkap sistem utama, menyediakan layanan pendukung seperti pengelolaan data, komunikasi, keamanan, atau integrasi.
3. Aplikasi Teknis adalah aplikasi yang digunakan dalam pelayanan teknis baik internal maupun eksternal sesuai dengan bidang tugas dan fungsi pada unit kerja tertentu.
4. Aplikasi Tingkat Kementerian adalah aplikasi yang digunakan oleh seluruh unit organisasi/unit kerja/UPT di lingkungan Kementerian Pekerjaan Umum.
5. Aset SPBE adalah sumber daya yang digunakan dalam penyelenggaraan SPBE.
6. Audit SPBE adalah pemeriksaan terhadap penyelenggaraan SPBE untuk menilai kesesuaian dengan ketentuan.
7. *Firmware* adalah jenis perangkat lunak permanen yang tertanam langsung pada perangkat keras (chip) perangkat. Fungsinya adalah untuk memberikan instruksi dasar tingkat rendah tentang bagaimana perangkat harus beroperasi dan mengelola dirinya sendiri.
8. Hak Akses adalah kewenangan pengguna untuk mengakses sumber daya SPBE.
9. Hak Akses Khusus adalah hak akses dengan kewenangan tinggi yang diberikan secara terbatas
10. Identitas Pengguna adalah identitas unik untuk mengenali pengguna sistem SPBE.
11. Insiden Keamanan Informasi adalah peristiwa yang mengganggu keamanan informasi SPBE.
12. *Instances* dalam penggunaan lisensi merepresentasikan satu instalasi atau penggunaan unik dari perangkat lunak. Dalam konteks komputasi awan, instance adalah unit komputasi yang digunakan untuk menjalankan aplikasi yang juga dapat berarti mesin virtual atau kontainer yang berjalan pada sistem komputasi awan.

13. Interoperabilitas adalah Kemampuan perangkat IoT untuk dapat bekerja dengan berbagai *platform* dan protokol.
14. Kenirsangkalan adalah jaminan bahwa suatu tindakan dalam sistem tidak dapat disangkal oleh pelakunya.
15. Kerahasiaan adalah jaminan bahwa data dan informasi hanya dapat diakses oleh pihak yang berwenang.
16. Ketersediaan adalah jaminan bahwa data, aplikasi, dan layanan SPBE dapat diakses saat dibutuhkan.
17. Keutuhan adalah jaminan bahwa data dan informasi terlindungi dari perubahan yang tidak sah.
18. *Key Performance Indicators* (KPIs) adalah metrik kinerja utama yang menampilkan metrik kinerja utama
19. *Malware* atau *Malicious Software* adalah rogram atau kode jahat yang dirancang untuk menyusup, merusak, atau mendapatkan akses tidak sah ke sistem komputer, *server*, atau jaringan (termasuk *virus*, *ransomware*, *spyware*).
20. Pemilik Sistem adalah pimpinan unit organisasi atau unit kerja yang bertanggung jawab dalam pembiayaan sistem elektronik atau aplikasi, pada umumnya adalah pengampu Proses Bisnis yang terkait pada sistem elektronik atau aplikasi.
21. Pencatatan Log adalah perekaman aktivitas sistem dan pengguna SPBE.
22. *Penetration testing* atau uji penetrasi adalah proses penilaian kerentanan keamanan informasi pada suatu sistem (yaitu jaringan komputer, sistem, aplikasi, atau bagian lain dari sistem TI) yang dilakukan dengan yang bersifat aktif berupa simulasi penyerangan.
23. Pengelola Sistem adalah tim atau unit kerja yang bertanggung jawab dalam penyelenggaraan pengelolaan sistem elektronik atau aplikasi.
24. Rencana Keberlangsungan Bisnis adalah rencana untuk menjaga keberlanjutan layanan SPBE.
25. Rencana Pemulihan Bencana adalah rencana pemulihan sistem SPBE setelah terjadi gangguan atau bencana.
26. Risiko Keamanan SPBE adalah potensi kejadian yang dapat mengganggu keamanan SPBE.
27. Skalabilitas adalah dukungan pada perangkat IoT untuk penambahan perangkat baru dan kompatibilitas dengan teknologi masa depan.
28. Uji Penetrasi, atau penetration testing adalah pengujian keamanan dengan simulasi serangan terhadap sistem SPBE.
29. *Virtual private server* adalah mesin server *virtual* yang bersifat unik dan independen secara logis, yang berbagi sumber daya dengan server *virtual* lain pada suatu server fisik.
30. *Vulnerability Assessment* atau penilaian kerentanan adalah proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat risiko pada kerentanan keamanan informasi pada suatu sistem (yaitu jaringan komputer, sistem, aplikasi, atau bagian lain dari sistem TI) yang dilakukan dengan menggunakan alat pemindaian (*scanning tools*) yang bersifat pasif tanpa simulasi penyerangan.

B. MANAJEMEN KEAMANAN INFORMASI SPBE

1. Manajemen keamanan informasi SPBE bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko Keamanan Informasi.

2. Penerapan manajemen keamanan informasi SPBE berlandaskan pada prinsip keamanan yang meliputi kerahasiaan, keutuhan, ketersediaan, kenirsangkalan otentikasi, otorisasi dan pencatatan terhadap sumber daya SPBE meliputi Data Digital, Infrastruktur SPBE, dan Aplikasi SPBE dan Platform Pemerintah Digital.

3. Manajemen Keamanan informasi SPBE dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.

4. Ruang Lingkup

   a. Isu internal keamanan informasi SPBE
      Isu-isu internal keamanan informasi SPBE mencakup:
      1) Penyelenggaraan layanan administrasi pemerintah dan layanan publik berbasis elektronik di lingkungan Kementerian semakin luas dan intensif serta memerlukan pengamanan yang memadai dan menyeluruh.
      2) Kewenangan pembangunan dan pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dimiliki pada setiap Unit Kerja Kementerian.
      3) Tantangan dalam pelaksanaan penerapan keamanan terhadap sumber daya SPBE.
      4) Kebutuhan pengendalian risiko keamanan dan peningkatan berkelanjutan dalam penyelenggaraan manajemen keamanan informasi SPBE Kementerian.
      5) Tingkat kesadaran keamanan informasi SPBE pada seluruh pegawai Kementerian yang relatif masih beragam.
      6) Isu internal lainnya yang selanjutnya diketahui atau diidentifikasi berdasarkan hasil proses manajemen risiko Keamanan SPBE.

   b. Isu eksternal manajemen keamanan informasi SPBE
      1) Potensi ancaman Keamanan SPBE yang semakin meningkat dan beragam, serta memiliki dampak risiko keamanan terhadap penyelenggaraan layanan SPBE.
      2) Peraturan perundang-undangan, standar dan praktik terbaik keamanan informasi serta teknologi yang semakin berkembang.
      3) Isu-isu eksternal lainnya yang selanjutnya diketahui atau diidentifikasi berdasarkan hasil proses manajemen risiko Keamanan SPBE.

   c. Ruang Lingkup Manajemen Keamanan Informasi SPBE
      Manajemen keamanan informasi SPBE mencakup seluruh aset informasi dan aset pemrosesan informasi Kementerian yang mencakup:

1) Data & informasi, yaitu data dan informasi yang dikelola dan menjadi tanggung jawab Kementerian.
2) Aplikasi untuk mendukung layanan administrasi Pemerintah dan Aplikasi mendukung layanan publik berbasis elektronik Kementerian. Aplikasi yang dimaksud adalah Aplikasi Tingkat Kementerian, Aplikasi Layanan Publik, Aplikasi Teknis, maupun Aplikasi Pendukung.
3) Infrastruktur SPBE Kementerian meliputi Pusat Data Kementerian, Jaringan Intra Kementerian dan Sistem Penghubung Layanan/*Aplication Programming Interface* (API) yang dimiliki atau dikelola Kementerian.
4) Aset pendukung SPBE lainnya seperti *platform* dan perangkat lunak, termasuk lisensi & hak cipta, pengetahuan, pengalaman dan keahlian, citra dan reputasi.

5. Arahan Manajemen untuk Keamanan Informasi SPBE
   a. Penyelenggaraan layanan SPBE harus dilakukan dengan menerapkan strategi dan kontrol-kontrol keamanan informasi SPBE sesuai ketentuan peraturan perundang-undangan.
   b. Seluruh sumber daya SPBE meliputi Data Digital, Aplikasi SPBE, Infrastruktur SPBE dan aset pendukung SPBE lainnya serta aset tak berwujud lainnya.
   c. Tim Koordinasi SPBE meningkatkan kepedulian (*awareness*), pengetahuan dan pemahaman tentang penerapan keamanan informasi SPBE bagi pegawai dan pihak di luar Kementerian/penyedia melalui pendidikan, pelatihan, dan sosialisasi secara berkala dengan memanfaatkan media komunikasi yang tersedia.
   d. Seluruh pegawai dan pihak di luar Kementerian termasuk pihak penyedia harus menjaga dan melindungi keamanan Data Digital, Aplikasi SPBE dan Infrastruktur SPBE yang dikelola dan/atau digunakan serta mematuhi kebijakan dan prosedur Keamanan SPBE yang telah ditetapkan.
   e. Pimpinan dan/atau penanggungjawab Unit Datin dari setiap Unit Organisasi harus mengkoordinasikan dan melaporkan seluruh kerawanan dan gangguan/insiden keamanan dalam penyelenggaraan layanan SPBE yang terjadi kepada pimpinan Unit Kerja yang bertanggung jawab terhadap keamanan untuk dapat segera dilakukan mitigasi risiko keamanan.
   f. Penggunaan aset TI dan perubahannya harus diidentifikasi, dianalisis dan dikendalikan risikonya dengan menerapkan kontrol-kontrol keamanan yang memadai sehingga potensi risiko yang mungkin terjadi dapat diminimalisir. Pelaksanaan pengukuran dan pengendalian risiko SPBE sesuai dengan ketentuan peraturan perundang-undangan.
   g. Setiap pengecualian terhadap pedoman ini dan kebijakan turunannya harus mendapatkan persetujuan dari Sekretaris Jenderal Kementerian.
   h. Kesesuaian terhadap pedoman ini akan dipantau secara berkala sekurang-kurangnya 2 (dua) tahun sekali dan setiap pelanggaran yang

terjadi dapat dikenakan sanksi atau tindakan disiplin sesuai dengan peraturan perundang-undangan.

6. Tanggung Jawab
   a. Penanggung jawab tertinggi penyelenggaraan manajemen keamanan informasi SPBE adalah Sekretaris Jenderal Kementerian selaku ketua tim pengarah pada tim koordinasi SPBE Kementerian.
   b. Penerapan manajemen keamanan informasi SPBE di tingkat Kementerian dikoordinasikan oleh Pusdatin.
   c. Penerapan manajemen keamanan informasi SPBE dilaksanakan Unit Kerja dikoordinasikan Unit Datin pada tingkat Unit Organisasi

7. Perencanaan Manajemen Keamanan Informasi SPBE
   a. Perencanaan manajemen keamanan informasi SPBE disusun dalam bentuk program kerja berdasarkan kategori risiko keamanan informasi SPBE dan target realisasi yang terukur sesuai dengan kebutuhan Kementerian.
   b. Perencanaan manajemen keamanan informasi SPBE paling sedikit mencakup:
      1) Edukasi kesadaran Keamanan SPBE, yang sekurang-kurangnya terdiri dari sosialisasi dan pelatihan Keamanan SPBE.
      2) Penilaian kerentanan Keamanan SPBE, yang mencakup inventarisasi seluruh aset SPBE, identifikasi kerentanan dan ancaman terhadap aset SPBE, dan mengukur tingkat risiko Keamanan SPBE.
      3) Peningkatan Keamanan SPBE, yang dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE dan rencana peningkatan Keamanan SPBE melalui penerapan standar teknis dan prosedur Keamanan SPBE dan pengujian fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.
      4) Penanganan insiden Keamanan SPBE dilaksanakan paling sedikit melalui identifikasi sumber serangan, analisis informasi yang berkaitan dengan insiden selanjutnya, prioritas penanganan insiden berdasarkan tingkat dampak yang terjadi, pendokumentasian bukti insiden yang terjadi, dan mitigasi dampak risiko Keamanan SPBE.
      5) Audit Keamanan SPBE, yang dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.
   c. Perencanaan manajemen keamanan informasi SPBE di tingkat Kementerian dilaksanakan setiap tahun dan dikoordinasikan oleh Pusdatin.
   d. Perencanaan manajemen keamanan informasi SPBE di tingkat Unit Organisasi dilaksanakan oleh Unit Datin serta dikoordinasikan dengan Pusdatin.

8. Dukungan Operasional Keamanan SPBE

   Tim koordinasi SPBE memastikan ketersediaan dukungan operasional Keamanan SPBE dalam bentuk kecukupan sumber daya manusia Keamanan SPBE dan anggaran operasional Keamanan SPBE:

a. Pemenuhan kebutuhan jabatan fungsional yang memiliki tugas dan fungsi terkait penerapan manajemen Keamanan SPBE.
b. Pemenuhan kecukupan sumber daya manusia melalui pelatihan dan/atau sertifikasi kompetensi serta bimbingan teknis mengenai standar Keamanan SPBE.
c. Kebutuhan anggaran operasional Keamanan SPBE disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

9. Evaluasi kinerja Keamanan SPBE

a. Evaluasi kinerja Keamanan SPBE dilakukan terhadap pelaksanaan Keamanan SPBE dengan cara:
    1) Mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE.
    2) Menetapkan indikator kinerja pada setiap area proses.
    3) Merumuskan dan menetapkan prosedur pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan.
    4) Menganalisi efektivitas pelaksanaan Keamanan SPBE dan
    5) Mendukung dan merealisasikan program audit Keamanan SPBE.
b. Evaluasi kinerja Keamanan SPBE dilakukan 1 (satu) tahun sekali dan dikoordinasikan oleh Pusdatin.

10. Perbaikan berkelanjutan Manajemen Keamanan Informasi SPBE

a. Perbaikan berkelanjutan Keamanan SPBE merupakan tindak lanjut dari hasil evaluasi kinerja dan dilaksanakan oleh Unit Datin.
b. Perbaikan berkelanjutan Keamanan SPBE dikoordinasikan oleh Pusdatin.
c. Perbaikan berkelanjutan dilakukan dengan:
    1) Mengatasi permasalahan dalam pelaksanaan Keamanan SPBE.
    2) Memperbaiki pelaksanaan Keamanan SPBE secara periodik.

11. Standar Teknis & Prosedur Keamanan Data dan Informasi

Standar teknis dan prosedur keamanan data dan informasi terdiri atas terpenuhinya aspek-aspek:

a. Kerahasiaan
b. Keutuhan
c. Kenirsangkalan
d. Ketersediaan
e. Otentikasi
f. Otorisasi; dan
g. Pencatatan.
    1) Pemenuhan aspek kerahasiaan dilaksanakan dengan standar dan prosedur yang ditetapkan sebagai berikut:
        a) Pemilik aset memiliki tanggung jawab untuk mengklasifikasikan aset informasi sesuai peraturan perundang-undangan dan melakukan peninjauan ulang terhadap pembatasan akses dan klasifikasi informasi secara berkala sekurang-kurangnya 1 (satu) tahun sekali.

b) Klasifikasi aset informasi terdiri atas Informasi Publik Terbuka dan Informasi Publik Yang Dikecualikan.

c) Informasi Publik Yang Dikecualikan dapat diklasifikasi secara lebih rinci berdasarkan kerahasiaan, risiko, atau klasifikasi lainnya sesuai dengan ketentuan peraturan perundang-undangan.

d) Dalam konteks Keamanan SPBE, metode dan penanganan klasifikasi aset informasi mengacu pada nilai informasi, sensitivitas/kekritisan informasi, tingkat kerahasiaan, dan tingkat kerawanannya bagi Kementerian.

e) Setiap dokumen yang di dalamnya terdapat informasi yang diklasifikasikan harus diberi label sesuai dengan klasifikasi dari informasi yang bersangkutan.

f) Pedoman Klasifikasi Aset Informasi

(1) Metode klasifikasi aset informasi mengacu hal berikut:

(a) Nilai informasi - berdasarkan dampak negatif terhadap Kementerian dalam menjalankan tugas dan fungsinya, reputasi, potensi risiko keamanan publik, potensi penggunaan oleh pihak lain yang mengancam ketersediaan sistem atau layanan yang diberikan Kementerian, dan/atau kriteria lain yang dinilai dalam penilaian risiko.

(b) Sensitivitas dan kekritisan informasi - berdasarkan risiko tertinggi dihitung untuk setiap item informasi selama penilaian risiko.

(c) Hukum dan kewajiban kontrak.

g) Peninjauan dan Klasifikasi Ulang

Pemilik aset informasi harus melakukan peninjauan dan klasifikasi ulang aset informasi setiap 1 (satu) tahun sekali.

h) Pelabelan Aset Informasi

Pelabelan Data Digital dilakukan dengan tahapan sebagai berikut:

(1) Setiap pegawai atau unit kerja yang membuat, menerima, atau mengolah Data Digital harus melakukan pelabelan dengan penentuan klasifikasi label berdasarkan tingkat kepentingan dan sensitivitas Data sesuai kebijakan klasifikasi informasi Kementerian, sebelum Data Digital tersebut disimpan atau dibagikan.

(2) Penentuan klasifikasi label sebagaimana dimaksud pada huruf a di atas meliputi:

(a) Rahasia;

(b) Internal/Terbatas;

(c) Terbuka.

(3) Pemberian Label pada Data Digital dengan Label dicantumkan pada:

(a) Nama file (contoh: Laporan_Anggaran_[Rahasia].xlsx),

(b) *Header*/*Footer* dokumen, atau
(c) Metadata sistem (jika menggunakan aplikasi manajemen dokumen).
(d) memastikan format label konsisten antar unit kerja.

(4) Setiap pegawai atau unit kerja harus memastikan pencatatan dan penyimpanan Data Digital berlabel sebagai berikut:
(a) Melakukan penyimpanan file berlabel di lokasi penyimpanan resmi (server unit, *cloud* Kementerian, atau DMS).
(b) Tidak melakukan penyimpanan data berlabel Rahasia atau Sangat Rahasia di perangkat pribadi.
(c) Data digital harus selalu dilakukan backup dan penerapan kontrol akses sesuai klaisifikasi label.

(5) Setiap pegawai atau unit kerja harus memastikan distribusi dan Penggunaan Data Digital berlabel sebagai berikut:
(a) Saat membagikan data, pastikan label tetap melekat pada file.
(b) Pegawai penerima wajib menghormati label tersebut dan tidak mengubah klasifikasi tanpa izin.
(c) Akses hanya diberikan kepada pihak yang sesuai dengan tingkat otorisasi label.

(6) Setiap pegawai atau unit kerja harus memastikan pemutakhiran Label (*Re-labelling*) Data Digital berlabel sebagai berikut:
(a) Jika terjadi perubahan status data (misalnya setelah dipublikasikan atau dikaji ulang), pegawai atau unit kerja wajib memperbarui label.
(b) Riwayat perubahan label dicatat untuk audit trail oleh unit kerja.

(7) Setiap pegawai atau unit kerja harus memastikan penghapusan atau Pemusnahan Data Data Digital berlabel sebagai berikut:
(a) Data berlabel yang sudah tidak diperlukan dihapus atau imusnahkan sesuai klasifikasi kerahasiaan dan kebijakan retensi data.
(b) Memastikan metode penghapusan aman (*secure delete*) untuk data rahasia.

**i)** Penerapan Enkripsi Dengan Sistem Kriptografi

Pemenuhan aspek kerahasiaan melalui penerapan enkripsi sesuai ketentuan peraturan perundang-undangan.

(1) Penerapan Enkripsi pada pengamanan data/informasi pada data/informasi dalam penyimpanan *(at rest)*, data/informasi yang sedang dipergunakan *(in-use)*,

maupun data/informasi yang dipertukarkan *(in-transit)* sesuai dengan klasifikasi dan pembatasan akses yang ditetapkan.

(2) Penerapan Enkripsi untuk melindungi kerahasiaan informasi milik Kementerian yang dikirimkan melalui jaringan komunikasi di luar Kementerian.

(3) Penerapan enkripsi dilakukan berdasarkan kajian risiko untuk menentukan tingkat perlindungan yang dibutuhkan.

j) Pengendalian Akses Terhadap Data/Informasi

(1) Hak akses terhadap aset-aset informasi harus diberikan sesuai dengan kebutuhan tugas dan fungsinya.

(2) Hak akses yang diberikan kepada pengguna tidak boleh melanggar prinsip pemisahan kewenangan dan tanggung jawab *(segregation of duty)*.

(3) Identitas pengguna beserta hak aksesnya hanya diberikan kepada pengguna setelah mendapat persetujuan dari pemilik data/informasi.

k) Pendaftaran pengguna dan Pemberian Hak Akses

Ketentuan pendaftaran akses pengguna:

(1) Identitas pengguna (*User ID*) melekat individu pegawai, dengan ketentuan:

(a) terintegrasi dengan sistem kepegawaian Kementerian

(b) dilarang menggunakan identitas pengguna bersama dengan pegawai/pengguna lain; dan

(c) penggunaan akun oleh pegawai/pengguna lain termasuk kategori pengguna tidak sah serta menjadi tanggung jawab pemilik akun.

(2) Identitas pengguna (*User ID)* masyarakat umum pengguna Aplikasi SPBE diatur oleh masing-masing Aplikasi SPBE.

(3) Identitas pengguna (*User ID*) harus unik, tidak diperbolehkan adanya Identitas pengguna yang sama.

(4) Identitas pengguna beserta hak aksesnya hanya diberikan kepada pengguna setelah mendapat persetujuan dari pemilik aset informasi.

(5) Hak akses yang diberikan kepada pengguna harus sesuai dengan kebutuhan tugas/operasional.

(6) Hak akses yang diberikan kepada pengguna tidak boleh melanggar prinsip pemisahan tanggung jawab (*segregation of duty*).

(7) Pengguna harus menyetujui pernyataan bahwa mereka memahami dan akan menaati ketentuan mengenai penggunaan Identitas pengguna.

(8) Daftar identitas pengguna untuk setiap aplikasi harus dimutakhirkan.

(9) Hak akses pengguna yang telah berganti jabatan harus segera disesuaikan atau dihapus.

(10) Identitas pengguna milik pegawai yang sudah berhenti bekerja dari Kementerian harus segera dinonaktifkan.

l) Pengelolaan Hak Akses Khusus

(1) Akses khusus seperti identitas pengguna *root, administrator, super user* atau akses VPN hanya diberikan dalam keadaan khusus untuk menjaga kelangsungan operasional atau tugas dan diberikan untuk jangka waktu sementara selama diperlukan berdasarkan penugasan yang diberikan oleh pejabat yang berwenang.

(2) Hak akses khusus dapat diberikan kepada unit organisasi yang mempunyai tugas menyelenggarakan pengawasan intern Kementerian selaku Aparat Pengawasan Intern Pemerintah (APIP) dalam penyelenggaraan tugasnya.

(3) Penggunaan hak akses khusus perlu memperhatikan beberapa hal berikut:

(a) Penggunaannya harus melalui proses otorisasi formal.

(b) Pemberian hak akses khusus hanya dilakukan dalam keadaan mendesak untuk mendukung kebutuhan tugas atau operasional.

(c) Penggunaan hak akses khusus harus memenuhi prinsip *"segregation of duties"* dan *"dual control".*

(d) Aktivitas yang dilakukan dengan menggunakan hak akses khusus harus dicatat, didokumentasikan, dan ditinjau.

m) Peninjauan Ulang Hak Akses Pengguna

(1) Peninjauan ulang terhadap hak akses dilaksanakan oleh pengelola sistem dan perangkat teknologi informasi paling sedikit 6 (enam) bulan sekali dalam rangka memastikan pengguna masih berhak terhadap akses yang diberikan, dan melakukan penghapusan pengguna yang sudah tidak aktif.

(2) Peninjauan ulang terhadap hak akses dilakukan pada saat pengguna yang bersangkutan mengalami perubahan tugas dan fungsi (promosi, demosi, atau mutasi) dilakukan oleh pimpinan yang bersangkutan, berkoordinasi dengan pengelola sistem/aplikasi atau pemilik data/informasi.

n) Pengelolaan Kata Sandi

Pengguna harus menerapkan kebiasaan keamanan yang baik ketika memilih dan menggunakan kata sandi:

(1) Kata sandi tidak boleh diketahui oleh orang lain, termasuk administrator.

(2) Kata sandi yang dibuat oleh pengguna tidak boleh

disebarkan melalui saluran apapun (melalui lisan, tertulis maupun secara elektronik dan lain-lain); kata sandi harus diganti apabila terdapat indikasi bahwa kata sandi atau sistem mungkin telah dibobol, dalam kasus tersebut, kejadian insiden keamanan ini harus segera dilaporkan.

(3) Kata sandi yang kuat harus digunakan, dengan cara sebagai berikut:
   (a) Menggunakan paling sedikit 12 (dua belas) karakter.
   (b) Menggunakan setidaknya satu karakter angka/numerik.
   (c) Menggunakan setidaknya satu karakter huruf besar dan huruf kecil.
   (d) Menggunakan setidaknya satu simbol.

(4) Kata sandi harus diganti secara periodik setiap 6 (enam) bulan dengan kata sandi yang berbeda.

(5) Kata sandi tidak boleh disimpan dalam sistem log-on otomatis kecuali yang sudah ditetapkan.

(6) Pengguna dapat memanfaatkan teknologi Password Manager atau Password Vault untuk memudahkan pengelolaan dan penggunaan kata sandi.
   (a) Penggunaan *Password Manager* atau *Password Vault* juga tetap harus mengedepankan kewaspadaan terhadap keamanan kata sandi yang dimiliki
   (b) penyedia *Password Manager*/*Password Vault* yang digunakan harus memiliki reputasi yang baik dan bukti kepatuhan (*compliance*) terhadap standar-standar keamanan dan pelindungan data privasi yang diakui secara internasional.

(7) Kata sandi harus dilengkapi otentikasi multi faktor pada sistem atau aplikasi penting dan strategis atau kritikal/sensitif sesuai dengan ketentuan peraturan perundang-undangan.

o) Pengendalian Akses Sistem Operasi dan Aplikasi

(1) Proses *log-on* ke dalam sistem operasi dan aplikasi harus dibuat untuk meminimalkan terjadinya akses tidak sah dengan tidak memunculkan informasi yang dapat membantu pengguna tidak sah untuk mengakses sistem operasi dan aplikasi.

(2) Kendali tambahan perlu dipertimbangkan untuk mengendalikan akses kedalam sistem operasi dan aplikasi yaitu:
   (a) Pada saat *log-on* terdapat peringatan bahwa komputer hanya dapat diakses oleh pengguna yang berhak.
   (b) Membatasi jumlah kesalahan dalam percobaan

*log-on* dan sistem harus melakukan hal-hal berikut apabila jumlah kesalahan maksimal telah dilampaui:

i. Mencatat setiap percobaan log-on baik yang gagal maupun berhasil.
ii. Memberikan jeda waktu sebelum log-on dapat dilakukan kembali atau menolak percobaan kembali setelah terjadi kesalahan dalam percobaan log-on.
iii. Memberikan pesan peringatan bahwa jumlah maksimal percobaan log-on telah terlampaui.

(c) Membatasi waktu minimal dan maksimal untuk proses *log-on*.
(d) Tidak menampilkan kata sandi yang dimasukkan pada saat *log-on*.
(e) Tidak mentransmisikan kata sandi yang tidak dienkripsi dalam jaringan.

(3) Identitas pengguna yang digunakan untuk mengakses sistem harus unik untuk setiap pengguna.

(4) Akses kedalam sistem harus diautentikasi sekurang-kurangnya dengan menggunakan kata sandi. Untuk aplikasi atau sistem elektronik penting atau strategis harus ditambahkan autentikasi lainnya (*multi-factor authentication*).

(5) Semua akses ke dalam sistem operasi beserta aktivitas yang dilakukan harus tercatat pada *log*.

(6) Sistem harus dikonfigurasi agar pengelolaan kata sandi oleh sistem dapat memenuhi beberapa persyaratan di bawah ini:
(a) Memungkinkan pengguna untuk memilih dan mengubah kata sandi sendiri.
(b) Memaksa pengguna menggunakan kata sandi yang kuat (tidak mudah ditebak atau diretas).
(c) Memastikan perubahan kata sandi secara berkala sesuai dengan ketentuan pengelolaan kata sandi.
(d) Memaksa pengguna mengganti kata sandi pada penggunaan pertama kali atau setiap kali memasuki masa kadaluwarsa.
(e) Mencegah penggunaan kembali kata sandi yang sudah pernah digunakan kecuali sudah melewati 2 (dua) kali siklus perubahan kata sandi yang diperbolehkan.
(f) Tidak menampikan kata sandi pada layar saat di-*input*.
(g) Penyimpanan dan pengiriman kata sandi harus menggunakan perlindungan khusus seperti enkripsi atau lainnya.

(7) Penggunaan *system utilities* harus dibatasi dengan proses autentikasi.
(8) *System utilities* harus terpisah dari aplikasi perangkat lunak.
(9) Terdapat *log* untuk semua penggunaan *system utilities.*
(10) *System utilities* yang tidak digunakan harus dihapus atau tidak diaktifkan.
(11) Pembatasan akses ke informasi dan fungsi aplikasi didokumentasikan.
(12) Pembatasan akses pada sistem aplikasi dan informasi dilakukan dengan pemberian hak akses baca *(read),* tulis *(write),* hapus *(delete)* dan eksekusi (*execute).*
(13) Akses pada direktori, folder, atau file yang diberikan kepada semua pengguna harus dihapus. Semua akses harus diberikan secara *granular* dan memenuhi prinsip *least privilledge.*
(14) Akses pegawai yang sudah tidak aktif bekerja di Kementerian masih dapat diberikan dalam jangka waktu 90 hari setelah tanggal efektif pemberhentian, atau ketentuan lain yang telah disepakati dengan pihak ketiga penyedia jasa terkait.

p) Pengendalian Akses ke Kode Sumber (*Source Code*)
(1) Akses atas kode sumber harus dikendalikan untuk mencegah akses oleh pihak yang tidak berwenang.
(2) Pengendalian akses ke kode sumber dilakukan dengan cara:
(a) Penyimpanan kode sumber tidak dilakukan pada sistem produksi.
(b) Akses terhadap kode sumber harus melalui proses otorisasi.
(c) Daftar kode sumber perlu dibuat, dipelihara dan dijaga.
(d) Setiap akses ke kode sumber perlu didokumentasikan, termasuk *log* untuk akses tersebut.
(e) Pemeliharaan kode sumber harus dilakukan melalui mekanisme Manajemen Perubahan.

2) Pemenuhan aspek keaslian data/informasi dilaksanakan dengan standar sebagai berikut:
a) Unit Kerja dan UPT yang menghasilkan data bersama-sama dengan Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi bertanggung jawab dalam verifikasi & validasi keaslian dan kebenaran data/informasi.
b) Unit Organisasi yang melaksanakan fungsi pengelolaan data, informasi, dan teknologi informasi berkoordinasi dengan Pusdatin dalam rangka penerapan *hash function*

dalam pemrosesan dan pengelolaan data/informasi sesuai dengan kebutuhan dan ketersediaan teknologi.

3) Pemenuhan aspek keutuhan data/informasi dilaksanakan dengan standar sebagai berikut:
   a) Perlindungan data dari modifikasi atau perubahan yang terjadi secara tidak sah dilakukan dengan penerapakan *hash function* dalam pemrosesan dan pengelolaan data/informasi.
   b) Penerapan tanda tangan elektronik hanya dilakukan melalui penyedia yang tersertifikasi sesuai dengan ketentuan peraturan perundang-undangan.
   c) Implementasi dan pengelolaan tanda tangan elektronik elektronik dikoordinasikan oleh Pusdatin.
4) Pemenuhan aspek aspek kenirsangkalan data/informasi dilaksanakan dengan standar sebagai berikut:
   a) Data/informasi sensitif harus dapat dipastikan penanggungjawabnya melalui penerapan tanda tangan elektronik
   b) Penerapan tanda tangan elektronik hanya dilakukan melalui penyedia yang tersertifikasi sesuai dengan ketentuan peraturan perundang-undangan.
   c) Implementasi dan pengelolaan tanda tangan elektronik elektronik dikoordinasikan oleh Pusdatin.
5) Pemenuhan aspek ketersediaan data/informasi dilaksanakan dengan standar sebagai berikut:
   a) Penerapan sistem pencadangan secara berkala sebagaimana diatur pada Bagian 16 Keamanan Operasional butir h. Pencadangan.
   b) Memastikan data/informasi dapat selalu diakses secara aman dan andal melalui penerapan manajemen dan standar teknis dan prosedur Keamanan SPBE secara utuh, termasuk namun tidak terbatas pada:
      (1) Pengelolaan *backup* data/informasi serta pengujian pemulihan sesuai ketentuan yang telah ditetapkan
      (2) Pengendalian akses terhadap data/informasi
      (3) Penerapan Keamanan Operasional
      (4) Penerapan Keamanan Aplikasi
      (5) Pengelolaan akses pihak di luar Kementerian
      (6) Penerapan Manajemen Insiden Keamanan SPBE
      (7) Penerapan Manajemen Keberlangsungan Layanan SPBE
      (8) Penerapan kepatuhan Keamanan SPBE
   c) Menerapkan sistem pemulihan dalam kerangka Manajemen Keberlangsungan Layanan SPBE sebagaimana diatur pada Bagian 19. Aspek Keamanan Informasi dari Manajemen Keberlangsungan Layanan SPBE

12. Standar Teknis & Prosedur Keamanan Aplikasi SPBE

Standar teknis dan prosedur keamanan Aplikasi diterapkan pada aplikasi berbasis *web* dan aplikasi berbasis *mobile*.

a. Persyaratan Keamanan Informasi

Persyaratan yang terkait keamanan informasi harus termasuk dalam persyaratan untuk sistem informasi baru atau pengembangan sistem informasi yang ada dan didokumentasikan. Persyaratan keamanan dimaksud termasuk namun tidak terbatas pada:

1) Pendefinisian hak akses dan prosedur autentikasinya.
2) Perlindungan data pengguna dan kata sandi atau data rahasia lainnya di dalam basis data harus dienkripsi atau disamarkan *(masking)*.
3) Merekam log transaksi (siapa melakukan apa dan kapan) di dalam *log* untuk keperluan pelacakan *(audit trail)*.

b. Lingkungan Pengembangan yang Aman

Pemilik sistem informasi harus menyiapkan lingkungan pengembangan yang aman mencakup seluruh daur hidup pengembangan sistem informasi serta berkoordinasi dengan Pusdatin.

c. Pengembangan oleh Alihdaya atau Pihak di luar Kementerian

Pemilik sistem informasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan.

d. Data Uji

1) Data yang digunakan dalam pengujian sistem harus dilindungi dari kemungkinan rusak, hilang, atau perubahan yang dilakukan tanpa izin.
2) Beberapa pengendalian berikut dapat dipertimbangkan untuk melindungi data produksi yang digunakan untuk pengujian sistem di lingkungan pengujian *(testing)* atau pengembangan *(development)*:
   a) Informasi pegawai/pribadi (seperti nama, alamat, nomor telepon dan sebagainya) agar disamarkan.
   b) Setelah proses pengujian selesai, dan data produksi yang bersangkutan tidak diperlukan lagi, maka harus segera dihapus.
   c) Penggunaan data produksi untuk pengujian harus didokumentasikan.

e. Keamanan Aplikasi Berbasis Web

1) Standar teknis keamanan aplikasi berbasis web mencakup:
   a) Autentikasi

      Terpenuhinya fungsi autentikasi dilakukan dengan prosedur:

      (1) Menggunakan manajemen kata sandi untuk proses autentikasi
      (2) Menerapkan verifikasi kata sandi pada sisi server
      (3) Mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi
      (4) Mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi
      (5) Mengatur mekanisme pemulihan kata sandi

(6) Menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi
(7) Menggunakan jalur komunikasi yang diamankan untuk proses autentikasi

b) Manajemen sesi
Terpenuhinya fungsi manajemen sesi dilakukan dengan prosedur:
(1) Menggunakan pengendali sesi untuk proses manajemen sesi
(2) Menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi
(3) Mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi
(4) Mengatur kondisi dan jangka waktu habis sesi
(5) Validasi dan pencantuman *session id*
(6) Pelindungan terhadap lokasi dan pengiriman *token* untuk sesi terautentikasi
(7) Pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna

c) Persyaratan kontrol akses
Terpenuhinya fungsi persyaratan kontrol akses dilakukan dengan prosedur:
(1) Menetapkan otorisasi pengguna untuk membatasi kontrol akses
(2) Mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi
(3) Mengatur antarmuka pada sisi administrator
(4) Mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.

d) Validasi input
Terpenuhinya fungsi validasi input dilakukan dengan prosedur:
(1) Menerapkan fungsi validasi input pada sisi server
(2) Menerapkan mekanisme penolakan input jika terjadi kesalahan validasi
(3) Memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input
(4) Melakukan validasi positif pada seluruh input
(5) Melakukan filter terhadap data yang tidak dipercaya
(6) Menggunakan fitur kode dinamis
(7) Melakukan pelindungan terhadap akses yang mengandung konten skrip
(8) Melakukan pelindungan dari serangan injeksi basis data.

e) Kriptografi pada verifikasi statis
Terpenuhinya fungsi kriptografi dilakukan dengan prosedur:
(1) Menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang- undangan

(2) Melakukan autentikasi data yang dienkripsi
(3) Menerapkan manajemen kunci kriptografi dan
(4) Membuat angka acak yang menggunakan generator angka acak kriptografi.

f) Penanganan eror dan pencatatan *log*
Terpenuhinya fungsi penanganan eror dan pencatatan log dilakukan dengan prosedur:
(1) Mengatur konten pesan yang ditampilkan ketika terjadi kesalahan
(2) Menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani
(3) Tidak mencantumkan informasi yang dikecualikan dalam pencatatan log
(4) Mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden
(5) Mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah
(6) Melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log
(7) Melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

g) Proteksi data
Terpenuhinya fungsi proteksi data dilakukan dengan prosedur:
(1) Melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan
(2) Melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi
(3) Melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan melakukan penentuan jumlah parameter
(4) Memastikan data disimpan dengan aman
(5) Menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna
(6) membersihkan memori setelah tidak diperlukan.

h) Keamanan komunikasi
Terpenuhinya fungsi keamanan komunikasi dilakukan dengan prosedur:
(1) Menggunakan komunikasi terenkripsi
(2) Mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna
(3) Mengatur jenis algoritma yang digunakan dan alat pengujiannya
(4) Mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

i) Pengendalian kode berbahaya
Terpenuhinya fungsi pengendalian kode berbahaya dilakukan

dengan prosedur:

(1) Menggunakan analisis kode dalam kontrol kode berbahaya
(2) Memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan
(3) Mengatur izin terkait fitur atau sensor terkait privasi
(4) Mengatur pelindungan integritas
(5) Mengatur mekanisme fitur pembaruan.

j) Logika bisnis

Terpenuhinya fungsi logika bisnis dilakukan dengan prosedur:

(1) Memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis
(2) Memastikan logika bisnis memiliki batasan dan validasi
(3) Memonitor aktivitas yang tidak biasa
(4) Membantu dalam kontrol antiotomatisasi
(5) memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

k) File

Terpenuhinya fungsi file dilakukan dengan prosedur:

(1) Mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah
(2) Melakukan validasi file sesuai dengan tipe konten yang diharapkan
(3) Melakukan pelindungan terhadap metadata input dan metadata file
(4) Melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya
(5) Melakukan konfigurasi server untuk mengunduh dan mengunggah file sesuai ekstensi yang ditentukan.

l) Keamanan API dan *web service*

Terpenuhinya fungsi keamanan API dan *web service* dilakukan dengan prosedur:

(1) Melakukan konfigurasi layanan web
(2) Memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan
(3) Membuat keputusan otorisasi
(4) Menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid
(5) Menggunakan validasi skema dan verifikasi sebelum menerima input
(6) Menggunakan metode pelindungan layanan berbasis web
(7) Menerapkan kontrol antiotomatisasi.

m) Keamanan konfigurasi

Terpenuhinya fungsi keamanan konfigurasi dilakukan dengan prosedur:

(1) Mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan
(2) Mendokumentasi, menyalin konfigurasi, dan semua dependensi
(3) Menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan
(4) Memvalidasi integritas aset jika aset aplikasi diakses secara eksternal
(5) Menggunakan respons aplikasi dan konten yang aman.

f. Keamanan Aplikasi Berbasis Mobile

Standar teknis keamanan aplikasi berbasis *mobile* terdiri atas terpenuhinya fungsi:

a) Penyimpanan data dan persyaratan privasi

Terpenuhinya fungsi penyimpanan data dan persyaratan privasi dilakukan dengan prosedur:

(1) Menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem
(2) Membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*
(3) Menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan
(4) Melindungi informasi yang dikecualikan saat terjadi *inter process communication*
(5) Melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

b) Kriptografi

Terpenuhinya fungsi kriptografi dilakukan dengan prosedur:

(1) Menghindari penggunaan kriptografi simetrik dengan *hardcoded key*
(2) Mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan
(3) Menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet
(4) Menghindari penggunaan kunci kriptografi yang sama
(5) Menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

c) Autentikasi dan manajemen sesi

Terpenuhinya fungsi autentikasi dan manajemen sesi dilakukan dengan prosedur:

(1). Menerapkan autentikasi pada remote endpoint terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh
(2). Menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi
(3). Memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi *stateless* berbasis

token

(4). Memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*

(5). Menerapkan pengaturan sandi pada *remote endpoint*

(6). Membatasi jumlah percobaan log in pada *remote endpoint*

(7). Menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*

(8). Melakukan otorisasi pada *remote endpoint*.

d) Komunikasi jaringan

Terpenuhinya fungsi komunikasi jaringan dilakukan dengan prosedur:

(1). Menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten

(2). Memverifikasi sertifikat *remote endpoint*.

e) Interaksi *platform*

Terpenuhinya fungsi interaksi platform dilakukan dengan prosedur:

(1) Memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan

(2) Melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna

(3) Menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*

(4) Menghindari penggunaan *JavaScript* dalam *WebView*

(5) Menggunakan protokol *hypertext transfer protocol* secure pada *WebView*.

(6) Mengimplementasikan penggunaan serialisasi API yang aman.

f) Kualitas kode dan pengaturan *build*

Terpenuhinya fungsi kualitas kode dan pengaturan build dilakukan dengan prosedur:

(1) Menandatangani aplikasi dengan sertifikat yang valid

(2) Memastikan aplikasi dalam mode rilis

(3) Menghapus simbol *debugging* dari *native binary*

(4) Menghapus kode *debugging* dan kode bantuan pengembang

(5) Mengidentifikasi kelemahan seluruh komponen *third party*

(6) Menentukan mekanisme penanganan eror

(7) Mengelola memori secara aman

(8) Mengaktifkan fitur keamanan yang tersedia

g) Ketahanan

Terpenuhinya fungsi ketahanan dilakukan dengan prosedur:

(1) Mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah

(2) Mendeteksi dan merespons *debugger*

(3) Mencegah *executable file* melakukan perubahan pada

sumber daya perangkat
(4) Mendeteksi dan merespons keberadaan perangkat *reverse engineering*
(5) Mencegah aplikasi berjalan dalam *emulator*
(6) Mendeteksi perubahan kode dan data di ruang memori
(7) Menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat
(8) Melindungi seluruh *file* dan *library* pada aplikasi
(9) Menerapkan *metode obfuscation*.

h) Distribusi Aplikasi *Mobile*
(1) Distribusi aplikasi *mobile* hanya dilakukan melalui akun resmi Kementerian yang dikelola Pusdatin pada *marketplace* aplikasi yang telah ditentukan.
(2) Tidak diperbolehkan mendistribusikan aplikasi *mobile* melalui layanan perpesanan dan/atau platfrom distribusi lain selain yang sudah ditentukan.

13. Standar Teknis & Prosedur Keamanan Sistem Penghubung Layanan

Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi:

a. Keamanan interoperabilitas data dan informasi
Terpenuhinya fungsi keamanan interoperabilitas data dan informasi dilakukan dengan prosedur:
1) menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik
2) menerapkan sistem enkripsi data
3) memastikan data dan informasi selalu dapat diakses sesuai otoritasnya
4) menerapkan sistem hash function pada file.

b. Kontrol sistem integrasi
Terpenuhinya fungsi kontrol sistem integrasi dilakukan dengan prosedur:
1) Menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi
2) Menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/internet protocol*
3) Menerapkan sistem anti *distributed denial of service*
4) Menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung
5) Menerapkan manajemen keamanan sesi
6) Menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan
7) Menerapkan validasi input
8) Menerapkan kriptografi pada verifikasi statis
9) Menerapkan sertifikat elektronik pada *web authentication*
10) Menerapkan penanganan eror dan pencatatan *log*

11) Menerapkan proteksi data dan jalur komunikasi
12) Menerapkan pendeteksi virus untuk memeriksa beberapa konten file
13) Menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus)
14) Memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

c. Kontrol perangkat integrator

Terpenuhinya fungsi kontrol perangkat integrator dilakukan dengan prosedur:

1) Menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini
2) Menggunakan anti virus dan *anti-spyware* terkini
3) Mengaktifkan fitur keamanan pada peramban web
4) Menerapkan *firewall* dan *host-based intrusion detection systems*
5) Mencegah instalasi perangkat lunak yang belum terverifikasi
6) Mencegah akses terhadap situs yang tidak sah; dan
7) Mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

d. Keamanan API dan web service

Terpenuhinya fungsi keamanan API dan *web service* dilakukan dengan prosedur:

1) Menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API
2) Menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*
3) Menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid
4) Melindungi layanan *web RESTful* yang menggunakan *cookie* dari *cross-site request forgery*
5) Memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

e. Keamanan migrasi data

Terpenuhinya fungsi keamanan migrasi data dilakukan dengan prosedur:

1) Memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem
2) Memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal
3) Mendokumentasikan format sistem basis data lama secara rinci
4) Melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data
5) Menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data
6) Melakukan validasi data ketika proses migrasi data selesai.

14. Standar Teknis & Prosedur Keamanan Jaringan Intra

Standar teknis keamanan Jaringan Intra terdiri atas terpenuhinya:

a. Aspek administrasi keamanan Jaringan Intra
   Terpenuhinya aspek administrasi keamanan Jaringan Intra dilakukan dengan prosedur:
   1) menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra
   2) mengidentifikasi seluruh aset infrastruktur jaringan
   3) menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra
   4) membuat laporan pengawasan keamanan jaringan secara periodik.
b. Kontrol akses dan autentikasi
   Terpenuhinya kontrol akses dan dilakukan dengan prosedur:
   1) Menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah
   2) Menggunakan autentikasi untuk mengakses Jaringan Intra
   3) Menerapkan pembatasan akses dalam Jaringan Intra
   4) mematikan atau membatasi *protocol, port*, dan layanan yang tidak digunakan
   5) Menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya
   6) Menerapkan fungsi honeypot untuk menganalisis celah keamanan berdasarkan jenis serangan
   7) Menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan
   8) Memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra
      a) Menerapkan *secure endpoints*
      b) Memblokir layanan yang tidak dikenal
      c) Menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra
      d) Menerapkan server perantara saat *client* mengakses server database dalam rangka pemeliharaan.
c. Persyaratan perangkat dan aplikasi keamanan Jaringan Intra
   Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra dilakukan dengan prosedur:
   1) Menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*
   2) Menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan
   3) Menggunakan perangkat *firewall*
   4) Menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*
   5) Menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas
   6) Menerapkan kontrol *update patching* pada infrastruktur Jaringan

Intra dan sistem komputer
7) Menggunakan perangkat *web application firewall*
8) Menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi
9) Memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas
10) Menerapkan sertifikat elektronik.

d. Kontrol keamanan *gateway*
Terpenuhinya kontrol keamanan *gateway* dilakukan dengan prosedur:
1) Menerapkan *content filtering*
2) Menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra
3) Menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*
4) Memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik
5) Melaksanakan manajemen *traffic gateway*
6) Memastikan *port* tidak dibuka secara *default*.

e. Kontrol keamanan access point pada jaringan nirkabel
Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel dilakukan dengan prosedur:
1) Menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini
2) Menerapkan *media access control* pada *address filtering*
3) Menerapkan *dedicated service set identifier*
4) Menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan
5) Menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah
6) Menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan
7) Melakukan *patching firmware* secara rutin.

f. Kontrol konfigurasi access point pada jaringan nirkabel
Terpenuhinya kontrol konfigurasi access point pada jaringan nirkabel dilakukan dengan prosedur:
1) Menggunakan kata sandi yang kuat
2) Menggunakan protokol *model authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi administrator *access point*
3) Memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan
4) Mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel
5) Menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

15. Keamanan Sumber Daya Manusia

a. Sebelum Menjadi Pegawai
   1) Verifikasi atas calon pegawai dilakukan dengan mengacu kepada prosedur rekrutmen yang diatur dalam kebijakan dan prosedur kepegawaian yang berlaku.
   2) Sebagai syarat tanggung jawab keamanan informasi, setiap calon pegawai harus menandatangani dokumen Pernyataan Menjaga Rahasia yang merupakan bagian dari perjanjian kerja/pakta integritas.

b. Selama Menjadi Pegawai
   1) Semua pegawai dan pihak di luar Kementerian/penyedia di Kementerian harus mendapatkan pengetahuan tentang keamanan informasi.
   2) Pegawai dan pihak di luar Kementerian/penyedia terkait yang terlibat dalam pengelolaan keamanan informasi harus mendapatkan dan/atau memiliki pendidikan dan pelatihan yang memadai.
   3) Program pelatihan dan kepedulian (*awareness*) harus dilakukan secara berkala sekurang-kurangnya 1 (satu) tahun sekali.
   4) Harus ada proses pendisiplinan yang resmi dan dikomunikasikan atau disosialisasikan terhadap penindakan pegawai yang melakukan pelanggaran keamanan informasi SPBE sesuai dengan ketentuan peraturan perundangan-undangan.

c. Penghentian dan Perubahan Kepegawaian
   1) Pengembalian aset milik Kementerian oleh pegawai yang berhenti bekerja sesuai prosedur yang berlaku.
   2) Aset yang harus dikembalikan adalah aset yang menjadi tanggung jawab pegawai selama bertugas.
   3) Pencabutan hak akses terhadap sistem informasi yang dimiliki pegawai dan pihak di luar Kementerian lainnya diatur sesuai dengan Pengendalian Hak Akses.

16. Keamanan Operasional

a. Prosedur dan Tanggung Jawab Operasional

   Prosedur operasional sistem informasi harus dibuat meliputi sekurang-kurangnya:
   1) *Job Scheduling*;
   2) Pencadangan dan *restore*;
   3) Penanganan dan eskalasi permasalahan;
   4) Prosedur *restart* dan *recovery* sistem;
   5) Pendistribusian output; dan
   6) Pengaktifan dan pengelolaan log.

b. Manajemen Perubahan
   1) Seluruh perubahan terhadap fasilitas pengolah dan pengelolaan informasi harus dikendalikan dan didokumentasi untuk menjamin perubahan pada sistem informasi terkelola dan terkendali dengan benar.

2) Setiap perubahan yang dilakukan pada sistem operasional atau sistem produksi harus dilakukan dengan cara berikut:
    a) Pengajuan perubahan dapat diajukan oleh Unit Organisasi/Unit Kerja/UPT;
    b) Perubahan harus disetujui oleh pemilik sistem/aplikasi;
    c) Perubahan harus diimplementasikan oleh personil yang berwenang;
    d) Pemilik sistem/aplikasi bertanggung jawab untuk memeriksa bahwa perubahan yang dilakukan telah memenuhi permintaan perubahan;
    e) Pemilik Sistem/Aplikasi bertanggung jawab untuk menguji dan memeriksa stabilitas sistem. Sistem tidak boleh dipasang ke dalam sistem produksi sebelum pengujian secara keseluruhan benar-benar dilakukan.
3) Konfigurasi sistem pengembangan, pengujian dan produksi harus dipelihara dan dimutakhirkan atas setiap perubahan yang dilakukan.
4) Implementasi perubahan harus dilakukan sosialisasi kepada pihak terkait.
5) Penerapan manajemen perubahan harus memastikan aspek keamanan operasional dan dilakukan sesuai dengan peraturan perundang-undangan.

c. Prinsip Pemisahan Tugas dan Tanggung Jawab (Segregation of Duties) dan Dual Control
1) Pemisahan tugas dan tanggung jawab dilaksanakan untuk mencegah adanya pihak atau personil yang dapat melakukan kesalahan atau pelanggaran baik disengaja atau tidak disengaja, tanpa diketahui atau tanpa terdeteksi.
2) Harus ada pemisahan tugas dan tanggung jawab diantara fungsi yang disebut di bawah ini:
    a) Pengembangan Teknologi Informasi
    b) Operasional Teknologi Informasi
    c) Strategi, Perencanaan, dan Keamanan Teknologi Informasi
3) Aktifitas yang memiliki risiko tinggi harus dikerjakan dan diperiksa oleh personil yang berbeda.
4) Sistem dan prosedur harus dirancang untuk tidak memungkinkannya seorang personil dapat menjalankan suatu proses atau transaksi yang berisiko tinggi, tanpa adanya kendali dari personil lainnya.
5) Prinsip *dual control* harus dilaksanakan untuk memastikan terlaksananya fungsi *check and balance*. *Dual Control* harus dilaksanakan untuk fungsi-fungsi berikut ini:
    a) Pengelolaan Konfigurasi Perangkat Keamanan Informasi SPBE;
    b) Pengelolaan Akses dan Otentikasi, terutama terkait dengan hak akses khusus~~;~~
    c) Perubahan parameter pada Sistem Operasi;
    d) Pemeliharaan *firewall rules*;

e) Pelaksanaan Prosedur Darurat (*emergency procedure*);
f) Pengelolaan kunci kriptografi;
g) Fungsi-fungsi lainnya yang dapat menimbulkan kerugian apabila dilaksanakan dengan cara yang salah atau dilakukan secara tidak sah.

6) Jika terjadi kendala dalam menjalankan prinsip *dual control* maka harus dilakukan bentuk pengawasan lain *(compensating control)* seperti proses *monitoring*, audit, *log review,* dan pengawasan dari pimpinan di atasnya.

d. Pemisahan Aktivitas Pengembangan, Pengujian, dan Operasional
1) Fasilitas pengembangan aplikasi dan pengujian aplikasi harus berada pada sistem yang terpisah dari lingkungan produksi.
2) Lingkungan pengujian aplikasi harus memiliki kesamaan konfigurasi dan spesifikasi dengan lingkungan produksi aplikasi.
3) Prosedur pemindahan aplikasi dari pengembangan ke produksi harus ditetapkan secara formal.
4) *Compiler, editor*, dan *tools* pengembangan lain tidak diperbolehkan untuk digunakan pada sistem produksi kecuali saat *emergency*.
5) Konfigurasi sistem pengembangan, pengujian dan produksi harus dipelihara.

e. Pengelolaan Layanan Pihak di Luar Kementerian
1) Keamanan Akses Pihak dari Luar Kementerian
a) Sebelum memberikan akses kepada mitra dan pihak di luar kementerian, pemilik sistem wajib mengevaluasi risiko-risiko yang mungkin muncul sehubungan dengan pemberian akses dan menerapkan kontrol yang memadai untuk mengurangi dampak atau mencegah terjadinya risiko-risiko tersebut.
b) Evaluasi dilakukan dengan memperhatikan aspek-aspek berikut:
(1). Jenis akses yang diperlukan baik akses fisik maupun akses non fisik (misalnya akses jaringan, basis data dan sistem informasi)
(2). Alasan kebutuhan akses, seperti untuk memberi dukungan teknis, audit keamanan informasi, atau pengembangan aplikasi/sistem informasi.
(3). Pengendalian risiko pemberian akses pada pihak dari luar Kementerian dilakukan antara lain melalui klausul-klausul dalam kontrak dan melalui Pernyataan Menjaga Kerahasiaan (*Non-Disclosure Agreement*).
c) Pada saat kontrak berakhir atau terjadi penghentian kontrak, hak akses bagi pegawai/personil dari pihak di luar Kementerian harus dihapus sesuai dengan kebijakan yang berlaku.

2) Kontrak
Dalam perjanjian kontrak dengan pihak di luar Kementerian dicantumkan antara lain:
a) Kewajiban pihak di luar Kementerian mematuhi kebijakan keamanan informasi SPBE sesuai ketentuan peraturan perundang-undangan.

b) Persetujuan untuk turut melindungi keamanan sumber daya informasi Kementerian terkait dengan akses yang diberikan.
c) Jenis akses yang diberikan dan tata cara penggunaan akses tersebut.
d) Identitas pegawai/personil pihak di luar Kementerian yang menggunakan akses tersebut.
e) Pembatasan lokasi dan waktu penggunaan akses.
f) Persetujuan atas hak pantau dan pengawasan yang dilakukan pemilik sistem terhadap penggunaan akses.
g) Setiap aset yang dipinjamkan kepada pihak di luar Kementerian wajib dikembalikan saat perjanjian kerja berakhir.
h) Sanksi atas pelanggaran terhadap kontrak diberlakukan sesuai dengan ketentuan peraturan perundang-undangan.

3) Layanan oleh pihak di luar Kementerian harus dipastikan memenuhi tingkat layanan yang sesuai dengan *Service Level Agreement* (SLA) dan persyaratan keamanan informasi yang sudah ditentukan.
4) Pihak di luar Kementerian harus memiliki kemampuan dan perencanaan untuk menghadapi kegagalan atau bencana, sehingga pihak di luar Kementerian yang bersangkutan dapat memelihara tingkat layanan yang sudah disepakati.
5) Pengawasan terhadap kinerja pihak di luar Kementerian harus dilakukan untuk menjamin:
   a) Kinerja atau *service level* pihak di luar Kementerian sudah sesuai dengan perjanjian.
   b) Kebenaran laporan layanan tahunan yang disusun oleh pihak di luar Kementerian.
   c) Bila terjadi insiden keamanan informasi, maka dapat dilakukan penanganan sesuai dengan prosedur penanganan insiden keamanan informasi yang berlaku.
6) Pemilik informasi/sistem harus memiliki kontrol atas keamanan dan kerahasiaan informasi yang diakses, diproses atau dikelola oleh pihak di luar Kementerian.
7) Pemilik informasi/sistem harus memastikan pihak di luar Kementerian melaksanakan pengamanan informasi, identifikasi atas kelemahan sistem informasi dan penanganan insiden keamanan informasi.
8) Perubahan sistem pada layanan TI oleh pihak di luar Kementerian harus ditinjau ulang dan disetujui oleh pemilik informasi/sistem sebelum perubahan diimplementasikan.

f. Perencanaan dan Pemantauan Kapasitas
1) Semua aktivitas atau proses pada sistem informasi baik yang sedang berjalan maupun yang akan diimplementasikan harus memperhitungkan kebutuhan kapasitas sumber daya sistem.
2) Proses monitoring sistem dan *system tuning* harus dilakukan untuk memastikan dan meningkatkan kinerja, ketersediaan dan efisiensi sistem.
3) Perkiraan/proyeksi kebutuhan kapasitas sistem untuk masa yang

akan datang harus diperhitungkan dengan memperhatikan tren pertumbuhan penggunaan sumber daya sistem dan perkembangan kebutuhan.

4) Perencanaan kapasitas harus dimutakhirkan agar sesuai dengan perubahan yang ada.
5) Semua sistem baru atau sistem hasil pengembangan harus melalui proses pengujian formal sebelum digunakan.
6) Proses pengujian sistem agar mengacu pada Pedoman Manajemen Layanan SPBE Bagian 3. Pengoperasian Aplikasi SPBE

g. Perlindungan Malware dan Pengelolaan Patch
   1) Penerapan sistem deteksi dan respon ancaman keamanan wajib dilakukan pada server atau perangkat Kementerian yang mengelola sistem elektronik penting dan strategis, termasuk didalamnya pengelolaan *patch* untuk meminimalkan potensi celah keamanan.
   2) Sebelum diterapkan di lingkungan operasional, risiko penerapan *security patch* perlu dikaji dan dilakukan pengujian di fasilitas pengembangan (*development*) yang tersedia untuk memastikan agar penerapannya tidak menyebabkan gangguan terhadap operasional layanan TI.
   3) Penerapan *security patch* harus dilakukan dengan mengikuti prosedur manajemen perubahan.
   4) Bukti penerapan *security patch* harus didokumentasikan dan disimpan.

h. Pencadangan *(Backup)*
   1) Pencadangan informasi/data dan perangkat lunak yang penting atau strategis harus dibuat untuk dapat memenuhi kebutuhan pemulihan bila terjadi permasalahan atau bencana.
   2) Media pencadangan harus ditempatkan pada lokasi yang aman dan terlindung dari pengaruh lingkungan. Kriteria pengamanan media pencadangan mengacu pada ketentuan yang berlaku jika telah terdapat ketentuan yang mengatur terkait media pencadangan, atau standar yang berlaku secara nasional atau internasional.
   3) Frekuensi pencadangan disesuaikan dengan kebutuhan.
   4) Masa retensi dari pencadangan informasi perlu ditentukan berdasarkan kebutuhan, sesuai dengan ketentuan peraturan perundang-undangan, dan kewajiban kontrak.
   5) Media pencadangan yang disimpan di luar lokasi utama (off-site) harus disimpan pada lokasi dengan jarak yang aman dari lokasi pencadangan di kantor (on-site backup).
   6) Media pencadangan harus dilengkapi dengan label.
   7) Hasil pelaksanaan pencadangan harus didokumentasikan.
   8) Media pencadangan data harus diuji secara berkala. Pengujian media pencadangan data dapat dilakukan pada saat pengujian Rencana Pemulihan Bencana atau pada saat adanya permintaan pemulihan (restore) data.
   9) Pencadangan (*backup*) dan pemulihan (*restore*)
      a) Pemilik/Pengelola aplikasi/sistem bertanggung jawab dalam pencadangan data, aplikasi, dan konfigurasi Infrastruktur SPBE

berkoordinasi dengan Unit Datin;

b) Pusdatin berkoordinasi dengan Pemilik/Pengelola aplikasi/sistem untuk pencadangan data, aplikasi, dan konfigurasi Infrastruktur SPBE di tingkat Kementerian.

10) Pengujian atas pencadangan data, aplikasi, dan konfigurasi infrastruktur menjadi tanggung Pemilik/Penangung jawab aplikasi/sistem.

i. Pencatatan *(Logging)* dan Pemantauan

1) Akses terhadap log harus dibatasi hanya bagi personil dengan tugas dan tanggung-jawab memerlukan akses ke dalam log.
2) Semua log harus dilindungi dari upaya perubahan, penghapusan, atau penambahan.
3) Kapasitas penyimpanan dokumen log harus dijaga agar tidak menyebabkan terhentinya sistem logging untuk mencatat events atau overwriting pada event log sebelumnya.
4) Log dan log reports dapat mengandung informasi yang bersifat rahasia sehingga harus diklasifikasikan sebagai informasi rahasia dan ditangani sesuai prosedur penanganan informasi rahasia.
5) *Logging* yang sudah ditetapkan untuk diaktifkan, tidak boleh dinonaktifkan.
6) *Log monitoring* sistem harus ditempatkan pada jaringan yang terpisah (segregated) dan dilindungi oleh firewall.
7) *Log* dari server, firewall, dan router harus dicadangkan ke suatu internal log server atau media penyimpan data yang aman dari upaya modifikasi.
8) Masa retensi penyimpanan log harus ditetapkan sesuai dengan kebutuhan dan ketentuan peraturan perundang- undangan.
9) Pencatatan log untuk mencatat aktivitas administrator dan aktivitas operasional pada server atau perangkat sistem lainnya harus meliputi:
   a) Identitas dari administrator atau operator yang digunakan.
   b) Tanggal dan jam dari kejadian (event) yang berhasil maupun yang gagal.
   c) Informasi mengenai kejadian (event) atau kegagalan yang terjadi.
10) Administrator dilarang menghapus atau menonaktifkan log dari aktivitas siapapun termasuk diri sendiri.
11) Setiap kegagalan atau kesalahan pada sistem harus dicatat, dilaporkan dan dianalisis serta dilakukan tindakan perbaikan yang sesuai.
12) *Error logging* pada sistem/aplikasi bila tersedia, harus selalu diaktifkan.
13) *Logging* dapat berpengaruh terhadap kinerja sistem, oleh sebab itu pengaktifan log harus dilakukan hanya pada error/fault log tertentu sesuai kebutuhan dan dilakukan oleh personil yang kompeten.
14) Jam (clock) dari semua server, komputer, dan perangkat pemroses informasi lainnya harus disinkronisasi sehingga menunjukkan

waktu yang sama dengan menggunakan *Network Time Protocol* (NTP).

15) Pemilik atau pengelola aplikasi bertanggungjawab memastikan pencatatan log diaktifkan dan dikelola sesuai ketentuan dan pelaksanaannya dikoordinasikan dengan Unit Datin.

j. Kendali Perangkat Lunak Operasional

Perangkat lunak berlisensi atau open source yang digunakan untuk kegiatan operasional harus disetujui oleh Pusdatin dalam rangka memastikan integritas sistem operasional.

k. Pengelolaan Kerentanan Teknis

1) Pengelolaan kerentanan teknis dilakukan melalui penilaian kerentanan (*Vulnerability Assessment* - VA) atau Uji penetrasi (*Penetration Testing* - PT).
2) Penilaian kerentanan (*Vulnerability Assessment* - VA) yang dimaksud pada butir 1) merupakan proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat risiko pada kerentanan keamanan informasi pada suatu sistem (yaitu jaringan komputer, sistem, aplikasi, atau bagian lain dari sistem TI) yang dilakukan dengan menggunakan alat pemindaian (*scanning tools*) yang bersifat pasif tanpa simulasi penyerangan.
3) Uji penetrasi (*Penetration Testing* - PT) yang dimaksud pada butir 1) merupakan proses penilaian kerentanan keamanan informasi pada suatu sistem (yaitu jaringan komputer, sistem, aplikasi, atau bagian lain dari sistem TI) yang dilakukan dengan yang bersifat aktif berupa simulasi penyerangan.
4) *Vulnerability Assessment* atau *Penetration Testing* (VA/PT) pada sistem operasi, jaringan, basis data maupun aplikasi harus dilakukan secara berkala sekurang-kurangnya dilakukan setiap 1 (satu) tahun sekali.
5) Pelaksanaan VA/PT:
    a. VA/PT untuk aplikasi tingkat kementerian dilaksanakan oleh Pusdatin.
    b. VA/PT untuk aplikasi Teknis & Aplikasi Pendukung yang hanya dipergunakan oleh Unit Organisasi/Unit Kerja/UPT tertentu dilaksanakan oleh Unit Datin.
    c. Unit datin dapat mengajukan permintaan VA/PT ke Pusdatin.
6) Unit Organisasi/Unit Kerja/UPT dapat mengajukan kebutuhan VA/PT kepada Pusdatin melalui Unit Datin.
7) Unit Organisasi/Unit Kerja/UPT harus menindaklanjuti hasil VA/PT dan melaporkan kepada Pusdatin melalui Unit Datin.
8) Setiap personel yang melaksanakan VA/PT harus memiliki standar kualifikasi sesuai ketentuan peraturan perundang-undangan (salah satunya Peraturan BSSN No 14 Tahun 2024).

17. Manajemen Insiden Keamanan Informasi

a. *Service Desk*, sebagai *Single Point of Contact* (SPOC), merupakan kontak

pertama dari pengguna jika terjadi insiden/gangguan dengan layanan teknologi informasi. Aktivitas penanganan insiden keamanan informasi adalah:

1) Pencatatan insiden *(incident logging)*
2) Pengkategorisasian insiden *(incident categorization)*
3) Prioritas insiden *(incident prioritization)*
4) Diagnosa Awal *(initial diagnosis)*.
5) Eskalasi insiden *(incident escalation)*
6) Investigasi *(investigation and diagnosis)*
7) Resolusi *(resolution dan recovery)*
8) Penutup *(incident closure)*
9) Pelaporan penanganan insiden

b. Penanganan insiden/gangguan harus dilaksanakan segera mungkin agar dapat mengembalikan fungsi layanan operasional TI, dengan melaksanakan solusi baik yang bersifat sementara maupun permanen, agar kelangsungan layanan operasional Kementerian tetap berjalan
c. Penanganan insiden/gangguan harus dilakukan berdasarkan klasifikasi prioritas. Prioritas penanganan dilihat dari sisi urgensi dan dampaknya terhadap operasional dan layanan Kementerian.
d. Pelaksanaan penanganan insiden/gangguan keamanan informasi dilakukan oleh Tim Tanggap Insiden Kementerian.
e. Penanganan insiden/gangguan keamanan informasi dapat melibatkan fungsi organisasi lainnya yang dibutuhkan, seperti bidang hukum, bidang komunikasi publik, dan/atau fungsi terkait lainnya.

18. Aspek Keamanan Informasi dari Manajemen Keberlangsungan Layanan SPBE

Aspek keamanan informasi harus diintegrasikan ke dalam sistem manajemen keberlangsungan Layanan SPBE Kementerian dengan:

a. Pemilik sistem/aplikasi melakukan pencadangan secara teratur terhadap data dan aplikasi yang digunakan dalam pelayanan teknologi informasi.
b. Dalam hal terjadi ketidaktersediaan Layanan SPBE maka layanan terhadap pengguna dan publik dapat dilakukan secara manual jika memungkinkan sesuai dengan ketentuan peraturan perundang undangan.
c. Setiap Unit Organisasi menyusun Rencana Keberlangsungan Bisnis (*Business Continuity Plan* atau BCP) dan Rencana Pemulihan Bencana (*Disaster Recovery Plan* atau DRP) berkoordinasi dengan Pusdatin.
d. Rencana Pemulihan Bencana dilakukan dengan mempertimbangkan hal-hal sebagai berikut:
   1) Pelaksanaan identifikasi layanan dan aset-aset informasi yang penting dan strategis.
   2) identifikasi kejadian-kejadian yang menyebabkan gangguan terhadap aset informasi yang vital dan sensitif.
   3) Tindak lanjut atas hasil-hasil kajian risiko keamanan informasi.
e. Untuk menjamin agar Rencana Keberlangsungan Bisnis (*Business Continuity Plan* atau BCP) dan Rencana Pemulihan Bencana (*Disaster*

*Recovery Plan* atau DRP) SPBE tetap relevan dan efektif, maka harus dilakukan pengujian secara rutin oleh Unit Organisasi dan berkoordinasi dengan Pusdatin, minimal sekali setahun.

f. Hasil pengujian Rencana Keberlangsungan Bisnis (*Business Continuity Plan* atau BCP) dan Rencana Pemulihan Bencana (*Disaster Recovery Plan* atau DRP) dan tindakan perbaikan yang perlu dilakukan harus dilaporkan ke Kepala Pusdatin dan pimpinan Unit Kerja Penyelenggara Layanan SPBE.

19. Kepatuhan

a. Identifikasi Terhadap Hukum dan Peraturan Perundang-undangan
   1) Seluruh pengguna sistem informasi milik Kementerian termasuk pihak di luar Kementerian terkait lainnya harus mematuhi kebijakan keamanan informasi Kementerian, dan mentaati ketentuan hukum dan peraturan perundang undangan yang terkait serta perjanjian tentang lisensi, termasuk persyaratan-persyaratan kontrak yang telah disepakati.
   2) Semua ketentuan tersebut harus dikomunikasikan kepada seluruh Unit Organisasi, Unit Kerja, dan UPT di Kementerian yang terkait agar mengetahui kewajibannya untuk mematuhi semua ketentuan tersebut.

b. Hak Atas Kekayaan Intelektual
   1) Seluruh Unit Organisasi, Unit Kerja, dan UPT di Kementerian harus mematuhi ketentuan perlindungan hak atas kekayaan intelektual (HAKI) yang mencakup penggunaan perangkat lunak berlisensi.
   2) Daftar aset yang memiliki hak atas kekayaan intelektual harus dipelihara dengan baik.
   3) Setiap penemuan, kegiatan, atau gagasan-gagasan praktis yang diperoleh pegawai, pihak di luar Kementerian, dan mitra kerja selama bekerja atau dibiayai Kementerian adalah menjadi hak milik Kementerian.
   4) Lisensi perangkat lunak yang disediakan Kementerian tidak boleh digunakan atau dipasang di peralatan komputer selain milik Kementerian. Pengecualian atas ketentuan ini, yaitu jika pada kondisi tertentu harus dilakukan pemasangan lisensi pada perangkat selain milik Kementerian harus mendapat persetujuan dari Pimpinan Unit Kerja pegawai yang bersangkutan.

c. Perlindungan Terhadap Dokumen Kementerian
   1) Dokumen penting milik Kementerian dan/atau yang digunakan dan dihasilkan oleh sistem informasi atau aset informasi yang dikelola Kementerian seperti basis data, audit log, dan transaction log harus dilindungi dari kehilangan, kerusakan, atau penyalahgunaan.
   2) Prosedur mengenai retensi, penyimpanan, penanganan, dan pemusnahan dokumen Kementerian sesuai dengan ketentuan peraturan perundang-undangan.

d. Perlindungan Data dan Informasi Pribadi

Seluruh Unit Organisasi, Unit Kerja, dan UPT di Kementerian harus melindungi kepemilikan dan kerahasiaan data pribadi pegawai, mitra kerja dan pihak di luar Kementerian yang bekerja sama dengan Kementerian. Data pribadi tersebut hanya boleh digunakan untuk kepentingan yang diperbolehkan oleh ketentuan peraturan perundang-undangan.

e. Kepatuhan Terhadap Kebijakan dan Pedoman Keamanan Informasi

1) Untuk menjamin dipatuhinya kebijakan dan pedoman keamanan informasi oleh seluruh pegawai, Unit Organisasi, Unit Kerja, dan UPT di Kementerian harus melakukan hal-hal sebagai berikut :
   a) Mengkomunikasikan kebijakan dan pedoman keamanan informasi.
   b) Meningkatkan pengetahuan dan keterampilan pegawai dalam pengelolaan keamanan informasi sesuai dengan bidang tugasnya.
   c) Memeriksa dan mengevaluasi tingkat kepatuhan atau kesesuaian pegawai terhadap pelaksanaan kebijakan ini secara berkala.
2) Setiap ketidakpatuhan terhadap kebijakan dan pedoman keamanan informasi, kepala Unit Organisasi, Unit Kerja, dan/atau UPT harus :
   a) Menentukan penyebab dari ketidakpatuhan.
   b) Menentukan dan menerapkan tindakan perbaikan yang sesuai.
   c) Menentukan tindakan yang diperlukan untuk mencegah terjadinya kembali ketidakpatuhan tersebut.
   d) Meninjau efektifitas tindakan perbaikan yang telah dilakukan.
3) Pemeriksaan kesesuaian teknis, seperti tes penetrasi (penetration test), pemindaian jaringan (*scanning*), atau teknik pencarian kelemahan keamanan informasi lainnya (*vulnerability assessment*), akan dilakukan secara berkala oleh pegawai yang kompeten baik dari internal Kementerian ataupun menggunakan jasa ahli independen dari luar Kementerian sesuai dengan spesifikasi atau standar yang berlaku.
4) Rencana pemeriksaan kesesuaian teknis harus didokumentasikan, dikomunikasikan, dan disetujui pimpinan Pusdatin.
5) Setiap pemeriksaan teknis harus dicatat dan dilaporkan sebagai masukan bagi evaluasi manajemen keamanan informasi.

f. Audit TIK

Pelaksanaan audit, penggunaan audit *tools*, dokumentasi dan pelaporan Audit TIK mengacu pada standar dan tata cara sesuai dengan peraturan perundang-undangan.

g. Hal-hal yang belum diatur pada pedoman ini dapat mengacu pada standar nasional indonesia atau standar internasional yang relevan dengan memperhatikan keselarasan dengan pedoman ini. Aspek-aspek yang lebih rinci dalam pelaksanaan pedoman ini dapat diatur dengan petunjuk teknis yang ditetapkan kemudian.

C. MANAJEMEN DATA

1. Ketentuan Umum
   a. Pelaksanaan manajemen data SPBE di Kementerian Pekerjaan Umum (PU) dilaksanakan melalui perangkat penyelenggara Satu Data Kementerian dan Bidang Data Pusdatin sesuai tugas dan kewenangannya.
   b. Manajemen data SPBE bertujuan untuk menjamin terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi, dan pengendalian pembangunan nasional sektor pekerjaan umum.
   c. Sasaran manajemen data SPBE dilaksanakan:
      1) Mampu memahami kebutuhan data.
      2) Mendapatkan, menyimpan, melindungi, dan memastikan integritas data.
      3) Meningkatkan kualitas data secara terus menerus; dan
      4) Memaksimalkan penggunaan data dan hasil yang efektif dari penggunaan data.
   d. Manajemen data SPBE dilaksanakan melalui serangkaian proses pengelolaan:
      1) Arsitektur data.
      2) Data induk dan data referensi.
      3) Basis data; dan
      4) Kualitas data.
2. Manajemen Arsitektur Data
   a. Manajemen arsitektur data terdiri atas komponen utama berupa spesifikasi data dan ketentuan data.
   b. Spesifikasi data terdiri atas format dan struktur baku untuk Data Induk dan Data Referensi.
   c. Ketentuan data mencakup tata cara perencanaan, pengumpulan, pemeriksaan dan penyebarluasan spesifikasi data.
   d. Manajemen arsitektur data disusun untuk:
      1) Menyediakan data yang berkualitas tinggi.
      2) Mengidentifikasi dan mendefinisikan kebutuhan data; dan
      3) Merancang struktur dan rencana untuk memenuhi kebutuhan data saat ini dan kebutuhan data jangka panjang.
   e. Kegiatan manajemen arsitektur data meliputi:
      1) Penyusunan dan penetapan.
      2) Penyebarluasan; dan
      3) Reviu.
   f. Koordinator Forum Satu Data Kementerian mengoordinasikan penyusunan arsitektur data SPBE bersama Pusdatin dan Unit Datin.
   g. Pusdatin melaksanakan penyusunan arsitektur data SPBE tingkat Kementerian bersama dengan Koordinator Produsen Data dan Produsen Data.
   h. Unit Datin melaksanakan penyusunan arsitektur data SPBE Tingkat Unit Organisasi bersama Koordinator Produsen Data dan Produsen Data dengan mengacu pada arsitektur data SPBE Kementerian.
   i. Koordinator Forum Satu Data Kementerian menyampaikan arsitektur

data SPBE yang telah dibuat kepada Ketua Dewan Pengarah Tim Koordinator SPBE.

j. Ketua Dewan Pengarah Tim Koordinator SPBE menyampaikan arsitektur data SPBE Kementerian kepada Menteri.
k. Untuk menyelaraskan rancangan arsitektur data SPBE tingkat Kementerian dengan arsitektur data SPBE nasional, Kementerian berkoordinasi dengan Kementerian Perencanaan Pembangunan Nasional/ Badan Perencanaan Pembangunan Nasional.
l. Arsitektur data SPBE tingkat Kementerian yang telah diselaraskan dengan arsitektur data SPBE nasional dan ditetapkan oleh Menteri.
m. Walidata menyebarluaskan arsitektur data SPBE melalui Portal Satu Data Kementerian.
n. Koordinator Forum Satu Data Kementerian mengoordinasikan reviu terhadap arsitektur data SPBE dalam Forum Satu Data Kementerian.
o. Arsitektur data SPBE Kementerian dilakukan reviu pada paruh waktu pelaksanaan arsitektur SPBE Kementerian dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

3. Manajemen Data Induk dan Data Referensi
   a. Manajemen Data Induk dan Data Referensi dilaksanakan untuk menyediakan data yang:
      1) Sesuai struktur dan format baku yang ditentukan.
      2) Dapat dijadikan acuan untuk menghasilkan data yang akurat, mutakhir dan dapat dibagipakaikan; dan
      3) Menghindari duplikasi.
   b. Kegiatan manajemen Data Induk dan Data Referensi meliputi:
      1) Perencanaan.
      2) Pengumpulan.
      3) Pemeriksaan.
      4) penyebarluasan; dan
      5) Pembaruan.
   c. Perencanaan Data Induk Dan data Referensi dilaksanakan oleh Forum Satu Data Kementerian berdasarkan:
      1) Daftar data.
      2) Usulan Pembina Data; dan
      3) Arahan Dewan Pengarah Satu Data Kementerian.
   d. Pengumpulan Data Induk dan Data Referensi dilakukan oleh Walidata dalam Forum Satu Data Kementerian.
   e. Pemeriksaan Data Induk dan Data Referensi dilakukan oleh Forum Satu Data Kementerian untuk memastikan:
      1) Kesesuaian dengan struktur dan format baku.
      2) Kesesuaian dengan Daftar Data tahun berikutnya; dan
      3) Tidak terjadi duplikasi.
   f. Data Induk dan Data Referensi disepakati dalam Forum Satu Data Kementerian.
   g. Data Induk dan Data Referensi yang telah disepakati disampaikan oleh Koordinator Forum Satu Data Kementerian kepada Dewan Pengarah Satu Data Kementerian.
   h. Menteri menetapkan Data Induk dan Data Referensi yang telah

disepakati.

i. Penyebarluasan Data Induk dan Data Referensi dilakukan oleh Walidata melalui Portal Satu Data Kementerian.

j. Pembaruan Data Induk dan Data Referensi diperbarui sesuai kebutuhan.

k. Kegiatan Manajemen Data Induk dan Data Referensi dilaksanakan selaras dengan perumusan dan penyepakatan Kode Referensi sebagaimana dimaksud dalam ketentuan peraturan perundang-undangan.

4. Manajemen Basis Data
   a. Manajemen basis data dilaksanakan untuk menyediakan basis data yang:
      1) Menjamin penyimpanan data yang akurat, mutakhir dan dapat dibagipakaikan di Pusat Data Nasional.
      2) Menjamin ketersediaan akses data yang terus menerus; dan
      3) Menjaga keamanan data dari akses yang tidak sesuai ketentuan peraturan perundang-undangan.
   b. Kegiatan manajemen basis data mencakup:
      1) Mendefinisikan kebutuhan Walidata dan Produsen Data untuk basis data.
      2) Mengelola basis data di Pusat Data Nasional.
      3) Melakukan pemeriksaan basis data untuk kesesuaian dengan prinsip Satu Data Indonesia.
      4) Menyebarluaskan basis data melalui Portal Satu Data Kementerian.
      5) Membuat cadangan dan distribusi basis data; dan
      6) Merencanakan dan mengelola pembaruan basis data.
   c. Ketentuan penyimpanan data di Pusat Data Nasional diatur oleh Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan digital.
5. Manajemen Kualitas Data
   a. Manajemen kualitas data dilaksanakan untuk menjamin data yang dihasilkan Produsen Data yang:
      1) Memenuhi prinsip Satu Data Indonesia; dan
      2) Diperbarui sesuai dengan jadwal pemutakhiran data.
   b. Kegiatan Manajemen Kualitas Data melingkupi kegiatan untuk:
      1) Mengembangkan dan mempromosikan kesadaran kualitas Data.
      2) Menentukan persyaratan kualitas Data.
      3) Menetapkan profil, analisis, dan nilai kualitas Data.
      4) Menentukan matriks kualitas Data.
      5) Menentukan aturan bisnis kualitas Data.
      6) Menguji dan memvalidasi persyaratan kualitas Data.
      7) Menetapkan dan mengevaluasi tingkat layanan kualitas Data; dan
      8) Mengukur dan memantau kualitas Data secara berkelanjutan.
   c. Kegiatan manajemen kualitas data dilaksanakan melalui tahapan:
      1) Perencanaan.
      2) Pemeriksaan; dan
      3) Penilaian.

d. Perencanaan kualitas data dilaksanakan oleh Forum Satu Data Kementerian.
e. Perencanaan kualitas data dilakukan dengan menyepakati daftar data, data prioritas dan jadwal pemutakhiran data.
f. Pemeriksaan kualitas data dilaksanakan dengan memeriksa kesesuaian data dengan:
   1) Prinsip Satu Data Indonesia; dan
   2) Ketepatan jadwal pemutakhiran data.
g. Pemeriksaan kualitas data dalam daftar data dan data prioritas dilaksanakan oleh Koordinator Produsen Data dan Produsen Data.
h. Koordinator Produsen Data melaporkan hasil pemerikasaan kualitas data kepada Walidata.
i. Penilaian kualitas data dilaksanakan untuk menilai kinerja Koordinator Produsen Data dan Produsen Data dalam pengelolaan data, sebagai bagian dari pemantauan dan evaluasi terhadap SPBE.

6. Data dan informasi statistik
   a. Ketentuan Umum
      Sesuai dengan batang tubuh pada Peraturan Menteri ini dan Bab Ketentuan Umum dalam lampiran ini.
   b. Daftar Data yang telah ditentukan dalam Forum Satu Data Kementerian
      Sesuai dengan daftar data yang ditentukan oleh Forum Satu Data Kementerian berdasarkan kesepakatan Forum Satu Data Indonesia dan dapat berkoordinasi dengan Kementerian/Lembaga yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional, jika diperlukan.
   c. Standar Data Statistik dan Metadata Statistik
      1) Standar Data Statistik
         Berdasarkan Peraturan Badan Pusat Statistik Peraturan Badan Pusat Statistik Nomor 4 Tahun 2020 tentang Petunjuk Teknis Standar Data Statistik dan Peraturan Badan Pusat Statistik Nomor 10 Tahun 2023 tentang Standar Data Statistik dan pembaruannya, Standar Data Statistik yang selanjutnya disebut SDS adalah konsep, definisi, klasifikasi, ukuran, dan satuan yang dibakukan untuk menghasilkan data statistik yang terstandar. Berikut penjelasan setiap komponen yang meliputi konsep, definisi, klasifikasi, ukuran, dan satuan:
         a) Konsep merupakan ide atau gagasan yang mendasari data dan menjelaskan lebih lanjut mengenai suatu Data Statistik yang terstandar.
         b) Konsep merupakan ide atau gagasan yang mendasari data dan menjelaskan lebih lanjut mengenai suatu Data Statistik yang terstandar.
         c) Klasifikasi merupakan penggolongan data secara sistematis ke dalam kelompok atau kategori berdasarkan kriteria yang telah ditetapkan oleh Badan atau dibakukan secara luas. Klasifikasi dapat dibedakan menjadi klasifikasi isian dan

klasifikasi penyajian. Klasifikasi isian digunakan pada data kategorik sedangkan klasifikasi penyajian digunakan pada data numerik.

d) Ukuran merupakan unit yang digunakan dalam pengukuran jumlah, kadar atau cakupan.

e) Satuan merupakan besaran tertentu dalam data yang digunakan sebagai standar untuk mengukur atau menakar sebuah keseluruhan.

Contoh pengisian SDS:

Tabel 1 Contoh pengisian standar data statistik

| Kode SDS | Nama Data | Konsep | Definisi | Klasifikasi Penyajian | Klasifikasi Isian | Ukuran | Satuan |
|---|---|---|---|---|---|---|---|
| 31010034<br><br>(Diisi oleh Pembina Data Statistik) | Jumlah Bendungan | Bendungan | Jumlah unit bangunan yang berupa urukan tanah, urukan batu, beton, dan/atau pasangan batu yang dibangun selain untuk menahan dan menampung air, dapat pula dibangun untuk menahan dan menampung limbah tambang (tailing), atau menampung lumpur sehingga terbentuk waduk. | Wilayah | - | Total | unit |
| 24410049<br><br>(Diisi oleh Pembina Data Statistik) | Panjang Jembatan | Jembatan | Panjang jembatan dalam ruas jalan nasional. | Wilayah | - | Panjang | meter |

2) Metadata Statistik

Metadata Statistik adalah informasi dalam bentuk struktur dan format yang baku untuk menggambarkan data, menjelaskan data, serta memudahkan pencarian, penggunaan, dan pengelolaan informasi data. Sesuai dengan amanat Peraturan Presiden Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, struktur dan format baku metadata statistik ditetapkan oleh pembina data statistik. Oleh karena itu, pengaturan mengenai metadata statistik merujuk pada peraturan yang ditetapkan oleh Badan Pusat Statistik (BPS), yaitu Peraturan Badan Pusat Statistik Nomor 5 Tahun 2020 tentang Petunjuk Teknis Metadata Statistik.

Struktur Metadata Statistik berdasarkan Peraturan BPS tersebut mencakup tiga komponen utama, yaitu Metadata Kegiatan Statistik (MS-Keg), Metadata Variabel (MS-Var), dan Metadata Indikator (MS-Ind) sebagaimana disajikan pada Tabel 2 berikut:

Tabel 2 Struktur metadata statistik

| MS-Keg | MS-Var | MS-Ind |
|---|---|---|
| • Identitas Kegiatan Statistik<br>• Blok I. Penyelenggara<br>• Blok II. Penanggung Jawab<br>• Blok III. Perencanaan dan Persiapan<br>• Blok IV. Desain Kegiatan<br>• Blok V. Desain Sampel<br>• Blok VI. Pengumpulan Data<br>• Blok VII. Pengolahan dan Analisis<br>• Blok VIII. Diseminasi Hasil | • Nama Variabel<br>• Alias<br>• Konsep<br>• Definisi<br>• Referensi Pemilihan<br>• Referensi Waktu<br>• Tipe Data<br>• Klasifikasi Isian<br>• Kalimat Pertanyaan<br>• Apakah Variabel dapat Diakses Umum | • Nama Indikator<br>• Konsep<br>• Definisi<br>• Interpretasi<br>• Metode/Rumus Penghitungan<br>• Ukuran<br>• Satuan<br>• Klarifikasi<br>• Publikasi Indikator Pembangun<br>• Nama Indikator Pembangun<br>• Kode Kegiatan Penghasil Variabel Pembangun<br>• Nama Variabel Pembangun<br>• Level Estimasi<br>• Dapat Diakses Umum |

a) Metadata Statistik Kegiatan (MS-Keg) adalah sekumpulan atribut informasi yang memberikan gambaran/dokumentasi dari penyelenggaraan kegiatan statistik.

Format pengisian Metadata Kegiatan:

Tabel 3 Format pengisian metadata

| Pertanyaan | Jawaban | Klasifikasi Isian | Keterangan |
|---|---|---|---|
| HALAMAN AWAL | | | |
| Apakah mendapatkan Rekomendasi kegiatan statistik dari BPS? | | (Ya/Tidak) | Pilih Salah Satu |
| Judul Kegiatan: | | | Harus terisi |
| Cara Pengumpulan Data: | | (Pencacahan Lengkap / Survei / Kompilasi Produk Administrasi) | Pilih Salah Satu |
| Sektor Kegiatan: | | Pertanian dan Perikanan, Demografi dan Kependudukan, Pembangunan, Proyeksi Ekonomi, Pendidikan dan Pelatihan, Lingkungan, Keuangan, Globalisasi, Kesehatan, Industri dan Jasa, Teknologi Informasi dan Komunikasi, Perdagangan Internasional dan Neraca Perdagangan, Ketenagakerjaan, Neraca Nasional, Indikator Ekonomi Bulanan, Produktivitas, Harga dan Paritas Daya Beli, Sektor Publik, Perpajakan, dan Regulasi Pasar, Perwilayahan dan Perkotaan, Ilmu Pengetahuan dan Hak Paten, Perlindungan Sosial dan Kesejahteraan, Transportasi | Pilih Salah Satu |
| | | | |
| BLOK I (Penyelenggara) | | | |
| 1.1. Instansi Penyelenggara: | | | Harus terisi |
| 1.2. Alamat Lengkap Instansi Penyelenggara: | | | Harus terisi |
| Telepon: | | | Harus terisi |
| Faksmile: | | | Harus terisi |
| Email: | | | Harus terisi |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| BLOK II (Penanggung Jawab) | | | | | |
| 2.1. Unit Eselon Penanggung Jawab | | | | | |
| Eselon 1: | | | | | Harus terisi |
| Eselon 2: | | | | | Harus terisi |
| 2.2. Penanggung Jawab Teknis (setingkat Eselon 3) | | | | | |
| Nama: | | | | | Harus terisi |
| Jabatan: | | | | | Harus terisi |
| Alamat: | | | | | Harus terisi |
| Telepon: | | | | | Harus terisi |
| Faksmile: | | | | | |
| Email: | | | | | Harus terisi |
| | | | | | |
| BLOK III (Perencanaan dan Persiapan) | | | | | |
| 3.1. Latar Belakang Kegiatan: | | | | | Harus terisi |
| 3.2. Tujuan Kegiatan: | | | | | Harus terisi |
| 3.3. Rencana Jadwal Kegiatan: | | | | | Diisi lengkap tangal, bulan dan tahun |
| Kegiatan | Tanggal Mulai | Tanggal Selesai | | | |
| A. Perencanaan | | | | | |
| 1. Perencanaan Kegiatan | | | | | |
| 2. Desain | | | | | |
| B. Pengumpulan | | | | | |
| 3. Pengumpulan Data | | | | | |
| C. Pemeriksaan | | | | | |
| 4. Pengolahan Data | | | | | |
| D. Penyebarluasan | | | | | |
| 5. Analisis | | | | | |
| 6. Diseminasi Hasil | | | | | |
| 7. Evaluasi | | | | | |
| 3.4. Variabel (Karakteristik) yang Dikumpulkan: | | | | | |
| Nama Variabel (Karakteristik) | Konsep | | Definsi | Referensi Waktu (Periode Enumerasi) | Diisi sesuai dengan variabel yang ada |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| BLOK IV (Desain Kegiatan) | | | | | |
| 4.1. Kegiatan Ini Dilakukan: | | (Hanya Sekali/Berulang) | | | Pilih Salah Satu |
| 4.2. Frekuensi Penyelenggaraan | | (Harian, Mingguan, Bulanan, Triwulan, Semesteran, Tahunan, Lebih dari 2 Tahun) | | | Jika 4.1 dilakukan berulang, silahkan pilih salah satu, jika tidak dikosongi |
| 4.3. Tipe Pengumpulan Data: | | (*Longitudinal Panel, Longitudinal Cross Sectional, Cross Sectional*) | | | Pilih Salah Satu |

| | | | |
|---|---|---|---|
| 4.4. Cakupan Wilayah Pengumpulan Data: | | (Seluruh Wilayah Indonesia, Sebagian Wilayah Indonesia) | Pilih Salah Satu |
| 4.5. Wilayah | | | Diisi jika 4.5 Sebagian Wilayah Indonesia |
| 4.6. Metode Pengumpulan Data: | | (Wawancara, Mengisi Kuesioner Sendiri, Pengamatan, Pengumpulan Data Sekunder, Lainnya) | Pilih Salah Satu |
| 4.7. Sarana Pengumpulan Data: | | *Paper-assisted Personal Interviewing* (PAPI*), Computer-assisted Personal Interviewing* (CAPI), *Computer-assisted Telephones Interviewing* (CATI), *Computer Aided Web Interviewing* (CAWI), Mail, Lainnya | Pilih Salah Satu |
| 4.8. Unit Pengumpulan Data: | | Individu, Rumah Tangga, Usaha/Perusahaan, Lainnya | Pilih Salah Satu |
| | | | |
| BLOK V (Desain Sampel) | | | |
| 5.1. Jenis Rancangan Sampel: | | *Single Stage* Atau *Phase/Multi Stage* Atau *Phase* | Diisi jika pengumpulan data (di halaman awal) menggunakan Survei |
| 5.2. Metode Pemilihan Sampel Tahap Terakhir: | | Sampel Probabilitas/Sampel Nonprobabilitas | |
| 5.3. Metode Yang Digunakan: | | (*Simple Random Sampling, Systematic Random Sampling, Stratified Random Sampling, Cluster Sampling, Probabilty Proportional to Size Sampling*) | |
| 5.4. Kerangka Sampel Tahap Terakhir: | | (*List Frame, Area Frame*) | |
| 5.5. Fraksi Sampel Keseluruhan: | | | |
| 5.6. Nilai Perkiraan Sampling Error Variabel Utama: | | | |
| 5.7. Unit Sampel: | | | |
| 5.8. Unit Observasi: | | | |
| | | | |
| BLOK VI (Pengumpulan Data) | | | |
| 6.1. Apakah Melakukan Uji Coba (Pilot Survey)? | | (Ya/Tidak) | Pilih Salah Satu |
| 6.2. Metode Pemeriksaan Kualitas Pengumpulan Data: | | (Kunjungan Kembali, Supervisi, *Task Force*, Lainnya) | Pilih Satu atau lebih |
| 6.3. Apakah Melakukan Penyesuaian Nonrespon? | | (Ya/Tidak) | Pilih Salah Satu |
| 6.4. Petugas Pengumpulan Data: | | (Staf Instansi Penyelenggara, Mitra Atau Tenaga Kontrak, Staf Instansi Penyelenggara Dan Mitra Atau Tenaga Kontrak) | Pilih Salah Satu |
| 6.5. Persyaratan Pendidikan Terendah Petugas Pengumpulan Data: | | (Kurang Dari Atau Sama Dengan SMP, SMA atau SMK, Diploma I Atau II Atau III, Diploma IV Atau S1 Atau S2 Atau S3) | Pilih Salah Satu |
| 6.6. Jumlah Petugas: | | | |
| Supervisor/penyelia/pengawas | | | Jumlah Orang |
| Pengumpul data/enumerator | | | Jumlah Orang |

| | | | |
|---|---|---|---|
| 6.7. Apakah Melakukan Pelatihan Petugas? | | (Ya/Tidak) | Pilih Salah Satu |
| | | | |
| BLOK VII (Pengolahan dan Analisis) | | | |
| 7.1. Tahapan Pengolahan Data: | | | |
| Penyuntingan (Editing) | | (Ya/Tidak) | Pilih Salah Satu |
| Penyandian (Coding) | | (Ya/Tidak) | Pilih Salah Satu |
| Data Entry | | (Ya/Tidak) | Pilih Salah Satu |
| Penyahihan (Validasi) | | (Ya/Tidak) | Pilih Salah Satu |
| 7.2. Metode Analisis: | | Deskriptif, Inferensia, Deskriptif dan Inferensia | Pilih Salah Satu |
| 7.3. Unit Analisis: | | (Individu, Rumah Tangga, Usaha/Perusahaan, Lainnya) | Pilih Satu atau lebih |
| 7.4. Tingkat Penyajian Hasil Analisis: | | (Nasional, Provinsi, Kabupaten/Kota, Lainnya) | Pilih Satu atau lebih |
| | | | |
| BLOK VIII (Diseminasi Hasil) | | | |
| 8.1. Produk Kegiatan yang Tersedia untuk Umum | | | |
| Tercetak (Hardcopy) | | (Ya/Tidak) | Pilih Salah Satu |
| Digital (Softcopy) | | (Ya/Tidak) | Pilih Salah Satu |
| Data Mikro | | (Ya/Tidak) | Pilih Salah Satu |

b) Metadata Statistik Variabel (MS-Var) adalah sekumpulan atribut informasi yang memberikan gambaran/dokumentasi dari penyusunan suatu variabel dalam kegiatan statistik.

Contoh pengisian MS-Var:

Tabel 4 Pengisian MS-Var

| No. | Nama Variabel | Alias | Konsep | Definisi | Referensi Pemilihan | Referensi Waktu | Tipe Data | Klasifikasi Isian | Aturan Validasi | Kalimat Pertanyaan | Kolom (2) Dapat Diakses Umum? Ya (1) Tidak (2) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) |
| Contoh 1 | Nama Instalasi Pengolahan Lumpur Tinja (IPLT) | Nama IPLT | Instalasi Pengolahan Lumpur Tinja | Instalasi pengolahan air limbah yang dirancang hanya menerima dan mengolah lumpur tinja yang berasal dari subsistem pengolahan setempat suatu wilayah. | Permen PUPR No. 4 Tahun 2017 tentang Penyelenggaraan Sistem Pengelolaan Air Limbah Domestik | Saat pengumpulan data | String | - | - | Nama IPLT | Ya |
| Contoh 2 | Nama Badan Usaha | Nama BUJK | Badan Usaha Jasa Konstruksi | Badan usaha yang berbentuk | Permen PUPR 8 | Tahunan | String | - | Wajib diisi | Nama BUJK | Ya |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Jasa Konstruksi | | | badan hukum atau tidak berbadan hukum yang kegiatan usahanya bergerak di bidang jasa konstruksi. | Tahun 2022 | | | | | | |

c) Metadata Statistik Indikator (MS-Ind) adalah sekumpulan atribut informasi yang memberikan gambaran/dokumentasi dasar terbentuknya suatu indikator.

Contoh pengisian MS-Ind:

Tabel 5 Pengisian MS-Ind

| No. | Nama Indikator | Konsep | Definisi | Interpretasi | Metode/Rumus Penghitungan | Ukuran | Satuan | Klasifikasi Penyajian |
|---|---|---|---|---|---|---|---|---|
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) |
| Contoh 1 | Jumlah Sertifikat Kompetensi Kerja Konstruksi | Sertifikat Kompetensi Kerja Konstruksi | Sertifikat kompetensi kerja konstruksi berfungsi untuk menunjukkan jumlah kepemilikan sertifikat kompeten kerja | Menggambarkan jumlah kawasan yang dilakukan program Pengembangan Kawasan Lingkungan | Menjumlahkan sertifikat kerja konstruksi yag diterbitkan $\sum_{n=0}^{\infty} SKK$ | Total | Sertifikat | Wilayah |
| Contoh 2 | Panjang Jalan Tol Konstruksi | Jalan Tol | Panjang jalan bebas hambatan dalam proses konstruksi yang merupakan bagian sistem jaringan jalan dan sebagai jalan nasional yang penggunanya diwajibkan membayar | Menggambarkan panjang jalan tol dalam proses pembangunan dalam suatu wilayah | Menjumlah panjang jalan tol dalam proses konstruksi $\sum_{n=0}^{\infty} panjangjalantolkonstruksi$ | Panjang | Kilometer | Wilayah |

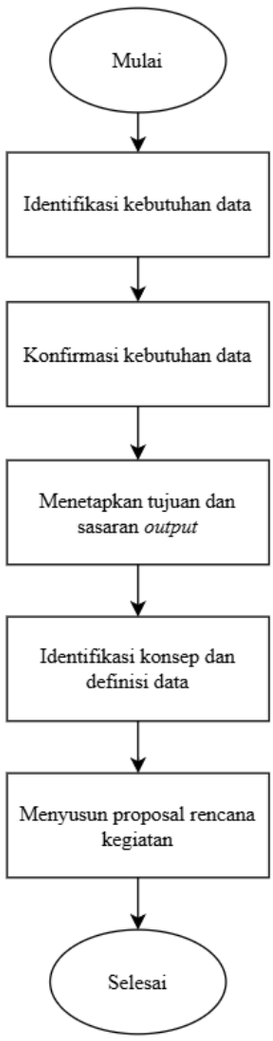
| Apakah Kolom (2) Indikator Komposit? Ya (1) Tidak (2) | Jika Kolom (10) berkode 1 | | Jika Kolom (10) berkode 2 | | | Level Estimasi | Apakah Kolom (2) Dapat Diakses Umum? Ya (1) Tidak (2) |
|---|---|---|---|---|---|---|---|
| | Indikator Pembangun | | Variabel Pembangun | | | | |
| | Publikasi Ketersediaan | Nama | Kegiatan Penghasil | Kode Keg. (diisi petugas) | Nama | | |
| (10) | (11) | (12) | (13) | (14) | (15) | (16) | (17) |
| Tidak | - | - | Kompilasi Data Kepemilikan | | Sertifikat Kerja Konstruksi | Provinsi | Ya |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | Sertifikat Kompeten Kerja | | | | |
| Tidak | | | Kompilasi Data Jaringan Jalan Tol Konstruksi | | Panjang jalan tol konstruksi | Provinsi | Ya |

d. Jadwal pemutakhiran data atau rilis data
   Sesuai dengan kebijakan Forum Satu Data Kementerian dan produsen data.
e. Prosedur Pengelolaan Data dan Informasi Statistik
   Prosedur ini disusun untuk memberikan pedoman bagi pemangku kepentingan dalam penyelenggaraan pengelolaan kegiatan statistik. Setiap aktivitas dalam prosedur pengelolaan data dan informasi statistik dilakukan dengan mengacu pada *Generic Statistical Business Process Model* (GSBPM) yang telah disesuaikan. Penyelenggaraan kegiatan statistik yang mengikuti GSBPM untuk menjamin dan menghasilkan data yang berkualitas dan bermutu.

   Ruang lingkup prosedur pengelolaan data dan informasi statistik terdiri atas beberapa rangkaian kerja yaitu identifikasi kebutuhan kegiatan statistik, perancangan kegiatan statistik, pengumpulan data statistik, pengolahan dan analisis data statistik, serta diseminasi dan evaluasi data statistik. Selain itu, prosedur pengendalian mutu bertujuan untuk memastikan setiap tahapan dapat memberikan hasil yang berkualitas.

1) Prosedur Identifikasi Kebutuhan Kegiatan Statistik



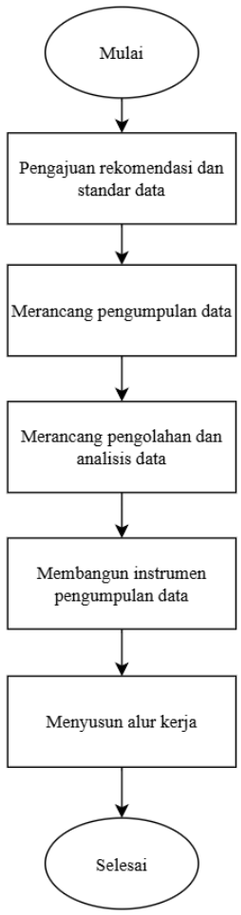

Gambar 1 Prosedur identifikasi kebutuhan kegiatan statistik

Tabel 6 Prosedur identifikasi kebutuhan kegiatan statistik

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Identifikasi kebutuhan data | Usulan dan/ atau permohonan data | Daftar usulan kebutuhan data | a. Melakukan proses identifikasi data secara mandiri<br>b. Menerima usulan permohonan data |
| 2. | Konfirmasi kebutuhan data | Daftar usulan kebutuhan data | a. Daftar kebutuhan data<br>b. Standar data statistik | c. Melakukan diskusi dengan balai/unit organisasi teknis/pihak terkait, berkaitan dengan prioritisasi kebutuhan data<br>d. Menetapkan standar data statistik |
| 3. | Menetapkan tujuan dan sasaran *output* | a. Daftar kebutuhan data<br>b. Standar data | Rencana *output* kegiatan statistik | Melakukan identifikasi dan reviu *output* kegiatan statistik yang dibutuhkan pengguna |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| | | statistik | | |
| 4. | Identifikasi konsep dan definisi data | a. Daftar kebutuhan data<br>b. Standar data statistik<br>c. Rencana *output* kegiatan statistik | Metadata statistik | a. Melakukan pengecekan konsep dan definisi variabel data yang ada dalam sistem metadata<br>b. Membuat konsep dan definisi variabel data, jika belum tersedia dalam sistem metadata, menurut perspektif pengguna. |
| 5. | Menyusun proposal rencana kegiatan | Daftar kebutuhan data<br>Standar data statistik<br>Rencana kegiatan statistik<br>Metadata Statistik | Proposal rencana kegiatan | Melakukan penyusunan dan reviu proposal kegiatan statistik |

2) Prosedur Perancangan Kegiatan Statistik




Gambar 2 Prosedur perancangan kegiatan statistik

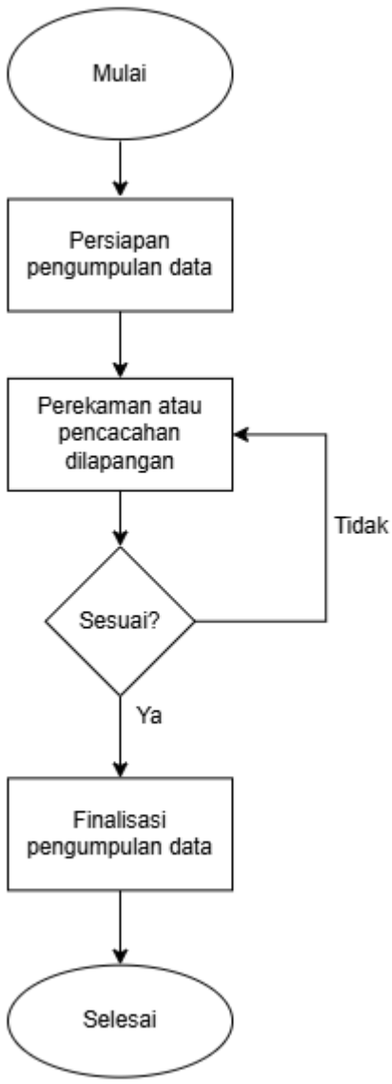
Tabel 7 Prosedur perancangan kegiatan statistik

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Pengajuan rekomendasi dan standar data | Proposal rencana kegiatan | a. Rekomendasi kegiatan statistik sektoral<br>b. Standar data statistik | a. Mengajukan proposal kegiatan pada aplikasi Pembina Data Statistik untuk mendapatkan rekomendasi kegiatan statistik sektoral<br>b. Mengajukan standar data statistik pada aplikasi Pembina Data Statistik |
| 2. | Merancang pengumpulan data | Proposal rencana kegiatan | a. Cara pengumpulan data<br>b. Metode pengumpulan data<br>c. Moda pengumpulan data | Menentukan cara, metode dan moda pengumpulan data |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 3. | Merancang pengolahan dan analisis data | Proposal rencana kegiatan | Metode pengolahan dan analisis data | Menentukan metode pengolahan dan analisis data yang tepat |
| 4. | Membangun instrumen pengumpulan data | Metode pengumpulan data | Instrumen pengumpulan data | a. Menyiapkan instrumen pengumpulan data dan menguji coba<br>b. Menyusun pedoman baku untuk instrumen baru<br>c. Menguji coba kembali apabila menggunakan instrumen yang sudah ada sebelumnya untuk memastikan keakuratannya |
| 5. | Menyusun alur kerja | a. Proposal rencana kegiatan<br>b. Metode pengolahan dan analisis data<br>c. Instrumen pengumpulan data | (1) Jadwal Kegiatan<br>(2) SOP (*Standard Operational Procedur*) | a. Penyusunan jadwal kegiatan<br>b. Penyusunan SOP (*Standard Operational Procedur*) sesuai rencana kegiatan |

3) Prosedur Pengumpulan Data Statistik

a) Data Primer

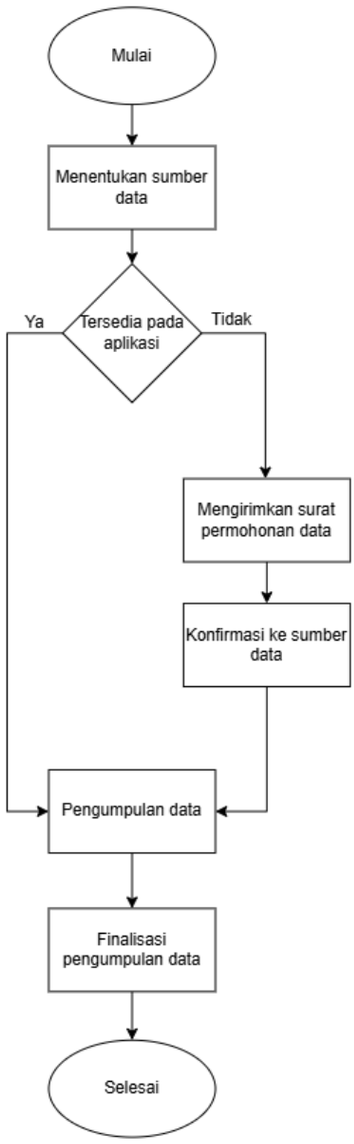



Gambar 3 Prosedur pengumpulan data statistik (Data Primer)

Tabel 8 Prosedur pengumpulan data statistik (Data Primer)

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Persiapan pengumpulan data statistik | Instrumen Pengumpulan data | Rencana survei/ pengumpulan data | a. Menyiapkan petugas pendataan dan mengadakan pelatihan jika dibutuhkan<br>b. Menyiapkan instrumen pengumpulan data sesuai rancangan<br>c. Menyiapkan protokol manajemen data |
| 2. | Perekaman/pencacahan di lapangan | Instrumen Pengumpulan data | Data dari lapangan | Melakukan pengukuran/ pengumpulan terhadap objek data dan/atau wawancara |
| 3. | Finalisasi Pengumpulan Data | *File* data | *Database* | Mememasukkan dan menyimpan data ke dalam *database* |

b) Data Sekunder



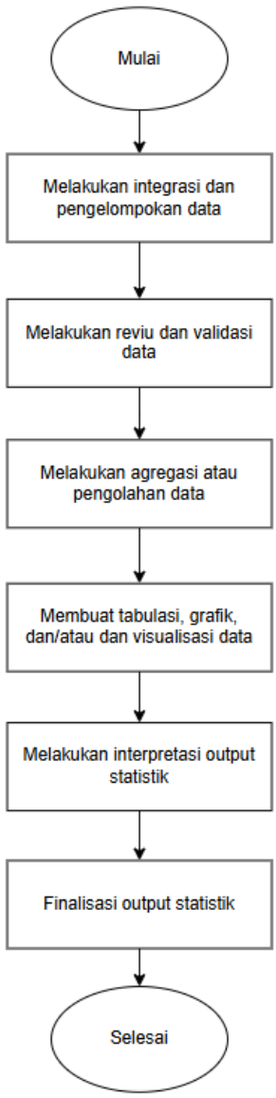

Gambar 4 Gambar 4 Prosedur pengumpulan data statistik (Data Sekunder)

Tabel 9 Prosedur pengumpulan data statistik (Data Sekunder)

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Menentukan sumber data | a. Data yang dimiliki<br>a. Daftar sumber data | Informasi dari sumber data | a. Koordinasi, memeriksa ketersediaan data yang dimiliki |
| 2. | Mengirimkan surat permohonan data | a. Format kebutuhan data<br>b. Daftar lokasi/ wilayah terpilih<br>c. Surat permohonan | a. Surat permohonan data<br>b. Surat terkirim/ tanda terima surat | a. Membuat surat permohonan permintaan data kepada unit pemilik data<br>b. Mengirimkan surat permohonan data kepada unit yang dituju |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| | | data | | |
| 3. | Konfirmasi ke sumber data | Surat permohonan data | Informasi ketersediaan, waktu dan cara pengambilan data | Menghubungi unit yang dituju perihal ketersediaan, waktu dan metode pengambilan data |
| 4. | Pengumpulan data | Informasi ketersediaan, waktu dan cara pengambilan data | Data dan informasi | Melaksanakan pengumpulan data dari unit tujuan, dapat dilakukan dengan mengunjungi langsung, surat elektronik, penyimpanan virtual atau *database service* |
| 5. | Finalisasi pengumpulan data | *File* data | *Database* | Mememasukkan dan menyimpan data ke dalam *database* |

4) Prosedur Pengolahan dan Analisis Data Statistik



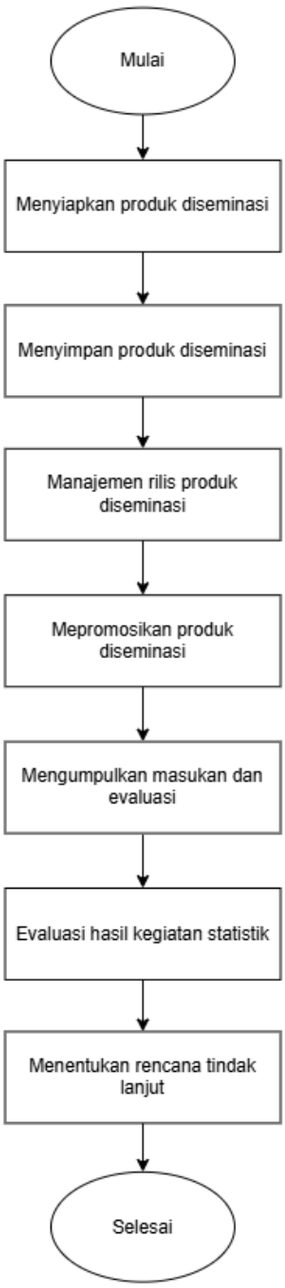

Gambar 5 Prosedur pengolahan dan analisis data statistik

Tabel 10 Prosedur pengolahan dan analisis data statistik

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Melakukan integrasi dan pengelompokan data | Daftar sumber data (internal atau eksternal) | *Dataset* terintegrasi | a. Mengidentifikasi dan melakukan pemilihan sumber data untuk diintegrasikan<br>b. Proses pengambilan data dari berbagai sumber data<br>c. Melakukan transformasi data agar format data seragam dan konsisten<br>d. Melakukan pengelompokkan (*clustering*) data |
| 2. | Melakukan reviu dan validasi data | *Dataset* terintegrasi | a. Laporan kualitas data<br>b. Data siap pakai | a. Melakukan validasi data<br>b. Menyusun laporan tentang data *error*<br>c. Melakukan perbaikan data |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| | | | | d. Mendapatkan persetujuan terhadap perbaikan dan imputasi data |
| 3. | Melakukan agregasi atau pengolahan data | Data siap pakai | Data agregat | Melakukan agregasi atau metode pengolahan data lainnya sesuai dengan kebutuhan |
| 4. | Membuat tabulasi, grafik dan/atau visualisasi data | Data agregat | Tabel, grafik dan/atau visualisasi | a. Merapikan tabel<br>b. Membuat grafik dan/atau visualisasi dari tabel |
| 5. | Melakukan interpretasi output statistik | Tabel, grafik dan/atau visualisasi | Draf dokumen atau laporan analisis | a. Melakukan analisis deskriptif<br>*b.* Melakukan *in-depth analysis*<br>c. Melakukan analisis khusus |
| 6. | Finalisasi output statistik | Draf dokumen/ laporan analisis | Produk diseminasi | a. Melakukan pengecekan final terhadap *output* statistik<br>b. Menyiapkan laporan analisis *output* dan draf publikasi atau materi diseminasi<br>c. Melakukan konsultasi/ diskusi dengan Produsen Data untuk melakukan finalisasi analisis *output* statistik<br>d. Menyetujui produk diseminasi untuk dirilis |

5) Prosedur Diseminasi dan Evaluasi Data Statistik



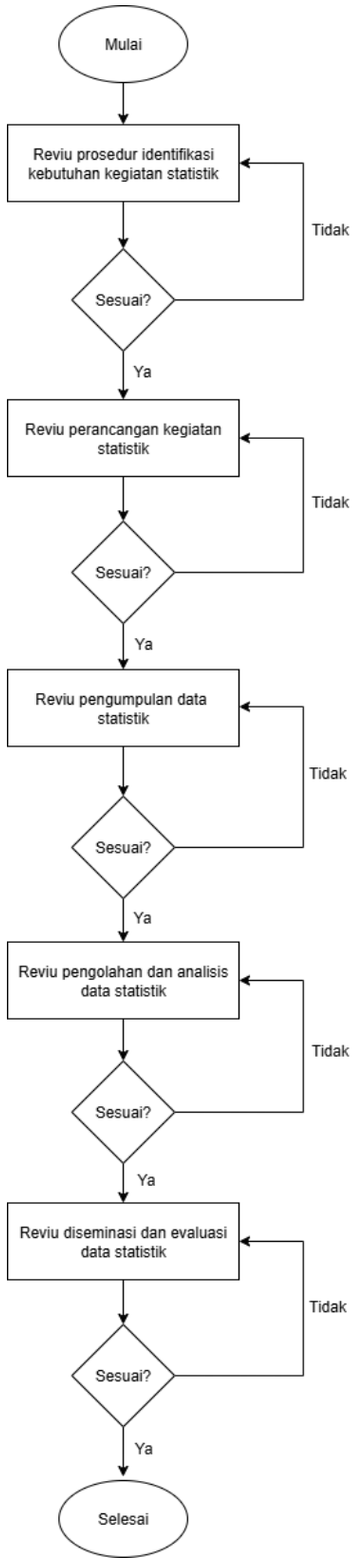

Gambar 6 Prosedur diseminasi dan evaluasi data statistik

Tabel 11 Prosedur diseminasi dan evaluasi data statistik

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Menyiapkan produk diseminasi | Produk diseminasi | Produk publikasi siap rilis | Menyiapka produk yang akan dilakukan publikasi sesuai dengan ketentuan dan kebutuhan |
| 2. | Manajemen penyimpanan produk diseminasi | Produk diseminasi | Direktori penyimpanan, arsip produk cetak dan *file* cadangan | a. *File* produk publikasi disimpan dalam media penyimpanan digital (komputer, *hardisk,* server atau penyimpanan virtual) sesuai dengan labelnya<br>b. Dibuatkan *backup* |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| | | | | penyimpanan pada direktori yang berbeda |
| 3. | Manajemen rilis produk diseminasi | Produk diseminasi | Jadwal dan mekanisme rilis | Menyusun dan menetapkan jadwal dan mekanisme rilis untuk setiap produk diseminasi |
| 4. | Mempromosikan produk diseminasi | Produk diseminasi | Publikasi produk | a. Produk cetak diberikan kepada unit/sasaran sesuai dengan kriteria<br>b. Produk digital ditayangkan dan disebarluaskan melalui media digital |
| 5. | Mengumpulkan masukan evaluasi | Saran dari pengguna data | Bahan evaluasi | Melakukan identifikasi dan klasifikasi masukan atau saran untuk mengevaluasi kegiatan |
| 6. | Evaluasi hasil kegiatan statistik | Bahan evaluasi | Laporan evaluasi | a. Melakukan evaluasi<br>b. Menyusun langkah perbaikan dari hasil evaluasi yang telah dilakukan |
| 7. | Menentukan rencana tindak lanjut | Laporan evaluasi | Laporan rencana tindak lanjut | a. Menyusun dan mendokumentasikan rencana tindak lanjut<br>b. Mendapatkan persetujuan terhadap rencana tindak lanjut yang telah disusun |

6) Pengendalian Mutu Produk




Gambar 7 Pengendalian mutu produk

Tabel 12 Pengendalian mutu produk

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1. | Reviu prosedur identifikasi kebutuhan kegiatan | Proposal kegiatan | Dokumen atau laporan hasil | Menelaah keseluruhan prosedur identifikasi kebutuhan kegiatan |

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| | statistik | | reviu | statistik |
| 2. | Reviu prosedur rancangan kegiatan statistik | a. Intrumen pengumpulan data<br>b. Jadwal Kegiatan<br>c. SOP (*Standard Operational Procedur*) | Dokumen atau laporan hasil reviu | Menelaah seluruh prosedur rancangan kegiatan statistik |
| 3. | Reviu prosedur pengumpulan data statistik | Data statistik | Dokumen atau laporan hasil reviu | Menelaah seluruh prosedur pengumpulan data statistik primer dan/atau sekunder |
| 4. | Reviu prosedur pengolahan dan analisis data statistik | Produk diseminasi | Dokumen atau laporan hasil reviu | Menelaah seluruh aspek hasil pengolahan data, seperti keakuratan, kebenaran, validitas data, narasi dan visualisasi |
| 5. | Reviu prosedur diseminasi dan evaluasi data statistik | Laporan evaluasi dan laporan rencana tindak lanjut | Dokumen atau laporan hasil reviu | a. Menelaah prosedur diseminasi untuk menghasilkan produk diseminasi yang bermutu<br>b. Menelaah prosedur evaluasi untuk menghasilkan rencana tindak lanjut yang sesuai |

7. Data dan informasi geospasial

   a. Ketentuan Umum
   Sesuai dengan batang tubuh pada Peraturan Menteri ini dan Bab Ketentuan Umum dalam lampiran ini.

   b. Daftar Data Yang Telah Ditentukan Dalam Forum Satu Data Kementerian
   Sesuai dengan daftar data yang ditentukan oleh Forum Satu Data Kementerian berdasarkan kesepakatan Forum Satu Data Indonesia dan dapat berkoordinasi dengan Kementerian/Lembaga yang menyelenggarakan urusan pemerintahan di bidang perencanaan pembangunan nasional, jika diperlukan.

   c. Standar Data Geospasial dan Meta Data Geospasial
   Berdasarkan Peraturan Badan Informasi Geospasial Nomor 3 Tahun 2025 tentang Pembentukan Standar Data Geospasial bahwa untuk membentuk/menyusun standar data geospasial dilaksanakan melalui tahapan pengusulan, harmonisasi, penetapan, dan penyebarluasan.

      1) Pengusulan dilengkapi dengan dokumen pengusulan yang terdiri atas kajian standar dan dokumen rancangan standar. Rincian isi dan substansi dari rancangan standar data mengacu pada Surat Keputusan Deputi Bidang Infrastruktur Informasi Geospasial BIG

Nomor 5 Tahun 2025 tentang Format Standar Data Geospasial. Untuk tahap harmonisasi, penetapan, dan penyebarluasan mengikuti ketentuan peraturan perundang-undangan di Kementerian PU dan atau lembaga yang menyelenggarakan urusan pemerintahan di bidang standardisasi dan penilaian kesesuaian.

2) Dokumen pengusulan dan kelengkapan dari standar data geospasial sebagai berikut;

Tabel 13 Dokumen pengusulan dan kelengkapan standar data geospasial

| No. | Dokumen Pengusulan | Isi |
|---|---|---|
| 1 | Kajian Standar Data | a. Urgensi<br>b. Konsep<br>c. Definisi<br>d. Klasifikasi<br>e. Ukuran<br>f. Satuan |
| 2 | Rancangan Standar Data | Bagian 1<br>a. Pendahuluan<br>b. Ruang Lingkup<br>c. Acuan Normatif<br>d. Istilah dan Definisi<br>e. Daftar Singkatan<br>f. Sistematika Dokumen<br><br>Bagian 2<br>a. Gambaran Umum/*Overview*<br>b. Identifikasi Produk Data<br>c. Lingkup Spesifikasi<br>d. Isi dan Struktur Data<br>e. Sistem Referensi Geospasial<br>f. Kualitas Data<br>g. Pemerolehan dan Produksi Data<br>h. Pemeliharaan Data<br>i. Penyajian/Penggambaran Data<br>j. Pengiriman Data<br>k. Metadata<br>l. Informasi Tambahan |

a) Gambaran Umum

Tabel 14 Dokumen pengusulan dan kelengkapan standar data geospasial (gambaran umum)

<table>
<tr><td>Judul</td><td>:</td><td colspan="2">berisi judul dari spesifikasi produk data geospasial</td></tr>
<tr><td>Versi</td><td>:</td><td colspan="2">versi spesifikasi produk data geospasial</td></tr>
<tr><td>Bahasa</td><td>:</td><td colspan="2">bahasa yang digunakan dalam mendokumentasikan dokumen standar data geospasial</td></tr>
<tr><td colspan="2">Kontak</td><td colspan="2" rowspan="4">Berisi nama instansi dan unit kerja yang bertanggung jawab atas spesifikasi produk data</td></tr>
<tr><td>Nama Instansi</td><td>:</td><td></td></tr>
<tr><td>Pos Elektronik / E-mail</td><td>:</td><td></td></tr>
<tr><td>Nomor Telepon</td><td>:</td><td></td></tr>
<tr><td>Situs Web</td><td>:</td><td></td><td></td></tr>
<tr><td>Alamat Situs Web Unduh</td><td>:</td><td colspan="2">URL untuk lokasi situs web tempat mengunduh dokumen spesifikasi produk data</td></tr>
<tr><td>Format</td><td>:</td><td colspan="2">format file dari dokumen standar data geospasial yang dapat diunduh pada web. Contoh formatnya adalah "application/ pdf" dan "text/xml".</td></tr>
<tr><td>Pemeliharaan</td><td>:</td><td colspan="2">informasi mengenai riwayat pemeliharaan dokumen standar data geospasial</td></tr>
<tr><td>Pembatasan</td><td>:</td><td colspan="2">kode klasifikasi yang menentukan batasan dalam menangani spesifikasi produk data.</td></tr>
<tr><td>Istilah dan Definisi</td><td>:</td><td colspan="2">istilah atau ungkapan pada dokumen spesifikasi produk data</td></tr>
<tr><td>Singkatan</td><td>:</td><td colspan="2">singkatan dari kata atau frasa tertulis pada dokumen spesifikasi produk data</td></tr>
</table>

b) Identifikasi Produk Data

Tabel 15 Dokumen pengusulan dan kelengkapan standar data geospasial (identifikasi produk data)

| | | |
|---|---|---|
| Judul | : | Penyebutan judul secara resmi dari sebuah produk data geospasial. Judul resmi dapat diperoleh dari surat keputusan atau dokumen lainnya.<br><br>Contoh: Peta Daerah Irigasi Rawa, Peta Neraca Sumber Daya Air |
| Judul Alternatif | : | Nama/judul lain dari sebuah produk data |
| Abstrak | : | Narasi singkat yang mendeskripsikan sebuah produk data geospasial |

| | | |
|---|---|---|
| Tujuan | : | Informasi mengenai maksud dan tujuan sebuah produk dikembangkan/diproduksi |
| Kategori Topik | : | Berisi kode angka dan kategori tema atau topik dari sebuah produk data geospasial |
| Representasi Spasial | : | Bentuk representasi dari sebuah produk data geospasial/informasi geospasial |
| Resolusi Spasial | : | Berisi tingkat kedetailan data yang dapat diwujudkan dalam skala atau resolusi spasial lainnya |
| *Supplemental Information* (Informasi Tambahan) | : | Informasi deskriptif lainnya tentang produk data geospasial |
| *Uniqueid* (ID Unik) | : | formasi untuk mengidentifikasi produk data, biasanya dalam bentuk kode URI |
| Kata Kunci | : | Kata atau frasa kunci yang digunakan untuk memudahkan identifikasi sebuah produk |
| Batasan | : | Informasi yang menerangkan batasan-batasan termasuk batasan hukum dan keamanan batasan dari sebuah produk data geospasial |
| Batasan Umum | | |
| Batasan Penggunaan | : | dapat berisi sebuah pernyataan/*disclaimer* batasan umum dari standar data geospasial |
| Batasan Legal/Hukum | | |
| Batasan Akses | : | |
| *Use Constraints* | : | |
| Batasan Lain | : | Contoh :<br>Data garis pantai bersifat terbuka |
| Batasan Keamanan | | |
| Klasifikasi | : | Nama pembatasan penanganan/klasifikasi batasan keamanan suatu produk data geospasial |
| *User Note* | : | Penjelasan penerapan pembatasan hukum atau pembatasan lain dan prasyarat hukum untuk memperoleh dan menggunakan produk data geospasial |
| *Handling Description* | : | Informasi tambahaan tentang pembatasan penanganan produk data geospasial |
| Kontak | : | Informasi tentang pihak penanggung jawab produk data geospasial |

| | | |
|---|---|---|
| Jangkauan | : | Berisi luasan cakupan geografis, atau cakupan waktu, atau tingkatan cakupan tertentu. |
| *Use Case* | | |
| Nama Penggunaan/*Use Case* | : | Nama kegiatan/proyek atau aktivitas lain yang menggunakan produk data geospasial |
| Nomor Penggunaan | : | Dapat berupa nomor kegiatan/tahun dan informasi kuantitatif lainnya |
| Ringkasan Penggunaan | : | Berisi deskripsi naratif tentang kasus penggunaan produk data |
| Tujuan Penggunaan* | : | Deskripsi singkat tentang tujuan yang ingin dicapai dari kasus penggunaan |
| Diagram/Skema* | : | Berupa bagan/diagram/skema dari penggunaan (use case) |
| Pelaku* | : | Nama pengguna produk data |
| Pemangku Kepentingan* | : | Berisi informasi pemangku kepentingan (K/L/D/swasta) yang terkait dengan penggunaan (use case) |
| Skenario Keberhasilan* | : | Urutan tindakan atau tahapan dalam mengeksekusi penggunaan (use case) |
| Pendorong/*Trigger** | : | Deskripsi status yang diperlukan untuk memulai penggunaan (use case) |
| Prakondisi* | : | Deskripsi mengenai kondisi yang diperlukan untuk memulai pelaksanaan penggunaan |
| Pascakondisi* | : | Deskripsi mengenai keberhasilan setelah penggunaan (use case) dijalankan |

c) Lingkup Spesifikasi

Tabel 16 Dokumen pengusulan dan kelengkapan standar data geospasial (lingkup spesifikasi)

| | | |
|---|---|---|
| Identifikasi Ruang Lingkup | : | Deskripsi singkat untuk cakupan dari spesifikasi produk data geospasial |
| Level | : | Suatu kode yang mengidentifikasikan level hierarki data |
| Nama Level | : | Nama level hierarki data geospasial |
| Deskripsi Level | : | Deskripsi detail level data geospasial |
| Jangkauan | : | Cakupan spasial, vertikal dan temporal data |

d) Isi dan Struktur Data

Isi dan struktur data secara umum menginformasikan penamaan data pada basis data yang akan disusun dan dilengkapi dengan informasi nama atribut yang terstruktur. Isi dan struktur data menjadi bagian penting dalam katalog

unsur geografi Indonesia. Katalog ini sangat strategis dalam rangka menjamin tata kelola IG yang baik terutama dalam interoperabilitas data.

Informasi isi produk data yang berbasis unsur dideskripsikan dalam bentuk skema aplikasi (*application schema*) dan sebuah katalog unsur. Sebuah skema aplikasi memberikan deskripsi formal tentang isi dan struktur data. Skema aplikasi merupakan sebuah model konseptual yang dideskripsikan menggunakan sebuah bahasa skema konseptual UML. Model memasukkan representasi tipe unsur, karakteristik unsur seperti atribut, operasi dan asosiasi unsur, hubungan turunan/pewarisan, dan pembatasan (*constraint*). Tipe atribut meliputi sifat deskriptif, geometrik, dan temporalnya. Asosiasi meliputi hubungan spasial dan temporalnya seperti hubungan topologi serta relasi nonspasial (misal kepemilikan) yang ada diantara tipe *feature*. Uraian skema aplikasi mengacu pada SNI ISO 19109. Skema aplikasi harus disertakan dalam isi dan struktur data untuk mengetahui relasi antar unsur dan karakteristiknya.

Katalog unsur merupakan repositori yang memberikan semantik kepada semua tipe unsur, berikut semua atribut dan juga domain nilai atributnya, asosiasi antar tipe unsur, dan operasi unsur yang terdapat pada skema aplikasi. SNI ISO 19110–Informasi geografis – Metodologi penyusunan katalog unsur geografi, digunakan untuk menetapkan katalog unsur pada dokumen spesifikasi produk data.

Beberapa narasi atau keterangan pada isi dan struktur data meliputi:

(1) Deskripsi naratif
Berisi deskripsi umum tentang skema aplikasi dan/atau katalog unsur untuk cakupan spesifikasi produk data geospasial yang ditentukan.

(2) Skema aplikasi
Model konseptual dari struktur data dan isi produk data menggunakan bahasa konseptual seperti UML.

(3) Konten informasi
Konten informasi berisi mengenai:
   (a) Informasi katalog unsur yang digunakan jika data berformat vektor (contoh: ShapeFile).
   (b) Informasi *Image Description* jika data merupakan data raster (contoh: citra satelit dan foto udara)
   (c) Informasi *Coverage* untuk mengisi informasi struktur atribut untuk data vektor maupun raster (MD_*Content Information*).

(4) Konten ruang lingkup
Ruang lingkup untuk konten data dan struktur informasi.

Contoh uraian sebuah unsur dan atributnya:

Tabel 17 Contoh uraian unsur dan atributnya

| Nama | | GARIS PANTAI_LN |
|---|---|---|
| Definisi | | Garis pertemuan antara daratan dengan lautan yang dipengaruhi oleh pasang surut air laut. |
| Sumber Definisi | | UU Nomor 4 Tahun 2011 tentang Informasi Geospasial |
| Kode | | – |
| Alias | | Garis Pantai |
| Nama Atribut Unsur | | Objectid, Shape, Fcode, Metadata, Srsid, Namobj, Remark, Tipe garis pantai, Karakteristik, Sumber data |

e) Sistem Referensi Geospasial
Tujuan dari bagian sistem referensi adalah untuk menentukan sistem referensi geospasial dan atau temporal yang digunakan oleh produk data geospasial.

Contoh pengisian elemen sistem referensi sebagai berikut:

Tabel 18 Contoh pengisian elemen sistem referensi

| Sistem Referensi Geospasial | | |
|---|---|---|
| *Identifier* Sistem Referensi | : | Pengenal (*identifier*) dan *codespace* untuk sistem referensi (MD_ReferenceSystem)<br>Contoh: SRGI2013-EPSG:9470 |
| Tipe Sistem Referensi | : | jenis sistem referensi yang digunakan<br>Contoh: Geographic2D |
| Sistem Referensi Temporal | : | sistem referensi temporal yang digunakan dalam spesifikasi produk data (MD_ReferenceSystem) |

f) Kualitas Data
Spesifikasi produk data harus menetapkan persyaratan kualitas data untuk produk data dengan memasukkan pernyataan mengenai tingkat kualitas yang dapat diterima. Elemen kualitas digunakan untuk mendeskripsikan kualitas produk data. Tiap elemen kualitas dideskripsikan lebih lanjut melalui:
(1) Ukuran kualitas.
(2) Metode evaluasi; dan
(3) Hasil evaluasi.

Pada data geospasial, dokumen standar kualitas yang digunakan adalah SNI ISO 19157, yang mendefinisikan kualitas data geospasial terdiri dari 6 elemen, yaitu kelengkapan, konsistensi logis, akurasi posisi, akurasi tematik, kualitas temporal, dan elemen pemanfaatan. Masing-masing produk data memiliki karakteristik yang khas sehingga pemilihan penggunaan elemen kualitas dapat disesuaikan berdasarkan kebutuhan penggunaan produk data. Pengisian masing-masing elemen Kualitas Data dapat menggunakan tabel dengan format sebagai berikut:

Tabel 19 Pengisian elemen kualitas data

| No. | KOMPONEN | DESKRIPSI |
|---|---|---|
| 1. | Nama | ... |
| 2. | Alias | ... |
| 3. | Komponen Nama | ... |
| 4. | Ukuran dasar | ... |
| 5. | Definisi | ... |
| 6. | Deskripsi | ... |
| 7. | Cakupan Evaluasi | ... |
| 8. | Parameter | ... |
| 9. | Jenis Nilai | ... |
| 10. | Struktur Nilai | ... |
| 11. | Sumber Referensi | ... |
| 12. | Contoh | ... |

g) Pemerolehan dan Produksi Data

Tujuan dari bagian pemerolehan dan produksi data adalah untuk memberikan panduan, instruksi, persyaratan dan atau deskripsi pemerolehan dan produksi data. Bagian ini tidak terlepas pada metode tertentu dan/atau langkah-langkah pemrosesan menjadi produk data. Bagian ini dapat meliputi perolehan data dari sumber data, pengolahan data termasuk survei lapangan hingga tercapai sebuah produk sesuai minimal kualitas data yang ditentukan. Untuk melengkapi uraian pemerolehan dan produksi data, dapat ditambah/digambarkan dalam bentuk diagram alir sebuah metode. Informasi pada elemen pemerolehan dan produksi terdiri atas:

(1) Pernyataan produksi data

Berisi narasi yang mendeskripsikan tentang proses pemerolehan dan produksi data.

(2) Panduan atribut.

Berisi referensi ke dokumen yang menjelaskan pemerolehan unsur dan atribut dari sumber informasi.

(3) Kriteria khusus

Berisi aturan logis yang menentukan kapan dan bagaimana unsur dan atribut harus disertakan dalam data.

(4) Lingkup pemerolehan
Merupakan cakupan untuk informasi pengambilan data.

(5) Pemrosesan dan pengambilan data
Berisi informasi tentang sumber dan/atau proses produksi yang digunakan dalam memproduksi produk data.

h) Pemeliharaan Data
Pemeliharaan data terdiri dari dua hal pokok yaitu jangka waktu pemeliharaan dan penyimpanan. Tujuan dari pemeliharaan data adalah untuk memberikan pedoman, instruksi, persyaratan, deskripsi, atau kriteria sebuah data dipelihara/dimutakhirkan dan disimpan. Beberapa ketentuan berikut sebagai gambaran isian pada bagian ini.

Contoh pengisian elemen Pemeliharaan Data:

Tabel 20 Contoh pengisian elemen pemeliharaan data

| | | |
|---|---|---|
| Deskripsi | : | Informasi tentang proses pemeliharaan suatu produk data |
| Frekuensi | : | Frekuensi pemeliharaan/pemutakhiran yang dilakukan pada suatu produk data |
| Tanggal Pemeliharaan Data (*User Defined*) | : | 1. Durasi periode sebagaimana ditentukan oleh ISO 8601.<br>2. Durasi pemeliharaan data berisi waktu (tanggal-bulan-tahun) kapan dilakukannya pemeliharaan data<br><br>Dapat diisi dengan narasi, misalnya Pemutakhiran dalam jangka waktu tertentu terhadap IGD dilaksanakan paling cepat setiap 1 (satu) tahun dan paling lambat setiap 5 (lima) tahun. |
| Penyimpanan | | Contoh isian: penyimpanan data dilakukan oleh walidata/produsen data |

i) Penyajian Data
Tujuan dari penyajian adalah untuk menentukan cara menggambarkan jenis unsur data agar dapat dibaca/pahami oleh pengguna. Spesifikasi penyajian dapat didasarkan pada ISO 19117 tetapi juga dapat didasarkan pada implementasi standar lainnya seperti OGC *Symbology Encoding*. Sebagai gambaran, salah satu bentuk penyajian

dapat dilihat pada simbologi, muka peta, dan legenda peta di bagian tepi peta.

j) Pengiriman Data

Tujuan dari pengiriman adalah untuk memberikan pedoman, instruksi, persyaratan, dan atau deskripsi format pengiriman data. Bagian ini juga menginformasikan sarana yang diperlukan untuk pengiriman bentuk fisik atau untuk pengiriman data menggunakan layanan unduhan.

Contoh implementasi elemen pengiriman adalah sebagai berikut:

Tabel 21 Contoh implementasi elemen pengiriman

| Deskripsi Format Data | | | |
|---|---|---|---|
| Nama Format Data | : | *file/database* | *Nama Format data |
| Versi Format | : | *latest version* | *Versi pengiriman |
| Spesifikasi format | | shape/database | *Spesifikasi atribut opsional berisi nama subset, profil, atau spesifikasi produk format |
| Struktur *file* | : | Vector | *Struktur dokumen pengiriman |
| Bahasa | : | ENG | *Bahasa pengiriman |
| Set Karakter | : | … | *Kode karakter yang digunakan untuk data hasil |
| Media Penyimpanan dan Pengiriman | | | |
| Unit satuan data | : | layer/NLP | *Deskripsi unit satuan data yang dikirim (misalnya:layer, tile, area geografis) |
| Perkiraan ukuran data (/unit) | : | … | *Perkiraan ukuran unit pada format yang spesifik, dinyatakan dalam Mbytes |
| Nama media data | : | file | *Nama media data pengiriman |
| Informasi Lain | : | … | *Informasi lain mengenai pengiriman data |
| Servis Pengiriman | | | |
| Service endpoint | : | … | *Berisi URL tempat klien dapat mengakses layanan tertentu |
| Tipe | : | WMS | *Properti yang menjadi ciri layanan |

| | | | |
|---|---|---|---|
| Nilai | : | … | *Teks yang merupakan nilai properti |
| Catatan | : | … | *Informasi lain tentang properti layanan tertentu |

k) Metadata

Tujuan dari bagian metadata adalah untuk memberikan persyaratan pada metadata yang akan disediakan produk data. Metadata juga merupakan sebuah katalog dengan tujuan menemukan dan membandingkan produk data. Elemen metadata yang akan diterapkan dalam metadata ditentukan standarnya, profil atau spesifikasinya. Bila diperlukan juga dengan deskripsi tentang cara menerapkan elemen metadata. Secara umum, penggunaan metadata di Indonesia mengacu pada SNI tentang profil metadata Indonesia. Dalam teknis aplikasinya, pengisian metadata memuat:

(1) Spesifikasi
Profil/standar yang digunakan sebagai referensi penyusunan metadata.

(2) Pengkodean
Format dan atau pengkodean untuk metadata.

(3) Elemen
Informasi tentang elemen metadata.

Metadata informasi geospasial garis pantai disusun mengacu pada SNI 8843–1, dengan informasi mengenai data yang berjenjang berdasarkan elemen penyusunnya. Metadata disusun mulai dari tahap pemerolehan data

l) Informasi Tambahan

Tujuan dari bagian informasi tambahan adalah untuk memberikan informasi dan atau deskripsi yang tidak tercakup pada bagian lain dalam spesifikasi produk data ini. Bagian informasi tambahan tidak boleh berisi informasi yang sudah tercakup di bagian lain dalam spesifikasi produk data.

Beberapa contoh penulisan informasi tambahan:

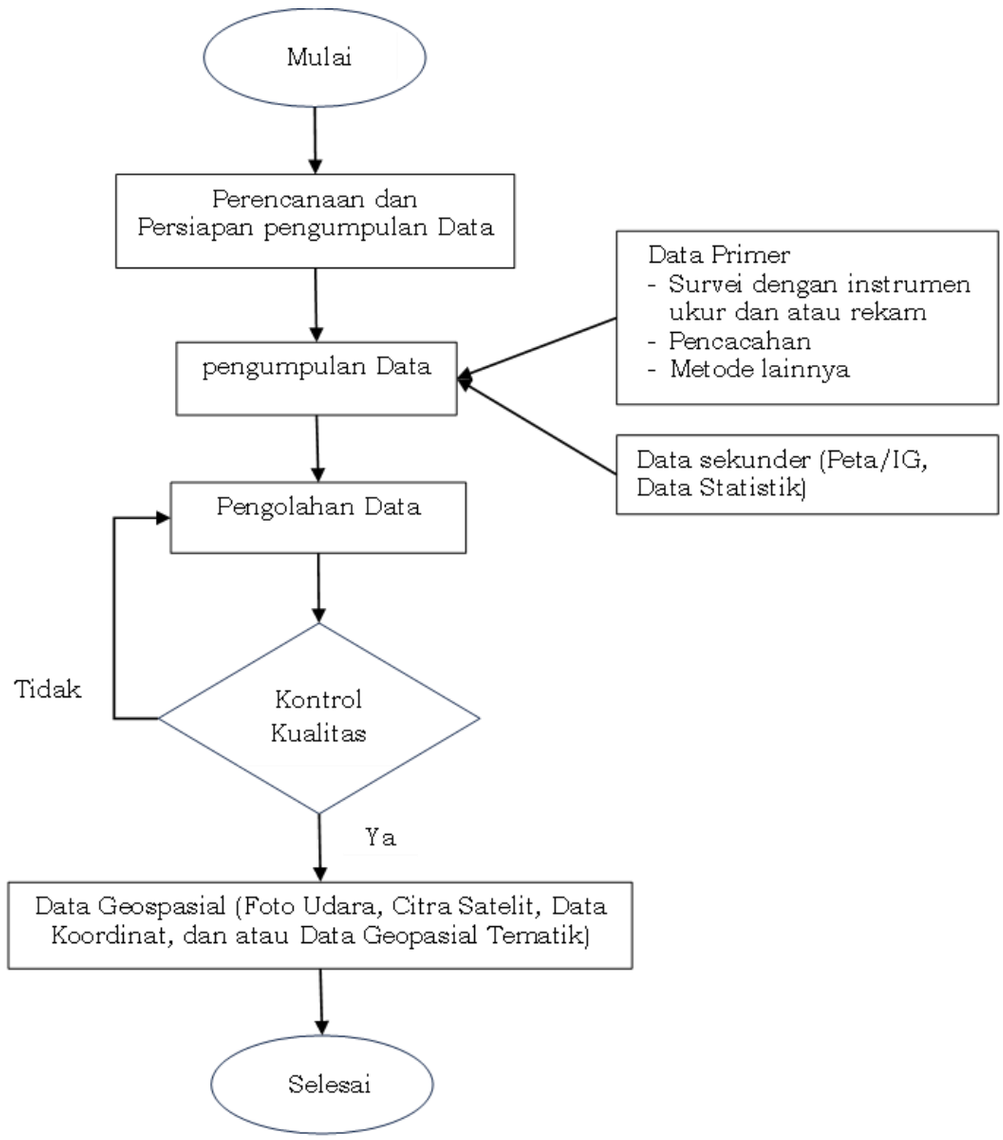
(1) “Produk data geospasial menjadi informasi resmi (institusi) ……., bila ditemui data yang sama maka penanggung jawab/produsen data tidak bertanggung jawab atas kualitas data yang dihasilkan.”

(2) “Bila ditemukan ada ketidaksesuaian antara data yang diterima konsumen dengan spesifikasinya maka akan segera dilakukan reviu dan tindak lanjut.”

3) Prosedur Penyelenggaraan Data dan Informasi Geospasial

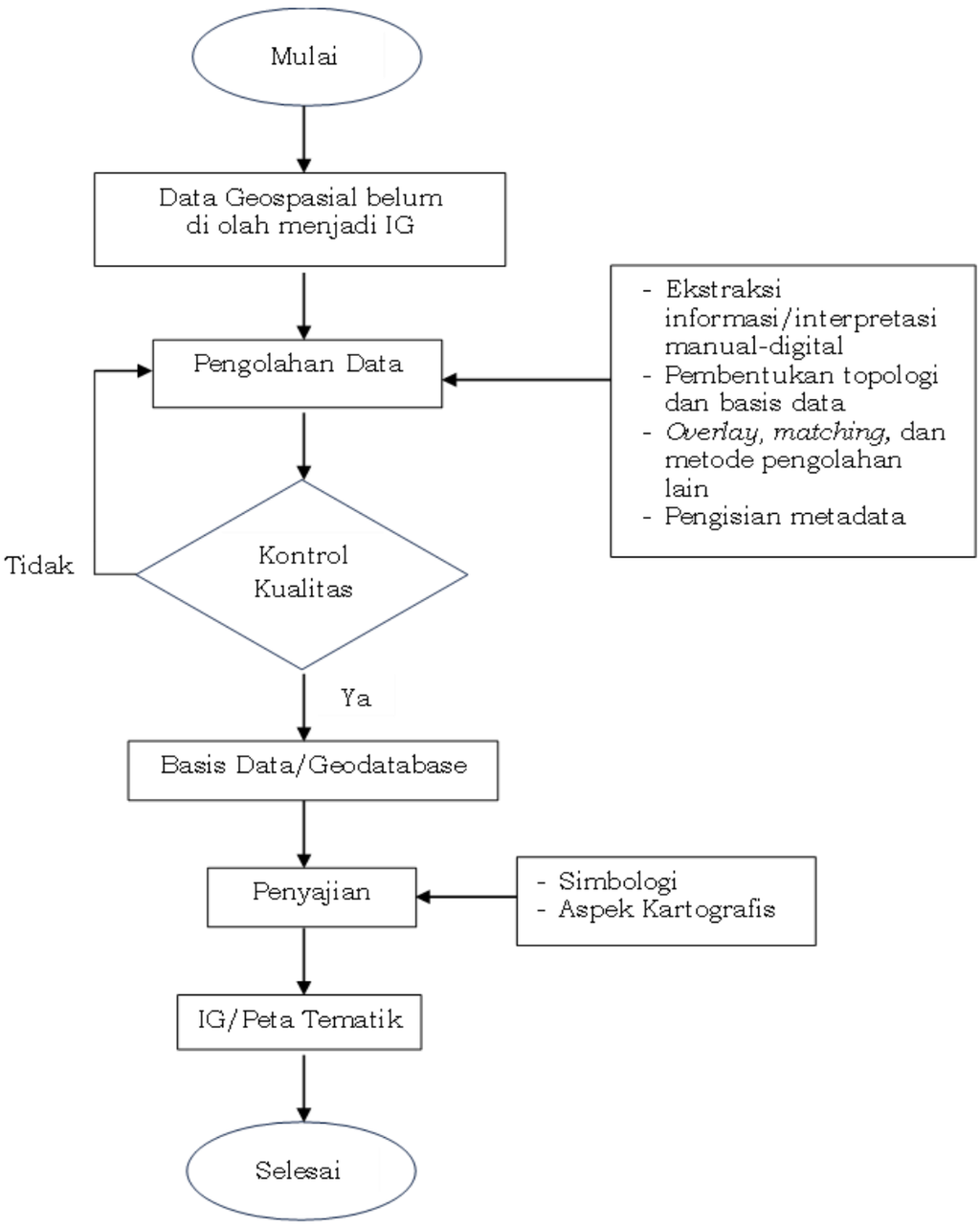
a) Ketentuan umum dan kriteria prosedur pengumpulan data geospasial mengacu pada Surat Keputusan Kepala BIG Nomor 133.2 Tahun 2024 tentang Pedoman Penyelenggaraan Data dan Informasi Geospasial untuk Instansi Pemerintah dan Pemerintah Daerah.
b) Secara umum prosedur penyelenggaraan meliputi perencanaan DG dan IG, pengumpulan data geospasial, pengolahan data geospasial (DG) dan informasi geospasial (IG), pengolahan dan penyimpanan DG dan IG, penyebarluasan IG, penggunaan IG, serta evaluasi penyelenggaraan DG dan IG.

4) Prosedur Pengumpulan Data Geospasial
a) Ketentuan umum dan kriteria prosedur pengumpulan data geospasial mengacu pada Peraturan Pemerintah Nomor 45 Tahun 2021 tentang Penyelenggaraan Informasi Geospasial dan Peraturan Badan Informasi Geospasial Nomor 18 Tahun 2021 tentang Tata Cara Penyelenggaraan Informasi Geospasial.
b) Secara umum bagan prosedur pengumpulan data geospasial sebagai berikut:




Gambar 8 prosedur pengumpulan data geospasial

5) Prosedur Pengolahan Data Geospasial dan Informasi Geospasial.
   a) Ketentuan umum dan kriteria prosedur pengolahan data geospasial dan informasi geospasial mengacu pada Peraturan Pemerintah Nomor 45 Tahun 2021 tentang Penyelenggaraan Informasi Geospasial dan Peraturan Badan Informasi Geospasial Nomor 18 Tahun 2021 tentang Tata Cara Penyelenggaraan Informasi Geospasial.
   b) Secara umum bagan prosedur pengolahan data geospasial dan informasi geospasial sebagai berikut:



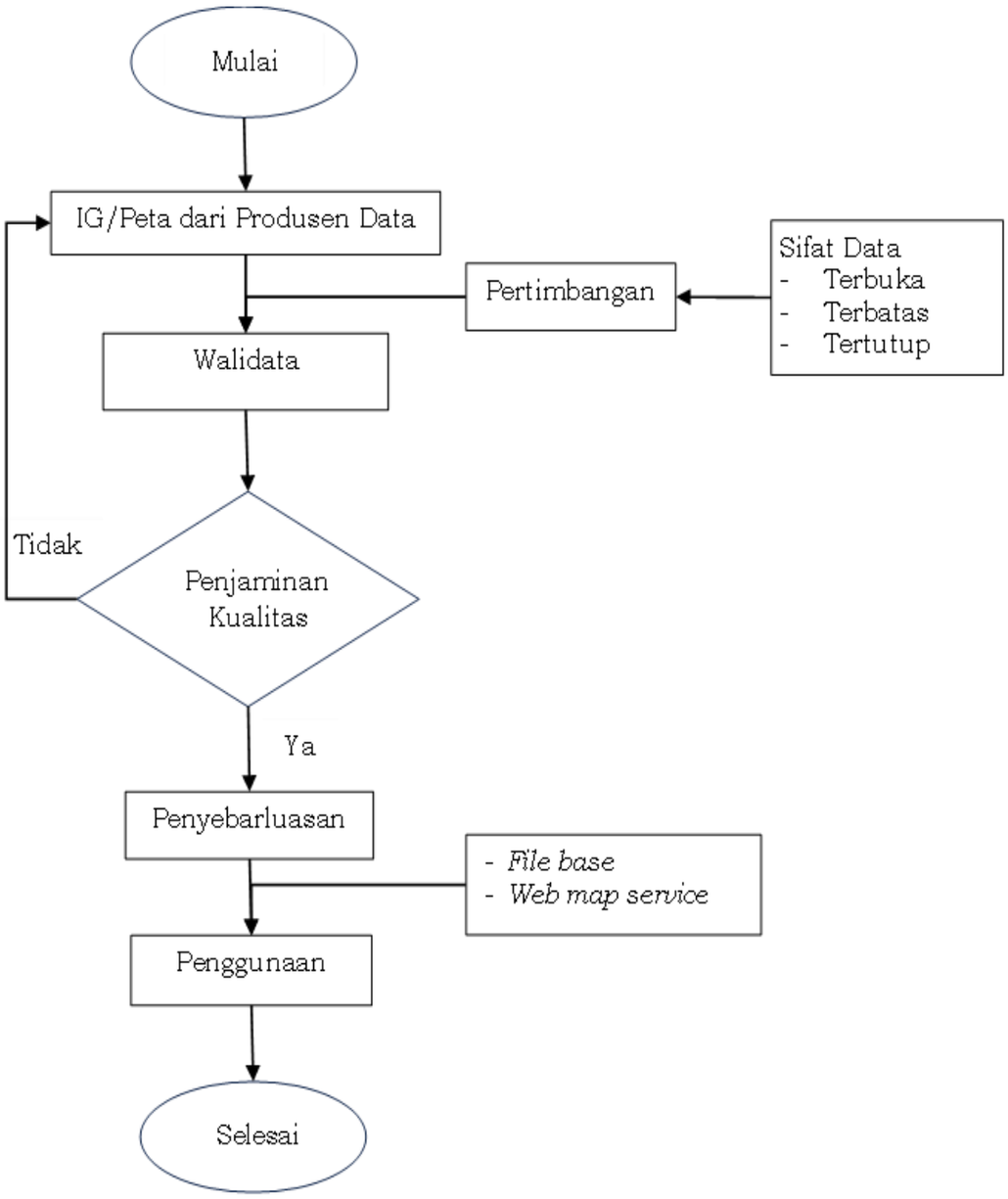

Gambar 9 prosedur pengolahan data geospasial dan informasi geospasial

6) Prosedur Penyimpanan Data Geospasial dan Informasi Geospasial
Ketentuan umum dan kriteria prosedur penyimpanan data geospasial dan informasi geospasial mengacu pada Peraturan Pemerintah Nomor 45 Tahun 2021 tentang Penyelenggaraan Informasi Geospasial dan Peraturan Badan Informasi Geospasial Nomor 18 Tahun 2021 tentang Tata Cara Penyelenggaraan Informasi Geospasial

7) Prosedur Penyebarluasan Informasi Geospasial
   a) Ketentuan umum dan kriteria prosedur penyebarluasan informasi geospasial mengacu pada Peraturan Pemerintah Nomor 45 Tahun 2021 tentang Penyelenggaraan Informasi Geospasial dan Peraturan Badan Informasi Geospasial

Nomor 18 Tahun 2021 tentang Tata Cara Penyelenggaraan Informasi Geospasial.

b) Secara umum bagan prosedur penyebarluasan informasi geospasial sebagai berikut:



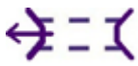
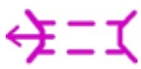

Gambar 10 Prosedur penyebarluasan informasi geospasial

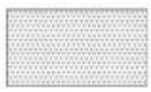
d. Muatan Peta Tematik

1) *Simbol Muatan Peta Tematik*

Tabel 22 Simbol muatan peta tematik Kementerian Pekerjaan Umum

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| **A.** SUMBER DAYA AIR | | | | | | |
| 1.Danau/Situ | Cekungan besar di permukaan bumi yang digenangi oleh air bisa tawar ataupun asin yang seluruh cekungan tersebut dikelilingi oleh daratan |  | Outline : 100 23 00 00 Fill : 100 23 00 00 | Outline : 0 196 255 Fill : 115 223 255 | Outline : 194 55 100 Fill : 194 100 100 | |
| 2. Waduk | Wadah buatan yang terbentuk sebagai akibat dibangunnya bendungan. |  | 100 00 00 00 | 00 255 255 | 180 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 3. Bendungan | Bangunan yg berupa urugan tanah, urugan batu, beton, dan/atau pasangan batu yang dibangun selain untuk menahan dan menampung air, dapat pula dibangun untuk menahan dan menampung limbah tambang (tailing) atau menampung lumpur sehingga terbentuk waduk. |  | 0 100 23 0 | 255 00 197 | 314 100 100 | |
| 4. Rencana Bendungan | Konstruksi yang dibangun untuk menahan laju air menjadi waduk, danau, atau tempat rekreasi. Seringkali bendungan juga digunakan untuk mengalirkan air ke sebuah Pembangkit Listrik Tenaga Air. Kebanyakan dam juga memiliki bagian yang disebut pintu air untuk membuang air yang tidak diinginkan secara bertahap atau berkelanjutan. |  | 0 78 39 15 | 255 00 197 | 330 200 217 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 5. Bendung | Suatu bangunan yang melintang pada aliran sungai (palung sungai), yang terbuat dari pasangan batu kali atau bronjong, atau beton, yang berfungsi untuk meninggikan muka air agar dapat dialirkan ke tempat yang diperlukan. |  | 86 100 6 1 | 79 46 137 | 262 66 54 | |
| 6. Rencana Bendung | Suatu bangunan yang direncanakan melintang pada aliran sungai (palung sungai), yang terbuat dari pasangan batu kali atau bronjong, atau beton, yang berfungsi untuk meninggikan muka air agar dapat dialirkan ke tempat yang diperlukan. |  | 86 100 6 1 | 79 46 137 | 262 66 54 | |
| 7. Bendung Gerak | Suatu bangunan yang melintang pada aliran sungai dilengkapi dengan pintu yang dapat digerakkan untuk mengatur ketinggian muka air. |  | 0 78 39 15 | 217 47 133 | 330 200 217 | |
| 8. Rencana Bendung Gerak | Suatu bangunan yang direncanakan melintang pada aliran sungai dilengkapi dengan pintu yang dapat digerakkan untuk mengatur ketinggian muka air. |  | 0 78 39 15 | 217 47 133 | 330 200 217 | |
| 9. Embung | Bangunan konservasi air berbentuk kolam untuk menampung air hujan dan air limpasan ( run off) serta sumber air lainnya untuk mendukung usaha pertanian, perkebunan dan peternakan. |  | 100 56 00 00 | 00 112 255 | 214 255 255 | |
| 10. Embung Potensi | |  | 0 78 39 15 | 217 47 133 | 330 200 217 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 11. Daerah Irigasi Berdasarkan Jenis | Kesatuan lahan yang mendapat air dari satu jaringan irigasi. | | | | | |
| a. Permukaan | Kesatuan lahan yang mendapat air dari satu jaringan irigasi dengan cara air dibiarkan mengalir bebas di atas permukaan lahan dan kemudian air akan mengisi daerah perakaran tanaman. |  | - | - | - | Warna menyesuaikan dengan kewenangan |
| b. Air Tanah | Kesatuan lahan yang mendapat air dari satu jaringan irigasi yang airnya berasal dari air tanah. |  | - | - | - | Warna menyesuaikan dengan kewenangan |
| c. Pompa | Kesatuan lahan yang mendapat air dari satu jaringan irigasi menggunakan tenaga mesin untuk mengalirkan berbagai jenis-jenis air dari sumber air. |  | - | - | - | Warna menyesuaikan dengan kewenangan |
| d. Rawa | Kesatuan lahan yang mendapat air dari satu jaringan irigasi yang airnya berasal dari rawa. |  | - | - | - | Warna menyesuaikan dengan kewenangan |
| e. Tambak | Kesatuan lahan yang mendapat air dari satu jaringan irigasi yang airnya berasal dari tambak. |  | - | - | - | Warna menyesuaikan dengan kewenangan |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 12.Daerah Irigasi Berdasarkan Kewenangan | | | | | | |
| a. Pusat | Status daerah irigasi yang pengelolaannya menjadi wewenang dan tanggungjawab Pemerintah Pusat. |  | 0 51 50 0 | 255 124 128 | 359 51 100 | |
| b. Provinsi | Status daerah irigasi yang pengelolaannya menjadi wewenang dan tanggungjawab pemerintah daerah provinsi. |  | 0 0 100 0 | 255 255 0 | 60 100 100 | |
| c. Kabupaten/ Kota | Status daerah irigasi yang pengelolaannya menjadi wewenang dan tanggungjawab pemerintah daerah kabupaten/kota. |  | 94 13 100 0 | 16 222 0 | 116 100 87 | |
| 13. Saluran Irigasi | | | | | | |
| a. Saluran Irigasi Primer | Saluran primer membawa air dari bendung ke saluran sekunder dan ke petak-petak tersier yang diairi. Batas ujung saluran primer adalah pada bangunan bagi yang terakhir. |  | 100 100 00 00 | 00 00 255 | 240 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| b. Saluran Irigasi Sekunder | Saluran sekunder membawa air dari saluran primer ke petak-petak tersier yang dilayani oleh saluran sekunder tersebut. Batas ujung saluran ini adalah pada bangunan sadap terakhir. |  | 34 100 10 00 | 00 00 255 | 284 100 90 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| c. Saluran Irigasi Tersier | Saluran tersier membawa air dari bangunan sadap tersier di jaringan utama ke dalam petak tersier lalu ke saluran kuarter. Batas ujung saluran ini adalah boks bagi kuarter yang terakhir. |  | 00 100 25 00 | 00 00 255 | 315 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| d. Saluran Pembuang Primer | Mengalirkan air lebih dari saluran pembuang sekunder ke luar daerah irigasi. Pembuang primer sering berupa saluran pembuang alamiah yang mengalirkan kelebihan air tersebut ke sungai, anak sungai atau ke laut. |  | 15 35 95 00 | 255 00 00 | 45 94 85 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| e. Saluran Pembuang Sekunder | Menampung air dari jaringan pembuang tersier dan membuang air tersebut ke pembuang primer atau langsung ke jaringan pembuang alamiah dan ke luar daerah irigasi. |  | 00 00 00 100 | 255 00 00 | 00 00 00 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| f. Suplesi | Saluran irigasi tambahan atau cadangan. |  | 100 56 | 00 112 255 | 214 100 100 | |
| 14. Bangunan Irigasi | Bangunan dan bangunan pelengkap yang diperlukan dalam penyediaan, pembagian, pemberian, penggunaan dan pembuangan air irigasi. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 15. Fasilitas Ramsar (lahan basah/rawa ) | | | | | | |
| a. Rawa Konservasi | Rawa yang mempunyai fungsi pokok melindungi, melestarikan, dan mengawetkan air untuk menyangga sistem kehidupan. |  | 53 69 16 00 | 120 215 80 | 102 63 84 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| b. Rawa Budidaya | Rawa yang fungsinya dapat dikembangkan untuk kegiatan budidaya. |  | 00 10 100 00 | 255 230 00 | 54 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| c. Daerah Reklamasi Rawa | Suatu upaya meningkatkan fungsi dan pemanfaatannya untuk kepentingan masyarakat luas terutama yang bermukim didaerah sekitar. |  | 100 60 00 6 | 00 96 239 | 216 255 239 | |
| 16. Bangunan Pengaman Pantai | Lokasi bangunan untuk mengamankan pantai dari gelombang pantai. |  | 100 23 0 0 | 0 197 255 | 194 100 100 | |
| 17. Sabo Dam | Jenis dan macam bangunan air yang dibangun dalam rangka pengendalian gerakan massa sedimen. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Font: Esri Hazardous, 14<br>Warna: Black |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 18. Mata Air | Tempat atau keluar air dari dalam tanah. |  | 20 00 00 00 | 204 255 255 | 180 20 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 19. Sumur Air Tanah | Bangunan/alat untuk pengambilan air tanah |  | 00 00 00 100 | 00 00 00 | 00 00 00 | |
| 20. Cekungan Air Tanah Lintas Provinsi | Batas cekungan air tanah yang melewati lintas provinsi. |   | 20 20 00 00 | 204 204 255 | 240 20 100 | CP : Cekungan air tanah lintas Provinsi Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 21. Cekungan Air Tanah Lintas Kabupaten/ Kota | Batas cekungan air tanah yang melewati lintas kabupaten/kota. |   | 20 20 00 00 | 204 204 255 | 240 20 100 | CK : Cekungan air tanah lintas kabupaten/kota. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 22. Neraca Air | | | | | | |
| a. Area Surplus Air | Suatu wilayah yang ketersediaan air permukaan atau rerata debit andalannya lebih besar dari kebutuhan airnya. |  | 70 0 100 0 | 80 170 0 | 100 100 70 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| b. Area Defisit Air | Suatu wilayah yang ketersediaan air permukaan atau rerata debit andalannya lebih kecil dari kebutuhan airnya. |  | 0 100 100 0 | 255 0 0 | 0 100 100 | |
| 23. Wilayah Sungai Lintas Provinsi | Batas sistem wilayah sungai yang melintas di sejumlah wilayah provinsi. |  | 00 00 100 00 | 230 230 00 | 60 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 24. Wilayah Sungai Lintas Kabupaten/ Kota | Batas sistem wilayah sungai yang melintas di sejumlah wilayah provinsi. |  | 33 00 100 00 | 170 255 00 | 80 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 25. Daerah Aliran Sungai | Batas wilayah daratan yang merupakan satu kesatuan dengan sungai dan anak-anak sungainya, yang berfungsi menampung, menyimpan, dan mengalirkan air, yang berasal dari curah hujan ke laut secara alamiah, yang batas di darat merupakan pemisah topografis dan batas di laut sampai dengan daerah perairan yang masih terpengaruh aktifitas daratan. |  | 39 54 100 00 | 155 115 00 | 45 100 00 | Tebal garis tepi 0.6 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 26. Sungai Utama | Sungai terbesar pada daerah tangkapan dan yang membawa aliran menuju muara laut |  | 100 34 10 0 | 00 169 230 | 196 100 90 | 1. Untuk Peta Tematik Sungai<br>2. Warna: Moorea Blue, width: 3 |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 27. Sungai Orde 1 | Tingkatan sungai 1 atau sungai utama, mulai dari mata air sampai bermuara di laut. |  | 100 34 10 0 | 00 169 230 | 196 100 90 | 1. Untuk Peta Tematik Sungai<br>2. Warna: Moorea Blue, width: 2 |
| 28. Sungai Orde 2 | Tingkatan sungai 2 atau anak sungai utama, mulai dari mata air sampai bermuara di sungai utama (orde 1) |  | 34 34 100 0 | 168 168 00 | 60 100 66 | Warna: Olive Green, width: 1 |
| 29. Sungai Orde 3 | Tingkatan sungai 3 adalah anak sungai orde 2, mulai dari mata air sampai bermuara di sungai orde 2. |  | 56 34 100 0 | 112 168 00 | 80 100 66 | Warna: Green, width: 1 |
| 30. Sungai Orde 4 | Tingkatan sungai 4 adalah anak sungai orde 3, mulai dari mata air sampai bermuara di sungai orde 3. |  | 34 56 100 0 | 168 112 00 | 40 100 66 | Warna: Dark Orange, width: 1 |
| 31. Sungai Orde 5 | Tingkatan sungai 5 adalah anak sungai orde 4, mulai dari mata air sampai bermuara di sungai orde 3. |  | 28 67 100 00 | 183 83 00 | 27 100 72 | |
| 32. Bangunan Pengambil/ Penyadapan Air Baku | Bangunan/alat untuk mengambil air dari sumbernya. |  | 25 09 00 00 | 191 232 255 | 202 25 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 33. Bak Penampungan Air Baku | Tempat penyimpanan air untuk sementara sebelum diolah atau didistribusikan. |  | 25 09 00 00 | 191 232 255 | 202 25 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 34. Jaringan Transmisi Air Baku | | | | | | |
| a. Jaringan Transmisi Air Baku Bersih Primer | Saluran atau pipa transmisi air bersih utama/primer. |  | 100 100 00 00 | 00 00 255 | 240 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| b. Jaringan Transmisi Air Baku Bersih Sekunder | Saluran atau pipa transmisi air bersih sekunder yang digunakan. |  | 100 00 00 00 | 00 255 255 | 180 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 35. Hidran Umum Air Baku | Kran umum yang dapat menggunakan bak penampungan air sementara dan dipakai oleh masyarakat umum di sekitar hidran umum. |  | | | | |
| 36. Sistem Pengendali Banjir | | | | | | |
| a. Saluran drainase primer | Saluran pengendali banjir primer. (Simbol di check kembali) |  | 100 100 00 00 | 00 00 255 | 240 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| b. Saluran drainase sekunder | Saluran pengendali banjir sekunder. |  | 100 00 00 00 | 00 255 255 | 180 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| c. Saluran air hujan primer | Saluran air hujan primer. |  | 00 100 25 00 | 255 00 191 | 315 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| d. Saluran air hujan sekunder | Saluran air hujan sekunder. |  | 15 35 95 00 | 217 166 13 | 45 94 85 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 37. Pos Curah Hujan | Lokasi alat pengukur tinggi hujan. |  | 36 0 59 49 | 83 129 53 | 96 58.9 50.6 | Font: ESRI Geometry Symbol, 12<br>Warna: Green |
| 38. Pos Duga Air | Lokasi alat pengukur tinggi muka air di sungai. |  | 65 42 0 23 | 68 114 196 | 258 92.9 76.9 | Font: ESRI Geometry Symbol, 12<br>Warna: Blue |
| 39. Pos Hidroklimatologi | Lokasi alat-alat pengukur suhu, kecepatan angin, kelembapan udara, penyinaran matahari, evaporasi, dan lain-lain. |  | 0 100 100 0 | 255 00 00 | 0 100 100 | Font: ESRI Geometry Symbol, 12<br>Warna: Dark Red |
| 40. Kanal | Jalur air buatan manusia. |  | 41 48 0 24 | 116 102 195 | 249 122 195 | |
| 41. Rencana Kanal | Rencana Jalur air buatan manusia. |  | 41 48 0 24 | 116 102 195 | 249 122 195 | |
| 42. Risiko Banjir | Kecenderungan suatu daerah untuk terlanda banjir atau keadaan di mana terendamnya suatu daerah atau daratan karena volume air yang meningkat. | | | | | |
| a. Tidak Rawan | |  | 83 0 94 1 | 44 252 16 | 131 93.7 98.8 | |
| b. Kerawanan Sedang | |  | 0 0 100 0 | 255 255 00 | 60 100 100 | |
| c. Rawan | |  | 0 53 96 11 | 228 108 10 | 28 100 89.4 | |
| d. Sangat Rawan | |  | 0 100 100 0 | 255 00 00 | 0 100 100 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 43. Risiko Kekeringan | Kecenderungan suatu daerah untuk mengalami kondisi ketersediaan air yang jauh di bawah kebutuhan air untuk kebutuhan hidup, pertanian, kegiatan ekonomi dan lingkungan. | | | | | |
| a. Tidak Rawan | |  | 83 0 94 1 | 44 252 16 | 131 93.7 98.8 | |
| b. Kerawanan Sedang | |  | 0 0 100 0 | 255 255 00 | 60 100 100 | |
| c. Rawan | |  | 0 53 96 11 | 228 108 10 | 28 100 89.4 | |
| d. Sangat Rawan | |  | 0 100 100 0 | 255 00 00 | 0 100 100 | |
| 44. Drainase Utama Perkotaan | Jaringan saluran drainase primer, sekunder, tersier beserta bangunan pelengkapnya yang melayani kepentingan sebagian besar warga masyarakat perkotaan. |  | 0 100 100 0 | 255 00 00 | 0 100 100 | |

| NAMA UNSUR | Pengertian | Simbol dan / atau Notasi | Spesifikasi | | | Keterangan |
|---|---|---|---|---|---|---|
| | | | CMYK (%) | RGB (255) | HSV (360 100 100) | |
| 1 | 2 | 3 | 4 | 5 | 6 | 8 |
| 45. Posko Banjir | Tempat dilakukannya pemantauan kondisi terkini terkait bencana banjir sekaligus melakukan penanggulangannya. |  | 80 30 80 20 | 50 120 70 | 136 57 47 | |
| 46. Pos Klimatologi | Tempat dilakukannya pengamatan, pengumpulan data dan penyampaian informasi berkaitan dengan iklim. |  | 0 100 100 0 | 255 0 0 | 0 100 100 | |
| 47. Pos Pemantauan | Tempat dilakukannya pemantauan kondisi dan kualitas air sungai. |  | 100 95 0 12 | 0 12 225 | 237 100 88 | |
| 48. Sistem Peringatan | Serangkaian kegiatan pemberian peringatan sesegera mungkin kepada masyarakat tentang kemungkinan terjadinya bencana pada suatu tempat oleh lembaga yang berwenang. |  | 0 10 100 0 | 255 85 00 | 20 100 100 | |
| 49. Daerah Rawan Longsor | Suatu daerah yang rentan atau memiliki kecenderungan tinggi mengalami salah satu jenis gerakan massa tanah atau batuan, ataupun percampuran keduanya, menuruni atau keluar lereng akibat terganggunya kestabilan tanah atau batuan penyusun lereng. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **A.** BINA MARGA | | | | | | |
| 1. Status Jalan | | | | | | Peta Tematik bedasarkan Status Jalan |

| | | | | | | |
|---|---|---|---|---|---|---|
| a. Jalan Nasional | Jalan arteri dan jalan kolektor dalam sistem jaringan jalan primer yang menghubungkan antar ibukota provinsi, dan jalan strategis nasional, serta jalan tol. |  | Infill<br>0%<br>100%<br>100%<br>0%<br><br>Garis base hitam<br>0%<br>0%<br>0%<br>100% | 255 0 0<br><br>base<br>0 0 0 | 0%<br>100%<br>100%<br><br>base<br>0%<br>0%<br>0% | Tebal garis base 0.8 mm<br><br>infil 0.5 mm |
| b. Jalan Nasional Belum Tersambung | Jalan Nasional yang belum tersambung baik itu masih konstruksi ataupun pembangunan jalan. |  | Infill<br>0%<br>100%<br>100%<br>0%<br><br>Garis base hitam<br>0%<br>0%<br>0%<br>100% | 255 0 0<br><br>base<br>0 0 0 | 0%<br>100%<br>100%<br><br>base<br>0%<br>0%<br>0% | Tebal garis base 0.8 mm<br><br>infil 0.5 mm<br><br>Interval garis putus 0.3 mm |
| c. Jalan Provinsi | Jalan kolektor dalam sistem jaringan primer yang menghubungkan ibukota provinsi dengan ibukota kabupaten/kota, atau antar ibukota kabupaten/kota, dan jalan strategis provinsi. |  | 0%<br>100%<br>100%<br>0% | 255 0 0 | 0%<br>100%<br>100% | Tebal garis 0.5 mm |
| d. Jalan Kabupaten/ Kota | merupakan jalan lokal dalam sistem jaringan jalan primer yang tidak termasuk jalan yang menghubungkan ibukota kabupaten dengan ibukota kecamatan, antar ibukota kecamatan, ibukota kabupaten dengan pusat kegiatan lokal, antarpusat kegiatan lokal, serta jalan umum dalam sistem jaringan jalan sekunder dalam wilayah kabupaten, dan jalan strategis kabupaten. |  | 0%<br>100%<br>100%<br>0% | 255 0 0 | 0%<br>100%<br>100% | Tebal garis 0.2 mm |
| 2. Fungsi Jalan | | | | | | Peta Tematik bedasarkan Fungsi Jalan |
| a. Jalan Arteri Primer | Jalan yang dikembangkan untuk melayani dan menghubungkan kota-kota antar pusat kegiatan nasional, antara pusat kegiatan nasional dan pusat kegiatan wilayah, antar pusat kegiatan |  | Infill<br>00 50 100 00<br>Grs bis hitam | 255 00 00 | 00 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| | | | | | | |
|---|---|---|---|---|---|---|
| | nasional dan/atau pusat kegiatan kawasan dan pelabuhan uatama/pengumpul, dan antara pusat kegiatan nasional dan/atau pusat kegiatan wilayah dan bandar udara utama/pengumpul. | | | | | |
| b. Jalan Kolektor 1 Primer | Jalan Kolektor Primer yang menghubungkan secara berdaya guna antar ibukota provinsi. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| c. Jalan Kolektor 2 Primer | Jalan Kolektor Primer yang menghubungkan secara berdaya guna antara ibukota provinsi dan ibukota kabupaten/kota. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | |
| d. Jalan Kolektor 3 Primer | Jalan Kolektor Primer yang menghubungkan secara berdaya guna antar ibukota kabupaten/ kota. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | |
| e. Jalan Kolektor 4 Primer | Jalan Kolektor Primer yang menghubungkan secara berdaya guna antara ibukota kabupaten/kota dan ibukota kecamatan. |  | | | | |
| f. Jalan Lokal Primer | Jalan yang dikembangkan untuk melayani dan menghubungkan kota-kota antar pusat kegiatan wilayah dan pusat kegiatan lokal dan/atau kawasan- kawasan berskala kecil dan/atau pelabuhan pengumpan regional dan pelabuhan pengumpan lokal. |  | 30 30 00 00 | 00 112 255 | 240 30 100 | Tebal garis 0.6 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| g. Jalan Lingkungan Primer | Jalan yang menghubungkan antarpusat kegiatan di dalam kawasan perdesaan dan jalan di dalam lingkungan kawasan perdesaan. |  | 49 76 96 0 | 130 60 10 | 26 92 51 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| h. Jalan Arteri Sekunder | Jalan yang menghubungkan kawasan primer dengan kawasan sekunder kesatu, kawasan sekunder kesatu dengan kawasan sekunder kesatu, atau kawasan sekunder kesatu dengan kawsan sekunder kedua. | | 25 100 100 0 | 190 0 0 | 0 100 75 | |
| i. Jalan Kolektor Sekunder | Jalan yang menghubungkan kawasan sekunder kedua dengan kawasan sekunder kedua, atau kawasan sekunder kedua dengan kawasan sekunder ketiga. | | 25 45 100 0 | 190 140 0 | 44 100 75 | |
| k. Jalan Lingkungan Sekunder | Jalan yang menghubungkan antarpersil dalam kawasan perkotaan. | | 34 100 10 0 | 169 0 230 | 284 100 90 | |
| 3. Kelas Jalan : | Pengelompokkan jalan berdasarkan fungsi dan intensitas lalu lintas guna kepentingan pengaturan penggunaan jalan dan kelancaran lalu lintas dan ankutan jalan, serta berdasarkan daya dukung untuk menerima muatan sumbu terberat dan dimensu kendaraan bermotor. | | | | | |
| a. Kelas I | Jalan arteri dan kolektor yang dapat dilalui kendaraan bermotor dengan ukuran lebar tidak melebihi 2.500 milimeter, ukuran panjang tidak melebihi 18.000 milimeter, ukuran paling tinggi 4.200 milimeter, dan muatan sumbu terberat 10 ton. | | 0 4 4 54 | 118 113 113 | 0 2 45 | Warna abu-abu, tebal 0.8 mm |
| b. Kelas II | Jalan arteri, kolektor, lokal, dan lingkungan yang dapat dilalui kendaraan bermotor dengan ukuran lebar tidak melebihi 2.500 milimeter, ukuran panjang tidak melebihi 12.000 milimeter, ukuran paling tinggi 4.200 milimeter, dan muatan sumbu terberat 8 ton. | | 0 4 4 54 | 118 113 113 | 0 2 45 | Warna abu-abu, tebal 0.5 mm |

| | | | | | | |
|---|---|---|---|---|---|---|
| c. Kelas III | Jalan arteri, kolektor, lokal, dan lingkungan yang dapat dilalui kendaraan bermotor dengan ukuran lebar tidak melebihi 2.100 milimeter, ukuran panjang tidak melebihi 9.000 milimeter, ukuran paling tinggi 3.500 milimeter, dan muatan sumbu terberat 8 ton. |  | 0 4 4 54 | 118<br>113<br>113 | 0 2 45 | Warna abu-abu, tebal 0.2 mm |
| d. Kelas Khusus | Jalan arteri yang dapat dilalui Kendaraan Bermotor dengan ukuran lebar melebihi 2.500 milimeter, ukuran panjang melebihi 18.000 milimeter, ukuran paling tinggi 4.200 milimeter, dan muatan sumbu terberat lebih dari 10 ton. |  | 71 0 8 12 | 64 224<br>206 | 173<br>72%<br>56% | Warna biru tosca, tebal: 0.2 mm |
| 4. Jalan Tol | Jalan alternatif untuk mengatasi kemacetan lalu lintas ataupun untuk mempersingkat jarak dari satu tempat ke tempat lain. Untuk melewatinya para pengguna harus membayar sesuai tarif yang berlaku. | | | | | |
| a. Jalan Tol Beroperasi | Jalan tol yang sudah berfungsi penuh, pengelolaan dan pemeliharaannya dilakukan oleh BUJT (Badan Usaha Jalan Tol) atau badan hukum yang bergerak di bidang pengusahaan jalan tol. |  | Infill<br>0%<br>50%<br>100%<br>0%<br><br>Garis base hitam<br>0%<br>0%<br>0%<br>100% | 255<br>127 0<br><br>base<br>0 0 0 | 30%<br>100%<br>100%<br><br>base<br>0%<br>0%<br>0% | Tebal garis base 1 mm<br><br>infil 0.6 mm |
| b. Jalan Tol Konstruksi | Jalan tol yang masih dalam<br>tahap pembangunan. |  | Infill<br>0%<br>50%<br>100%<br>0%<br><br>Garis base hitam<br>0%<br>0%<br>0%<br>100% | 255<br>127 0<br><br>base<br>0 0 0 | 30%<br>100%<br>100%<br><br>base<br>0%<br>0%<br>0% | Tebal garis base 1 mm<br><br>infil 0.6 mm<br><br>Interval kotak putih 0.3 mm |
| c. Jalan Tol Rencana | Rencana Jalan alternatif untuk mengatasi kemacetan lalu lintas ataupun untuk mempersingkat jarak dari satu tempat ke tempat lain. Untuk melewatinya para pengguna harus |  | Infill<br>0%<br>50%<br>100%<br>0%<br><br>Garis base hitam | 255<br>127 0<br><br>base<br>0 0 0 | 30%<br>100%<br>100%<br><br>base<br>0%<br>0% | Tebal garis base 1 mm<br><br>infil 0.6 mm<br><br>Interval garis putus 0.3 mm |

| | | | | | | |
|---|---|---|---|---|---|---|
| | membayar sesuai tarif yang berlaku. | | 0%<br>0%<br>0%<br>100% | | 0% | |
| 5. Jalan Layang | Struktur konstruksi yang terletak di atas permukaan tanah atau jalan lainnya untuk menghindari daerah/kawasan yang mengalami permasalahan kemacetan lalu lintas, melewati persilanagan kereta api atau meningkatkan keselamatan lalu lintas dan efisiensi. | | 00 00 00 100 | 223<br>115<br>255 | 00 100<br>100 | |
| 6. Status Jembatan | Jalan yang terletak diatas permukaan air dan/atau di atas permukaan tanah | | | | | |
| a. Jembatan Nasional | Jembatan yang berada di bawah pengelolaan dan tanggung jawab Kementerian PU, berfungsi untuk meneruskan jalan melalui rintangan seperti sungai atau lembah, dan memiliki peran strategis dalam menghubungkan antarwilayah dan mendukung transportasi nasional. |  | 00 00 00 100 | 00 00<br>00 | 00 00<br>00 | |
| b. Jembatan Khusus | Jembatan yang dibangun dengan desain khusus, bentang, panjang, pilar, dan tipe tertentu, menggunakan teknologi tertentu dan/atau memiliki kompleksitas tinggi |  | 00 50 100 00 | 255<br>127<br>00 | 30 100<br>100 | |
| c. Jembatan Gantung | Sistem struktur jembatan yang menggunakan wirerope (kabel) sebagai pemikul utama beban lalu intas dan Berat Sendiri. Pada sistem ini wirerope utama memikul beberapa hanger (penggantung) yang menghubungkan antara wirerope utama dengan gelagar/ struktur jembatan. |  | 100 00 00 00 | 00<br>175<br>239 | 196<br>100 94 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| d. Jembatan Provinsi | Konstruksi bangunan yang berfungsi menghubungkan satu tempat dengan tempat lain yang terpisah oleh rintangan seperti sungai, lembah, atau jalan raya lain, yang kemudian digolongkan berdasarkan kelas jalan dan fungsinya, termasuk untuk jaringan jalan provinsi. |  | 100 00 100 00 | 00 168 9 | 123 100 66 | |
| e. Jembatan Kabupaten/ Kota | Konstruksi jembatan yang merupakan bagian integral dari jaringan jalan daerah, berfungsi meneruskan jalan melalui rintangan alami atau buatan seperti sungai, lembah, atau jalan lain yang lebih rendah, untuk memastikan konektivitas dan aksesibilitas transportasi lokal. |  | 59 82 100 43 | 150 75 0 | 30 100 59 | |
| C. Cipta Karya | | | | | | |
| Pengembangan Sistem Penyediaan Air Minum | | | | | | |
| 1. Kapasitas Produksi Pelayanan Air Minum (≤2.5 L/Dt ) | Tersedianya akses air minum yang aman melalui Sistem Penyediaan Air Minum dengan Jaringan non perpipaan terlindungi dengan kapasitas produksi ≤ 2.5 L/Dt. |  | 0 100 100 0 | 255 00 00 | 0 100 100 | |
| 2. Kapasitas Produksi Pelayanan Air Minum (2.5 – <10 L/Dt ) | Tersedianya akses air minum yang aman melalui Sistem Penyediaan Air Minum dengan Jaringan perpipaan dan non perpipaan terlindungi dengan kapasitas produksi 2.5 – <10 L/Dt |  | 0 0 100 0 | 255 242 15 | 57 100 100 | Usulan Perubahan Simbologi |
| 3. Kapasitas Produksi Pelayanan Air Minum (10-50 L/Dt ) | Tersedianya akses air minum yang aman melalui Sistem Penyediaan Air Minum dengan Jaringan non perpipaan terlindungi dengan kapasitas produksi 10-50 L/Dt . |  | 0 0 100 0 | 00 168 9 | 123 100 66 | Usulan Perubahan Simbologi |
| 4. Kapasitas Produksi Pelayanan Air Minum ( >50 - 250 L/Dt ) | Tersedianya akses air minum yang aman melalui Sistem Penyediaan Air Minum dengan Jaringan non perpipaan terlindungi dengan kapasitas produksi > 50 - 250 L/Dt. |  | 100 0 100 0 | 00 168 9 | 123 100 66 | Usulan Perubahan Simbologi |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5. Kapasitas Produksi Pelayanan Air Minum (> 250 L/Dt ) | Tersedianya akses air minum yang aman melalui Sistem Penyediaan Air Minum dengan Jaringan non perpipaan terlindungi dengan kapasitas produksi > 250 L/Dt. |  | 100 0 0 0 | 00 175 239 | 196 100 94 | Usulan Perubahan Simbologi |
| 6. Cakupan Pelayanan Air Minum <20 % | Tersedianya wilayah cakupan air minum yang aman melalui Sistem Penyediaan Air Minum dengan jaringan perpipaan dan bukan jaringan perpipaan terlindungi dengan cakupan pelayanan <20 % |  | 0 100 100 0 | 237 50 55 | 358 88 93 | Usulan Perubahan Simbologi |
| 7. Cakupan Pelayanan Air Minum 20-<40 % | Tersedianya wilayah cakupan air minum yang aman melalui Sistem Penyediaan Air Minum dengan jaringan perpipaan dan bukan jaringan perpipaan terlindungi dengan cakupan pelayanan 20-<40 % |  | 0 60 100 0 | 245 134 52 | 28 87 96 | Usulan Perubahan Simbologi |
| 8. Cakupan Pelayanan Air Minum 40-<60 % | Tersedianya wilayah cakupan air minum yang aman melalui Sistem Penyediaan Air Minum dengan jaringan perpipaan dan bukan jaringan perpipaan terlindungi dengan cakupan pelayanan 40-<60 % |  | 0 0 100 0 | 255 242 18 | 57 100 100 | Usulan Perubahan Simbologi |
| 9. Cakupan Pelayanan Air Minum 60-<80% | Tersedianya wilayah cakupan air minum yang aman melalui Sistem Penyediaan Air Minum dengan jaringan perpipaan dan bukan jaringan perpipaan terlindungi dengan cakupan pelayanan 60-<80% |  | 100 0 100 0 | 00 168 89 | 123 100 66 | Usulan Perubahan Simbologi |
| 10. Cakupan Pelayanan Air Minum 80-100% | Tersedianya wilayah cakupan air minum yang aman melalui Sistem Penyediaan Air Minum dengan jaringan perpipaan dan bukan jaringan perpipaan terlindungi dengan cakupan pelayanan 80-100% |  | 73 36 0 14 | 52 152 219 | 204 76 86 | Baru |
| Pengembangan Layanan Sanitasi | | | | | | |
| 1. Tempat Pemrosesan Akhir (TPA) | Tempat untuk memproses dan mengembalikan sampah ke media lingkungan. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2. Tempat Pengolahan Sampah Terpadu (TPST) | Tempat dilaksanakannya kegiatan pengumpulan, pemilahan, penggunaan ulang, pendaur ulang, pengolahan, dan pemrosesan akhir sampah. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 3. Tempat Pengolahan Sampah Dengan Prinsip 3R (reduce, reuse dan recycle) (TPS 3R) | Tempat dilaksanakannya kegiatan pengumpulan, pemilahan, penggunaan ulang, dan pendauran ulang skala kawasan. |  | 00 00 00 100 dan 75, 20, 100, 5 | 0 00 00 dan 67, 138, 41 | 00 00 00 dan 107, 70, 54 | Usulan Perubahan Simbologi |
| 4. Tempat Penampungan Sementara (TPS) | Tempat sebelum sampah diangkut ke tempat pendaur ulang, pengolahan dan/atau tempat pengolahan sampah terpadu. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 5. Instalasi Pengolahan Air Limbah (IPAL) | Bangunan air yang berfungsi untuk mengolah air limbah. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 6. Instalasi Pengolahan Lumpur Tinja | Instalasi pengolahan air limbah yang dirancang hanya menerima dan mengolah lumpur tinja yang berasal dari Sub-sistem Pengolahan Setempat |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 7. Sanimas | Sistem sarana pengolahan air limbah berbasis masyarakat. |  | 00 00 00 100 dan 68, 34, 0, 0 | 00 00 00 dan 89, 149, 219 | 00 00 00 dan 211, 59, 86 | Usulan Perubahan Simbologi |
| 8. Sanitasi Lembaga Pendidikan Keagamaan (LPK) | Sarana dan prasarana sanitasi di Lembaga Pendidikan Keagamaan (LPK) |  | 00 00 00 100 dan 0, 29, 100, 41 | 00 00 00 dan 153, 107, 0 | 00 00 00 dan 40, 100, 60 | Usulan Perubahan Simbologi |

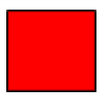
| | | | | | | |
|---|---|---|---|---|---|---|
| 9. Cuci Tangan Pakai Sabun (CTPS) | Sarana untuk pelaksanaan Cuci Tangan Pakai Sabun (CTPS) |  | 00 00 00 100 | 00 00 00 | 00 00 00 | baru |
| 10. Inpres Sanitasi | Penyediaan layanan pengelolaan air limbah domestik melalui perluasan layanan Sistem Pengelolaan Air Limbah Domestik Terpusat (SPALD-T) dan perluasan layanan Sistem Pengelolaan Air |  | 30 0 62 18 | 146 208 80 | 89 62 82 | Simbologi Baru |
| Pengembangan Kawasan Strategis | | | | | | |
| 1. Kawasan Strategis Pariwisata Nasional | Kawasan Strategis Priwisata Nasional (KSPN) adalah kawasan yang memiliki potensi untuk pengembangan pariwisata nasional yang mempunyai pengaruh penting dalam satu atau lebih aspek seperti pertumbuhan ekonomi, sosial dan budaya, pemberdayaan sumber daya alam, daya dukung lingkungan hidup. Serta pertahanan dan keamanan. (PP No. 50 tahun 2016) |  | 35 12 0 4 | 155 213 244 | 201 36 96 | |
| 2. Kawasan Strategis Pendukung Kawasan Industri | Penyelenggaraaan keterpaduan infrastruktur pada kawasan di sekitar Kawasan Industri. |  | 30 50 75 10 | 169 124 80 | 29 52 66 | Simbologi Baru |
| 3. Kawasan Strategis Pendukung Kawasan Ekonomi Khusus | Penyelenggaraaan keterpaduan infrastruktur pada kawasan di sekitar Kawasan Ekonomi Khusus. |  | 83 35 17 0 | 3 136 178 | 193 98 69 | Simbologi Baru |
| 4. Kawasan Perbatasan | Kawasan Perbatasan adalah bagian dari Wilayah Negara yang terletak pada sisi dalam sepanjang batas wilayah Indonesia dengan negara lain, dalam hal Batas Wilyah Negara di darat, Kawasan Perbatasan berada di kecamatan. (Undang-undang No. 43 tahun 2008 tentang Wilayah Negara) |  | 0 0 0 40 | 153 153 153 | 0 0 60 | |

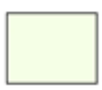
| | | | | | | |
|---|---|---|---|---|---|---|
| 5. Penanganan Kemiskinan Ekstrem | Kemiskinan Ekstrem adalah kondisi ketidakmampuan masyarakat dalam memenuhi kebutuhan dasar, yaitu makanan, air bersih, sanitasi layak, kesehatan, tempat tinggal, pendidikan dan akses informasi terhadap pendapatan dan layanan sosial. |  | Outline: 0, 6, 90, 9 Fill: 0, 28, 68, 42 | Outline: 233,218,23 Fill: 147 106 47 | Outline: 56 90 91 Fill: 35 68 57 | baru |
| 6. Infrastruktur Perdesaan | Pembangunan Infrastruktur Kawasan Berbasis Masyarakat |  | 25 40 65 0 | 196 154 | 31 44 76 | Simbologi Baru |
| 7. Kawasan Strategis Nasional | Kawasan Strategis Nasional adalah wilayah yang penataan ruangnya diprioritaskan karena mempunyai pengaruh sangat penting secara nasional terhadap kedaulatan negara, pertahanan dan keamanan negara, ekonomi, sosial, budaya, dan/atau lingkungan, termasuk wilayah yang ditetapkan sebagai warisan dunia. (PP No. 26 Tahun 2008 tentang Rencana Tata Ruang Wilayah Nasional) |  | 80 43 0 0 dan 35 12 0 0 | 44 128 195 dan 161 198 233 | 206 77 76 dan 208 30 91 | Simbologi Baru |
| 8. Kawasan Prioritas Nasional | Pengembangan Kawasan pada Kawasan Prioritas Nasional (KPN). KPN adalah kawasan dengan program/kegiatan/proyek untuk pencapaian Sasaran Rencana Pembangunan Jangka Menengah Nasional dan Kebijakan Presiden lainnya. |  | 80 43 0 0 dan 35 12 0 0 | 44 128 195 dan 161 198 233 | 206 77 76 dan 208 30 91 | Simbologi Baru |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9. Kawasan Tertentu | Pengembangan kawasan pada Kawasan Tertentu. Kawasan Tertentu merupakan wilayah yang ditetapkan sebagai prioritas pengembangan dengan karakteristik spesifik/tematik, dalam rangka mengoptimalkan potensi lokal dan/atau mengatasi tantangan pembangunan. |  | 80 43 0 0 dan 35 12 0 0 | 44 128 195 dan 161 198 233 | 206 77 76 dan 208 30 91 | Simbologi Baru |
| 10. Kawasan Perkotaan Wilayah Metropolitan | Kawasan Perkotaan Wilayah Metropolitan adalah kawasan perkotaan yang terintegrasi secara fungsional, meliputi sebuah kota inti dan kawasan sekitarnya yang memiliki ketergantungan yang erat. |  | 83 35 17 0 | 3 136 178 | 193 98 69 | Simbologi Baru |
| 11. Kawasan Perkotaan Non Wilayah Metropolitan | Pengembangan kawasan pada Kawasan Perkotaan Non Wilayah Metropolitan, yang merupakan kawasan perkotaan yang memiliki potensi sebagai pusat pertumbuhan ekonomi dan berperan dalam pemerataan pembangunan |  | 68 11 17 0 | 62 175 201 | 190 69 78 | Simbologi Baru |
| Bina Penataan Bangunan | | | | | | |
| 1. Tempat Evakuasi Sementara (TES) | Tempat perlindungan sementara terhadap gelombang tsunami maksimal hingga batas waktu dua jam setelah kejadian. |  | 7-99-93-0 dan 25-100-100-0 | 223-36-45 dan 193-39-45 | 357-84-87 dan 358-80-76 | Simbologi Baru |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2. Pos Lintas Batas Negara (PLBN) | Pembangunan wilayah PLBN bertujuan untuk meningkatkan keberadaan dan kualitas sarana dan prasarana penunjang di kawasan perbatasan. |  | 4-25-88-0 dan 3-41-91-0 | 245-191-59 dan 241-162-53 | 43-76-96 dan 35-78-95 | Simbologi Baru |
| 3. Bangunan Gedung Cagar Budaya (BGCB) | Fasilitasi fisik kepada K/L/Pemda dalam bentuk rehabilitasi atau revitalisasi bangunan cagar budaya yang dilestarikan. Bangunan cagar budaya adalah bangunan yang telah berusia 50 (lima puluh) tahun atau lebih, mewakili masa gaya paling singkat berusia 50 tahun, dan memiliki nilai penting bagi sejarah, ilmu pengetahuan, pendidikan, agama, dan/atau kebudayaan melalui penetapan |  | 2 27 93 0 | 248 196 29 | 46 88 97 | Usulan Simbologi Baru |
| 4. Bangunan Gedung Perkantoran/BGN Fungsi Perkantoran | Fasilitasi fisik kepada K/L/Pemda dalam bentuk rehabilitasi atau pembangunan baru bangunan gedung kantor |  | 2 27 93 0 | 248 196 29 | 46 88 97 | Usulan Simbologi Baru |
| 5. Bangunan Gedung Fungsi Khusus (BGFK) | Rehabilitasi atau pembangunan bangunan gedung fungsi khusus yang telah ditetapkan sebagaimana tercantum dalam kriteria pada PP 16 Tahun 2021 |  | 2 27 93 0 | 248 196 29 | 46 88 97 | Usulan Simbologi Baru |
| 6. Legenda Kegiatan Pembangunan Fisik Bidang Penataan Bangunan dan Lingkungan | Kegiatan fisik bidang penataan bangunan dan lingkungan. |  | 4-25-88-0 dan 3-41-91-0 | 245-191-59 dan 241-162-53 | 43-76-96 dan 35-78-95 | |
| 7. Ruang Terbuka Hijau (RTH) | Ruang terbuka hijau adalah satu bentuk dari ruang terbuka, yang ditandai oleh keberadaan pepohonan sebagai pengisi lahan yang utama, kemudian di dukung oleh keberadaan tanaman lain sebagai pelengkap seperti perdu, semak, rerumputan, dan tumbuhan penutup tanah lainnya. |  | 40 00 25 00 | 153 255 191 | 142 40 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8. Kota Pusaka | Program Penataan dan Pelestarian Kota Pusaka |  | 2 27 93 0 | 248 196 29 | 46 88 97 | Usulan Perubahan Simbologi |
| 9. Rumah Sakit Umum tipe A | Pusat atau tempat pelayanan dan perawatan kesehatan tipe A. |  | 100 00 10000 | 00 255 00 | 120 100 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 10.Rumah Sakit Umum tipe B | Pusat atau tempat pelayanan dan perawatan kesehatan tipe B. |  | 12 33 94 00 | 224 170 15 | 95 93 88 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 11. Rumah Sakit Umum tipe C | Pusat atau tempat pelayanan dan perawatan kesehatan tipe C. |  | 00 100 00 00 | 255 255 00 | 60 100 10 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 12. Puskesmas | Pusat atau tempat pelayanan kesehatan masyarakat. |  | 00 50 23 00 | 255 128 196 | 120 100 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| E. Prasarana Strategis | | | | | | |
| 1. Perguruan Tinggi Skala Wilayah | Pusat kegiatan pendidikan tingkat tinggi skala wilayah. |  | 00 00 00 100 | 00 255 255 | 180 100 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 2. Pendidikan Dasar (SD) | Pusat kegiatan pendidikan tingkat dasar. |  | 10 70 100 00 | 230 76 00 | 20 100 90 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3. Pendidikan Menengah Pertama (SLTP) | Pusat kegiatan pendidikan tingkat menengah pertama |  | 00 50 50 00 | 255 127 127 | 00 50 1 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 4. Pendidikan Menengah Atas (SLTA) | Pusat kegiatan pendidikan tingkat menengah atas. |  | 12 33 94 00 | 224 170 15 | 95 93 88 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 5. Pendidikan Taman Kanak-Kanak | Pusat kegiatan pendidikan atau tempat pendidikan taman anak- anak. |  | 00 00 97 00 | 255 255 08 | 60 97 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 6. Pendidikan Sekolah Luar Biasa | Pusat kegiatan pendidikan atau tempat pendidikan luar biasa. |  | 00 100 23 00 | 255 00 197 | 314 100 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 7. Pendidikan Lainnya | Pusat kegiatan pendidikan lainnya. |  | 18 00 55 00 | 209 255 115 | 80 55 100 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 8. Pasar induk wilayah. | Pasar utama di kota besar yang merupakan pusat penyalur barang-barang kebutuhan untuk pasar-pasar lainnya. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 9. Stadion wilayah. | Pusat atau tempat kegiatan olah raga atau kegiatan lainnya yang berskala besar wilayah. |  | 00 00 00 100 | 00 00 00 | 00 00 00 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 10. Pusat olah raga skala wilayah. | Pusat atau tempat khusus kegiatan olah raga pada skala wilayah. |  | 10 100 34 00 | 230 00 68 | 316 100 90 | Sesuai Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| F.Infrastruktur Wilayah | | | | | | |
| 1. Pusat Kegiatan Nasional (PKN) | Kota yang berfungsi untuk melayani kegiatan skala |  | 00 100 100 00 | 255 00 00 | 00 100 100 | Simbol minimal 3 mm. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | internasional, nasional atau beberapa provinsi. | | | | | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 2. Pusat Kegiatan Strategis Nasional (PKSN) | Kota yang ditetapkan untuk mendorong pengembangan kawasan perbatasan negara. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | Simbol minimal 3 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 3. Pusat Kegiatan Wilayah (PKW) | Kota yang berfungsi untuk melayani kegiatan skala atau beberapa kabupaten/kota. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | Simbol minimal 3 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 4. Pusat Kegiatan Lokal (PKL) | Kota yang berfungsi untuk melayani kegiatan skala kabupaten/kota atau beberapa kecamatan. |  | 00 100 100 00 | 255 00 00 | 00 100 100 | Simbol minimal 3 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 5. Kawasan Lindung | Kawasan yang ditetapkan dengan fungsi utama melindungi kelestarian lingkungan hidup yang mencakup sumber daya alam dan sumber daya buatan. |  | 04 00 10 00 | 245 255 230 | 84 10 100 | Simbol minimal 3 mm. Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 2. Kawasan Suaka Alam | Kawasan yang mempunyai keanekaragaman jenis tumbuhan dan satwa serta tipe ekosistemnya, dengan kondisi alam baik biota maupun fisiknya yang masih asli. |  | 15 15 00 00 | 217 217 255 | 240 15 100 | Sudah ada dalam Lampiran PP No. 8 Tahun 2013 Tentang Ketelitian Peta Rencana Tata Ruang |
| 3. P2KPB | Program Pengembangan Kawasan Perdesaan Berkelanjutan |  | 1 0 1 0 | 00 255 00 | 120 100 100 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4. -P3KP | Program Penataan dan Pelestarian Kota Pusaka |  | 1 0 1 0 | 00 255 00 | 120<br>100<br>100 | |
| 5. P2KH | Program Pengembangan Kota Hijau |  | 1 0 1 0 | 00 255 00 | 120<br>100<br>100 | |

2) Tata Letak Peta Tematik

Tata Letak Peta atau yang sering disebut dengan *Layout* Peta, paling sedikit memuat:

a) Logo dan Nama Instansi

Logo dan Nama instansi berfungsi untuk menunjukkan instansi yang memproduksi peta tersebut.

b) Judul Peta

Judul Peta memuat informasi nama peta menurut tipe dan lokasi pemetaan yang diletakkan pada tepi peta. Jenis huruf dan ukuran huruf yang digunakan sebagai judul peta harus lebih dominan dibandingkan dengan informasi pada tepi peta yang lain dan sangat bergantung dengan ukuran kertas.

c) Arah Mata Angin

Arah Mata Angin adalah arah utara pada peta.

d) Skala Peta

Skala Peta adalah perbandingan jarak antara dua titik di peta dengan jarak sebenarnya dari dua titik tersebut di permukaan bumi/lapangan, karena itu jarak di peta dengan jarak di lapangan menggunakan satuan ukuran yang sama. Pemilihan suatu skala peta tergantung dari tujuan penggunaan peta tersebut.

e) Sistem Koordinat dan Proyeksi Peta

Sistem Koordinat dan Proyeksi Peta menyajikan informasi tentang jenis proyeksi, unit datum. Informasi sistem koordinat dan proyeksi peta diletakkan di bawah judul peta.

f) Legenda Peta

Legenda Peta berisi penjelasan dari simbol yang mewakili objek di permukaan bumi yang terdapat pada muka peta. Semua simbol yang disajikan pada legenda digambarkan secara jelas dan sesuai dengan ukuran sebenarnya dari simbol pada muka peta. Banyak sedikitnya simbol yang disajikan tergantung pada kompleksitas informasi dari suatu peta. Letak legenda pada peta umumnya di sebelah kanan atau di sebelah bawah dari kotak muka peta.

g) Petunjuk Letak Peta (*Inset*)

Petunjuk Letak Peta merupakan kotak yang menggambarkan lokasi pemetaan secara keseluruhan, dan memberikan indikasi mengenai posisi peta bersangkutan terhadap keseluruhan daerah

yang dipetakan. Petunjuk letak peta akan memudahkan pemakai peta untuk mengetahui secara tepat posisi daerah yang ada di peta tersebut.

h) Sumber Peta
Sumber peta menyajikan informasi tentang sumber data untuk membuat peta. Informasi yang ditampilkan meliputi sumber peta dasar, sumber peta batas administrasi, dan tahun pembuatan peta. Informasi sumber peta diletakkan di bawah petunjuk letak peta (*inset*) pada tepi peta.

i) Penyusunan dan Tahun Pembuatan Peta
Penyusun dan tahun pemrosesan data merupakan Unit Kerja penyusun peta dilengkapi dengan Tahun saat proses pembuatan peta dilakukan.

j) Grid dan Koordinat Bujur/Meter Timur (x) dan Lintang/Meter Utara-Selatan (y)
Koordinat peta merupakan angka koordinat untuk menentukan letak peta pada muka peta. Koordinat Peta tergantung pada sistem proyeksi peta yang digunakan, antara lain: *Geographic Coordinate System* (GCS) dalam bujur (x) dan lintang (y) atau *Projected Coordinate System* (PCS) dalam nilai X dan Y, salah satu PCS yang umum digunakan adalah UTM (*Universal Transverse Mercator*). Koordinat Peta ditunjukkan dengan grid pada muka peta dan angkanya ditunjukkan di luar kotak muka peta.

k) Muka Peta
Muka Peta adalah tempat untuk menempatkan muatan peta yang telah diberi simbol titik, garis, atau poligon sesuai kaidah kartografis yang berlaku, yang merupakan isi utama dari peta tersebut.
Contoh format tata letak tata letak peta tematik dapat diunduh melalui
https://drive.google.com/drive/folders/1hpzmT_9I4dQncfsaE147wDypl0IHPvQ0?usp=sharing

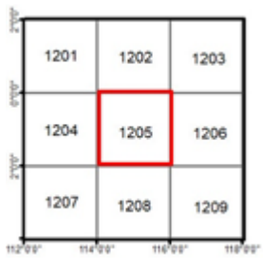
Secara grafis tata letak (*layout*) peta disajikan pada gambar-gambar di bawah ini. Kemudian tabel selanjutnya menampilkan kriteria isian dan contoh unsur-unsur layout, dan kriteria tipe huruf. Contoh hasil layout ditampilkan dalam gambar-gambar setelahnya.


Gambar 11 *Layout* peta orientasi *landscape*


Gambar 12 *Layout* peta orientasi *portrait*

Tabel 23 Kriteria *layout* peta

| No. | Unsur Layout | Kriteria | Contoh |
|---|---|---|---|
| 1 | Logo dan Nama Instansi | Huruf besar, san serif, tegak, hitam, bold.<br>Nama instansi dapat ditulis sampai dengan Unit Kerja eselon I. | KEMENTERIAN PEKERJAAN UMUM |
| 2 | Judul Peta | Huruf besar, san serif, tegak, hitam, bold. | PETA INFRASTRUKTUR<br>BIDANG PEKERJAAN UMUM |
| 3 | Arah Mata Angin | Menampilkan penunjuk arah utara. | U |
| 4 | Skala Peta | Pada peta cetak dapat menggunakan skala numerik dan skala garis, sedangkan peta digital (jpg, pdf dan sebagainya) hanya menggunakan skala garis.<br>Skala numerik ditulis menggunakan huruf san serif, tegak, hitam.<br>Skala garis digambarkan dalam satuan kilometer atau satuan lainnya sesuai dengan skala peta. | Skala 1:50.000<br>0 4.5 9 18 27 36<br>Kilometer |
| 5 | Sistem Koordinat dan Proyeksi Peta | Isian proyeksi ialah: Geografi/ Universal Transverse Mercator (UTM).<br>Isian Ellipsoid Referensi ialah: WGS 84<br>Isian Sistem Grid: Grid Geografi/ Grid UTM<br>Penulisan menggunakan huruf san serif, tegak, hitam. | Proyeksi : Geografi<br>Ellipsoid Referensi : WGS 84<br>Sistem Grid : Grid Geografi |
| 6 | Legenda | Legenda dikelompokkan berdasarkan peta dasar maupun peta tematik. Setiap kelompok peta mencantumkan nama dari kelompok muatan peta dasar maupun peta tematik tersebut.<br>Penulisan nama unsur dalam legenda menggunakan huruf san serif, tegak, hitam. | LEGENDA<br>INFORMASI DASAR<br>Ibukota Provinsi<br>Ibukota Kabupaten<br>Ibukota Kecamatan<br>Batas Negara<br>Batas Provinsi<br>Batas Kabupaten/Kota<br>Batas Kecamatan<br>Garis Pantai<br>Sungai<br>Waduk/Danau<br>BIDANG BINA MARGA<br>Jalan Nasional<br>Jalan Provinsi<br>Jalan Kabupaten/Kota<br>Jalan Tol Beroperasi<br>Jalan Tol Konstruksi<br>Rencana Jalan Tol<br>BIDANG CIPTA KARYA<br>TPA<br>IPAL<br>IPLT<br>SPAM<br>≤ 2,5 l/dt<br>> 2,5 - 5 l/dt<br>> 5 - 20 l/dt<br>> 20 - 50 l/dt<br>> 50 - 100 l/dt<br>>100 l/dt<br>BIDANG SUMBER DAYA AIR<br>Bendungan<br>Rencana Bendungan<br>Sabo Dam<br>Air Tanah<br>Pengaman Pantai<br>Daerah Irigasi Kewenangan Pusat |

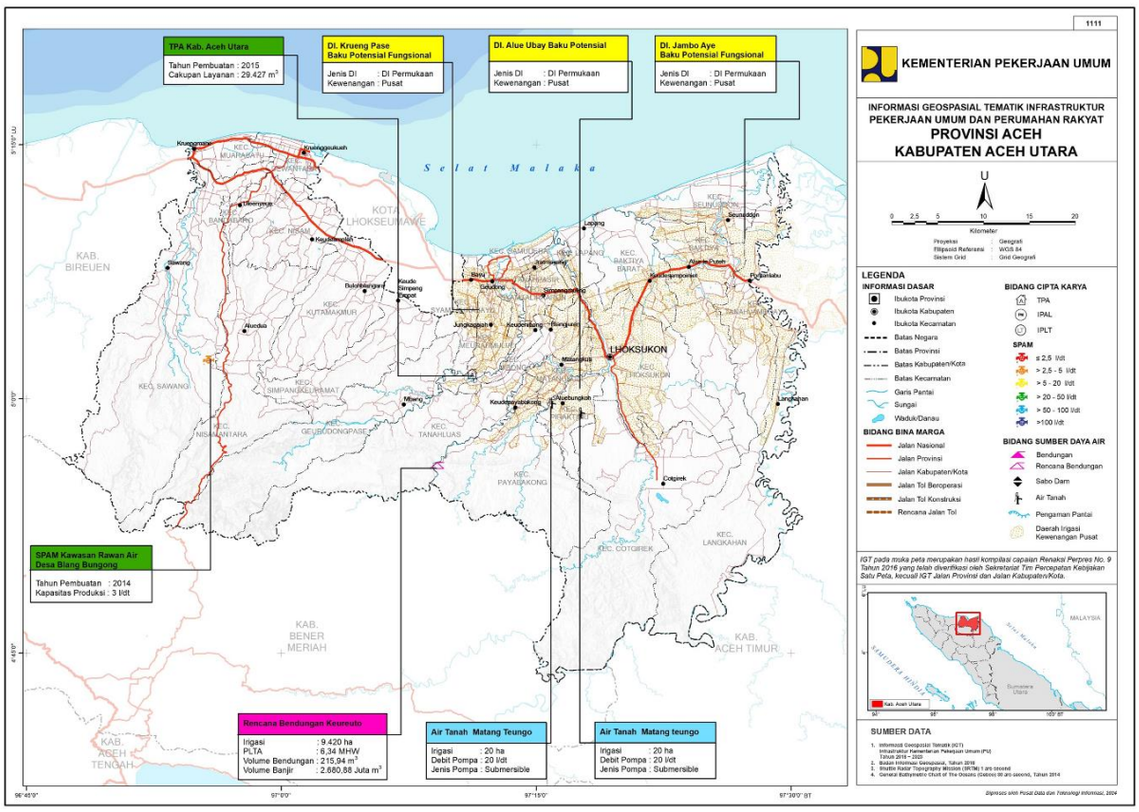
| No. | Unsur Layout | Kriteria | Contoh |
|---|---|---|---|
| | | | |
| 7. | Inset Peta | a. Berdasarkan lokasi relatif<br>Menggambarkan lokasi relatif dari peta yang digambarkan dalam muka peta.<br>Area ekstensi tampilan peta inset harus berada di atas level area muka peta. Misal: Muka peta menampilkan Kabupaten Paser, maka ekstensi inset peta menampilkan Provinsi Kalimantan Timur.<br>Lokasi dalam muka peta diberikan tanda segi empat dengan warna yang kontras dengan warna peta.<br>b. Berdasarkan indeks<br>Menggambarkan lokasi muka peta dalam indeks peta. Indeks peta dibuat berdasarkan kebutuhan menampilkan potongan-potongan area dengan skala yang sama.<br>Inset peta berdasarkan indeks dibuat menggunakan penomoran saja atau dapat dikombinasikan dengan nama dari tiap nomor indeks.<br>Lokasi dalam muka peta diberikan tanda segi empat dengan warna yang kontras dengan warna peta. |  <br>  |
| 8. | Sumber Peta | Penulisan menggunakan penomoran diurutkan mulai dari sumber data peta dasar terlebih dahulu lalu peta tematik.<br>Menggunakan huruf san serif, tegak, hitam. | **SUMBER DATA :**<br>1. Informasi Geospasial Tematik (IGT )<br>Infrastruktur Kementerian Pekerjaan Umum dan Perumahan Rakyat (PUPR)<br>Tahun 2016 – 2017<br>2. Badan Informasi Geospasial, Tahun 2018<br>3. Shuttle Radar Topography Mission (SRTM) 1 arc-second<br>4. General Bathymetric Chart of the Oceans (Gebco) 30 arc-second, 2014 |
| 9. | Grid dan Koordinat | Grid yang digunakan adalah sistem grid Geografis (bujur dan lintang) atau grid UTM (x dan y). Penulisan harus dilengkapi dengan lokasi grid, misal: BT (bujur timur) atau mT (meter Timur) serta Lintang Utara (LU) atau meter Utara (mU) – Lintang Selatan (LS) atau meter Selatan (mS) | Grid Geografis: 116°40’0” BT<br>4°25’0” LU<br>Grid UTM : 785500 mT<br>9677900 mU |

| No. | Unsur Layout | Kriteria | Contoh |
|---|---|---|---|
| 10. | Penyusun dan Tahun Pembuatan Peta | Diisikan menurut Unit Kerja eselon III, eselon II, serta tahun pembuatan peta. | Pusat Data dan Teknologi Informasi, 2025 |
| 11. | Muka Peta | Jika diperlukan dapat ditambahkan hillshade untuk menampilkan kenampakan morfologi serta batimetri laut. |  |
| | a. Perairan: samudera, laut, sungai, teluk, selat, danau, dan sejenisnya | Serif, italic, biru. Ukuran huruf dari nama unsur periran disesuaikan dengan luas unsur tersebut. | *SAMUDERA*<br>*LAUT*<br>*SELAT*<br>*DANAU*<br>*SUNGAI*<br>*Danau*<br>*Sungai* |
| | a. Rupa bumi: Pegunungan, gunung, bukit, tanung, pulau, kepulauan, lembah dan sejenisnya. | Serif, italic, hitam.<br>Ukuran huruf dari nama unsur rupa bumi disesuaikan dengan luas unsur tersebut. | *PEGUNUNGAN*<br>*GUNUNG*<br>*Gunung*<br>*Bukit* |
| | b. Nama-nama ibukota: Ibukota Negara, Ibukota Provinsi, Ibukota Kabupaten/ Kota, Ibukota Kecamatan/ Kampung lainnya. | Ibukota Negara, Ibukota Provinsi, Ibukota Kabupaten/Kota menggunakan huruf besar, serif, tegak, hitam.<br>Ibukota Kecamatan/Kampung lainnya menggunakan huruf besar dan kecil, serif, tegak, warna hitam.<br>Ukuran huruf dari nama unsur nama ibukota disesuaikan dengan tingkat administrasi dari unsur tersebut. | *JAKARTA*<br>*BANDUNG*<br>*BOGOR*<br>*Cibinong* |
| | c. Nama daerah administrasi: Negara, Provinsi, Kabupaten/ Kota, Kecamatan, Desa/ Kelurahan. | San Serif, huruf besar, tegak, hitam.<br>Ukuran huruf dari nama unsur daerah administrasi disesuaikan dengan tingkat administrasi dari unsur tersebut. | *INDONESIA*<br>*JAWA BARAT*<br>*KLATEN*<br>*KEBAYORAN BARU* |

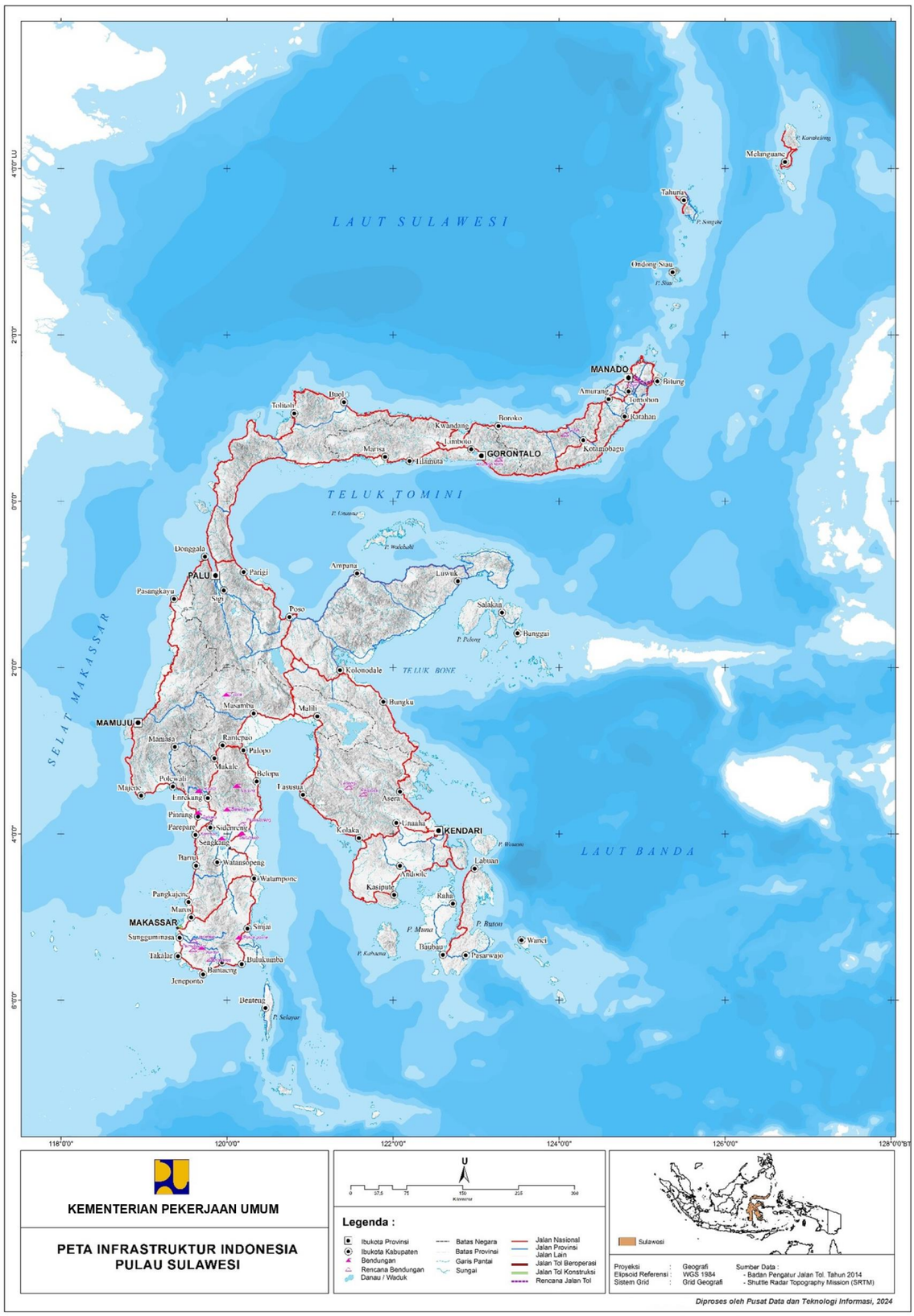
| No. | Unsur Layout | Kriteria | Contoh |
|---|---|---|---|
| | d. Nama unsur di luar tersebut: a, b, c, dan d. | San serif, huruf besar dan kecil, tegak, hitam. | *Bandar Udara Blang Bintang* |

Tabel 24 Kriteria Tipe Huruf

| No. | Tipe Huruf | Pengertian | Contoh |
|---|---|---|---|
| 1. | Serif | Tipe huruf yang memiliki garis-garis kecil pada ujung-ujung badan huruf. Garis-garis tersebut berdiri horisontal terhadap badan huruf. Contoh jenis huruf: Times New Roman, Century, Book Antiqua, Bookman Old Style, dan sebagainya. | Serif<br>Serif |
| 2. | San Serif | Tipe huruf yang tidak memiliki garis-garis kecil pada ujung-ujung badan huruf dan memiliki ketebalan huruf yang sama atau hampir sama. Contoh jenis huruf: Arial, Calibri, Century Gothic, Lucida Sans dan sebagainya. | San Serif<br>San Serif |




Gambar 13 *Layout* peta orientasi *landscape*




Gambar 14 *Layout* peta orientasi *portrait*

e. Jadwal pemutakhiran data atau rilis data
Sesuai dengan Forum Satu Data Kementerian dan produsen data.

8. Data dan informasi Kebencanaan

a. Ketentuan Umum

1) Bencana adalah peristiwa atau rangkaian peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan, baik oleh faktor alam dan/atau faktor nonalam maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa manusia, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis.
2) Data bencana adalah fakta, angka, atau catatan terkait kejadian bencana, dampak, sumber daya, maupun upaya penanggulangan.
3) Informasi bencana infrastruktur adalah data yang berkaitan dengan infrastruktur pekerjaan umum dalam fase pra bencana, tanggap darurat, dan pasca bencana.
4) *Monitoring* kejadian bencana adalah kegiatan pengawasan secara terus-menerus terhadap potensi, kejadian, dan dampak bencana untuk memastikan respon cepat dan tepat.
5) Tim Sekretariat Satgas PPB adalah unit pendukung yang bertugas mengoordinasikan administrasi, komunikasi, dan pelaporan Satuan Tugas Penanggulangan Bencana.
6) Sistem Informasi Tanggap Bencana adalah *platform* berbasis teknologi yang dikelola oleh Pusdatin dan digunakan untuk mengumpulkan, mengolah, dan menyajikan data bencana secara real time sebagai dasar pengambilan keputusan.
7) Pelaporan Bencana adalah proses penyampaian informasi mengenai kejadian, dampak, dan penanganan bencana secara sistematis kepada pihak terkait.
8) Data prabencana merupakan data yang diperoleh pada saat tidak terjadi bencana dan/atau terdapat potensi terjadinya bencana.
9) Data saat tanggap darurat adalah data yang bersifat sementara yang dikumpulkan dalam rangka pemenuhan kebutuhan selama kondisi kedaruratan bencana.
10) Data pascabencana adalah data yang diperoleh dari kegiatan rehabilitasi dan rekonstruksi.
11) Data Pembiayaan Penanggulangan Bencana merupakan Data mengenai pembiayaan dan/atau investasi dalam penyelenggaraan penanggulangan bencana.

b. Daftar Data Yang Telah Ditentukan Dalam Forum Satu Data Kementerian

Data Bencana terdiri atas:

1) Data prabencana.
   a) Data Mitigasi.
   b) Data Kesiapsiagaan.
   c) Data Peringatan Dini.
2) Data saat tanggap darurat
   a) Data kejadian bencana.

b) Data kerusakan infrastruktur.
c) Data penanganan bencana infrastruktur.
d) Data sumber daya kebencanaan.

3) Data pasca bencana berupa data program dan kegiatan pemulihan.
4) Data pembiayaan penanggulangan bencana.
   a) Data biaya per Unit Organisasi.
   b) Data biaya per Fase Bencana.
   c) Data biaya per Jenis Bencana.
5) Data dan informasi lainnya yang terkait dengan kebencanaan.

c. Standar Data dan Metadata

Beriringan dengan proses penyusunan data bencana infrastruktur, untuk menjaga kesinambungan data agar terus berdaya guna dilakukan pula penyusunan metadata kegiatan bencana infrastruktur. Kegiatan pengumpulan data bencana infrastruktur meliputi upaya penyediaan dan penyebarluasan informasi mengenai kejadian bencana yang berdampak pada infrastruktur, upaya pengembangan metode pengumpulan data bencana, serta upaya yang mengarah pada berkembangnya Sistem Informasi Bencana Nasional. Metadata kegiatan bencana infrastruktur merupakan kumpulan informasi yang menjelaskan mengenai penyelenggaraan kegiatan pengumpulan data bencana tersebut. Metadata kegiatan bencana infrastruktur yang digunakan di Kementerian Pekerjaan Umum mengacu pada metadata bencana sektoral yang dikeluarkan oleh Badan Nasional Penanggulangan Bencana (BNPB).

1) Standar Data
   Standar data digambarkan dalam bentuk struktur data infrastruktur bidang pekerjaan umum yang menyesuaikan dengan kebutuhan dari masing-masing Produsen Data. Data infrastruktur harus memiliki atribut sekurang-kurangnya terdiri atas:

   a) Data Kejadian Bencana
      Struktur data mengikuti ketentuan peraturan perundang-undangan.
   b) Data kerusakan infrastruktur
      Struktur data mengikuti ketentuan peraturan perundang-undangan.
   c) Data penanganan bencana infrastruktur.

Tabel 25 Data penanganan bencana infrastruktur

| No. | Nama *Field* | Tipe Data | Panjang Maksimal / Ukuran | Deskripsi | Contoh |
|---|---|---|---|---|---|
| 1. | Jenis Bencana | *Text* | - | Kategori bencana (banjir, tanah longsor, gempa, dll.) sesuai Juklak BNPB | Banjir |

| No. | Nama *Field* | Tipe Data | Panjang Maksimal / Ukuran | Deskripsi | Contoh |
|---|---|---|---|---|---|
| 2. | Nama Kejadian | *Text* | | Nama atau identifikasi kejadian sesuai Juklak BNPB | Banjir Bandang |
| 3. | Tanggal Pelaporan | *Date* | - | Tanggal laporan dibuat | 15 Agustus 2025 |
| 4. | Tanggal Kejadian | *Date* | - | Tanggal kejadian bencana terjadi | 14 Agustus 2025 |
| 5. | Jam Kejadian | *Time* | - | Waktu kejadian bencana | 14:30 |
| 6. | Wilayah Waktu | *Text* | - | Zona waktu Indonesia (WIB, WITA, WIT) | WIB |
| 7. | Pilih Pulau | *Text* | - | Pilihan Pulau kejadian | Jawa |
| 8. | Pilih Provinsi | *Text* | - | Pilihan Provinsi kejadian | Jawa Timur |
| 9. | Pilih Kab/Kota | *Text* | - | Pilihan Kab/Kota kejadian | Provinsi Sidoarjo |
| 10. | Pilih Kecamatan | *Text* | - | Pilihan Kecamatan kejadian | Kecamatan Gedangan |
| 11. | Pilih Kelurahan | *Text* | - | Pilihan kabupaten/kota | Kelurahan Sawotratap |
| 12. | Latitude | *Text* | 225 | Koordinat lintang | -6.912345 |
| 13. | Longitude | *Text* | 225 | Koordinat bujur | 107.634567 |
| 14. | Detail Lokasi | *Text* | 225 | Deskripsi detail lokasi | Jl. Ngagel Jaya No. 17 Surabaya, Jawa Timur, 15 km dari Jembatan Suramadu |
| 15. | Tambahkan Nama DAS dan WS | *Text* | 225 | Nama Daerah Aliran Sungai dan Wilayah Sungai | DAS Brantas – WS brantas |
| 16. | Tambahkan PCH dan Intensitas Curah Hujan | *Text* | 225 | Perkiraan curah hujan | 120 mm/hari |
| 17. | Tambahkan Ruas Jalan dan Nomor Ruas | *Text* | 225 | Nomor ruas jalan terkait | Ruas 03 – Jalan Nasional 1 |
| 18. | Kewenangan Infrastruktur (Provinsi/Kabupaten/ Kota) | Text | - | Tingkat kewenangan infrastruktur | Pusat / Provinsi / Kabupaten |
| 19. | Nama Instansi Terkait | *String* | 225 | Nama instansi terkait penanganan | BPBD Jawa Timur |

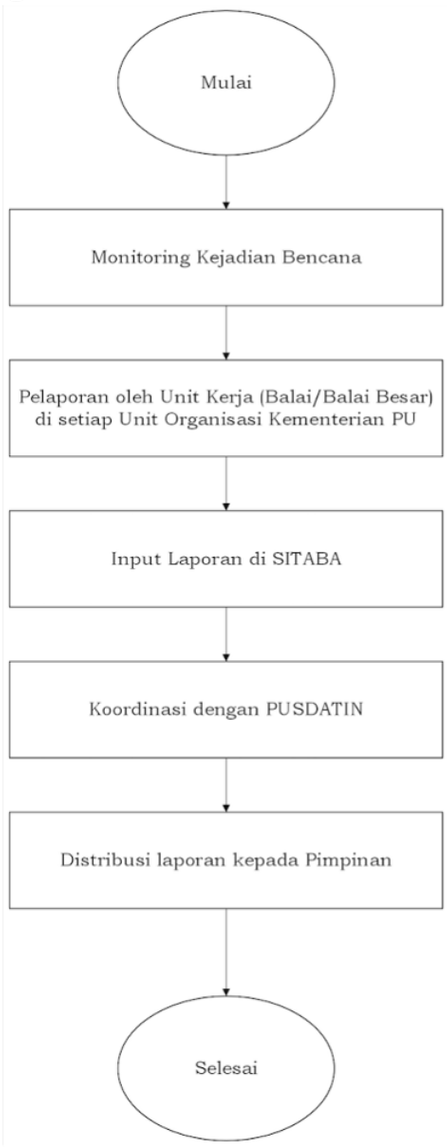
| No. | Nama *Field* | Tipe Data | Panjang Maksimal / Ukuran | Deskripsi | Contoh |
|---|---|---|---|---|---|
| 20. | Nama Penanggung Jawab | *String* | 225 | Nama penanggung jawab lapangan | Andi Pratama |
| 21. | No HP Penanggunan Jawab | *String* | 225 | Nomor telepon/HP penanggung jawab | 081234567890 |
| 22. | Unit Organisasi | *Text* | - | Pilihan Unit Organisasi Kementerian PU | Direktorat Jenderal Sumber Daya Air |
| 23. | Unit Kerja/Balai | *Text* | - | Pilihan Balai/Balai Besar Kementerian PU | Balai Besar Wilayah Sungai Brantas |
| 24. | Nama Kepala Balai | *Auto-fill* | - | Nama Kepala Balai/Balai Besar sesuai *database* | Muhammad Noor |
| 25. | No. HP | Auto-fill | - | No. Hp Kepala Balai/Balai Besar sesuai database | 08125153364 |
| 26. | Deskripsi Penyebab Bencana | *Long text* | Unlimited | Deskripsi penyebab terjadinya bencana | Curah hujan tinggi menyebabkan banjir bandang |
| 27. | Dampak Kerusakan | *Long text* | Unlimited | Deskripsi kerusakan akibat bencana | 5 rumah rusak berat, 1 jembatan putus |
| 28. | Dokumentasi | *File* (JPEG/MP4) | 5 MB | Foto/video dokumentasi | banjir.jpg |
| 29. | Penanganan Sementara | *Long text* | Unlimited | Upaya penanganan sementara | Evakuasi warga, pemasangan tanggul darurat |
| 30. | Tanggal Penanganan | *Date* | - | Tanggal dilakukan penanganan sementara | 14 Agustus 2025 |
| 31. | Kewenangan Penanganan | *Text* | - | Tingkat kewenangan penanganan | Pusat / Provinsi / Kabupaten |
| 32. | Unit Organisasi Penanganan | *Text* (Unit Organisasi PU), *Text* (Provinsi/Kabupaten/Kota) | - | Unit organisasi yang menangani | Direktorat Jenderal Sumber Daya Air |

| No. | Nama *Field* | Tipe Data | Panjang Maksimal / Ukuran | Deskripsi | Contoh |
|---|---|---|---|---|---|
| 33. | Unit Kerja Penanganan | *Text* (Unit Organisasi PU), *Text* (Provinsi/ Kabupaten /Kota) | - | Unit kerja terkait penanganan | BBWS Brantas |
| 34. | Tindak Lanjut | *Long text* | Unlimited | Rencana tindak lanjut pasca bencana | Perbaikan permanen tanggul |
| 35. | Tanggal Tindak Lanjut | *Date* | - | Tanggal pelaksanaan tindak lanjut | 14 Agustus 2025 |
| 36. | Unit Organisasi Tindak Lanjut | *Text* (Unit Organisasi PU), *Text* (Provinsi/ Kabupaten /Kota) | - | Unit organisasi tindak lanjut | Direktorat Jenderal Sumber Daya Air |
| 37. | Unit Kerja Tindak Lanjut | *Text* (Unit Organisasi PU), *Text* (Provinsi/ Kabupaten /Kota) | - | Unit kerja tindak lanjut | BBWS Brantas |
| 38. | Status Terkini | *Long text* | Unlimited | Kondisi terbaru lokasi bencana | Sudah surut, warga kembali ke rumah |
| 39. | Kebutuhan Mendesak | *Long text* | Unlimited | Kebutuhan darurat yang diperlukan | Logistik makanan, dan lain-lain |
| 40. | Dokumen Laporan Pimpinan | *File* (PDF) | 5 MB | Dokumen laporan resmi pimpinan (*Briefnotes*) | 20251508 BN GEDANGAN .pdf |
| 41. | Unit Organisasi | *Text* | - | Unit organisasi pelapor | Direktorat Jenderal Sumber Daya Air |
| 42. | Unit Kerja Pelapor | *Text* | - | Unit kerja pelapor | BBWS Brantas |
| 43. | Nama PIC | *Auto-fill* | - | Nama PIC utama | Fauzan |
| 44. | No_HP_PIC | *Auto-fill* | - | Nomor HP PIC utama | 081553558 559 |

d) Data sumber daya kebencanaan
   (1) Struktur data personel.
   (2) Struktur data alat.
   (3) Struktur data bahan.

d. Jadwal pemutakhiran data atau rilis data
   1) Data Kejadian Bencana
      Sesuai dengan ketentuan peraturan perundang-undangan.
   2) Data kerusakan infrastruktur
      Sesuai dengan ketentuan peraturan perundang-undangan.
   3) Data penanganan bencana infrastruktur
      Sesuai dengan ketentuan peraturan perundang-undangan.
   4) Data sumber daya kebencanaan
      Sesuai dengan ketentuan peraturan perundang-undangan.

e. Prosedur Pengelolaan Data dan informasi Kebencanaan




Gambar 15 Prosedur pengelolaan data dan informasi kebencanaan

Tabel 26 Prosedur pengelolaan data dan informasi kebencanaan

| No. | Aktivitas | *Input* | *Output* | Proses |
|---|---|---|---|---|
| 1 | *Monitoring* Kejadian Bencana | Informasi awal kejadian bencana dari lapangan / laporan masyarakat / instansi terkait | Data awal lokasi dan jenis bencana | Melakukan survei lapangan dan berkoordinasi dengan Pemprov/Pemkot/Pemda untuk memperoleh informasi awal kejadian bencana |
| 2 | Pelaporan Balai PU | Data dan informasi penanganan darurat, dokumentasi pendukung (foto/video) | Laporan kejadian bencana terverifikasi pimpinan Balai PU | Mengumpulkan informasi penanganan darurat dan dokumentasi lapangan, kemudian melakukan verifikasi oleh pimpinan Balai PU |
| 3 | Input Laporan di SITABA | Laporan bencana terverifikasi | Data bencana terkini di SITABA | Menginput laporan bencana ke dalam sistem SITABA menggunakan format laporan penanganan bencana (15 unsur) sesuai ND Kahar No. 247/ND/Ek/2025 |
| 4 | Koordinasi dengan PUSDATIN | Data bencana terkini di SITABA | Laporan siap disebarkan | Melakukan koordinasi dengan PUSDATIN (Tim Sekretariat PPB) terkait data bencana yang sudah diinput |
| 5 | Distribusi Laporan kepada Pimpinan | Laporan siap disebarkan | Laporan bencana diterima Menteri dan Eselon I (via email dan WA *blast*) | PUSDATIN mengirimkan laporan secara rutin pada pukul 12.00, 17.00, dan 22.00 WIB melalui email blast dan WA blast |

f. Prosedur Pengendalian Mutu Data

Sesuai dengan ketentuan peraturan perundang-undangan.

9. Data dan informasi Digital Infrastruktur

a. Ketentuan Umum
Sesuai dengan batang tubuh pada Peraturan Menteri ini dan Bab Ketentuan Umum dalam lampiran ini.

b. Definisi
Data dan informasi digital infrastruktur adalah data berupa model tiga dimensi beserta atribut geometris dan non-geometris, serta data dan dokumen lain tentang perencanaan, perancangan, konstruksi, pengawasan, dan pengelolaan aset infrastruktur dan bangunan.

c. Ruang Lingkup Data Digital Infrastruktur
1) Semua paket pekerjaan infrastruktur yang sesuai dengan tugas dan fungsi unit organisasi, termasuk yang dibina oleh Kementerian Pekerjaan Umum, harus melengkapi dan mengelola data digital infrastruktur sebagai bagian dari pelaksanaan SPBE dan kebijakan Satu Data Indonesia.
2) Data Digital Infrastruktur terdiri atas:
a) Data Dokumentasi (*Documentation*) adalah semua data hasil dokumentasi sebuah objek. Sebagai contoh data foto, data video, hasil pemindaian dokumen-dokumen seperti dokumen

kontrak, hasil fotogrametri, hasil lidar, dan dokumen lainnya.

b) Data *Alpha-Numeric* (*Alphanumerical Information*) adalah data berupa huruf-angka, baik dalam bagian dokumen laporan, rekap pekerjaan, rekaman data yang digunakan dalam sebuah proses kolaborasi melalui sebuah file.

c) Data Geometrik (*Geometrical Information*) adalah data grafis yang memiliki unsur geometrik baik secara satu (1) dimensi, dua (2) dimensi, maupun tiga (3) dimensi.

3) *Building Information Modeling* (BIM) merupakan suatu metode yang memanfaatkan teknologi digital untuk menyusun dan mengelola seluruh data dan informasi di seluruh tahapan konstruksi berbasis model 3 dimensi (3D) dengan prinsip kolaborasi.

4) Dimensi BIM

a) Ketentuan BIM 3D

BIM 3D merupakan model 3D bangunan yang memuat informasi grafis dan non-grafis serta komponen detail, sebagai acuan utama dalam proses perencanaan, perancangan, dan dokumentasi teknis pekerjaan, dengan tingkat kedetailan yang mengikuti *Level of Development* (LOD) dan *Level of Information* (LoI) sesuai tahapan pembangunan infrastruktur dan bangunan.

(1) *Level of Development*

LOD merupakan identifikator atas seberapa jauh perkembangan geometri sebuah elemen/ objek/ komponen objek atas penggunaan informasi serta menunjukan tahapan dari siklus hidup paket pekerjaan. Semakin tinggi LOD dari suatu model maka dapat dipastikan model tersebut juga semakin representatif. Target LOD untuk setiap tahapan implementasi BIM adalah sebagai berikut:

Tabel 27 Target LOD untuk setiap tahapan implementasi BIM

| No. | LOD | Definisi | Tahap |
|---|---|---|---|
| 1 | LOD 100 | Representasi konsep secara umum dalam bentuk 3D *solid model* tanpa detail yang spesifik | Perencanaan |
| 2 | LOD 200 | Pendetailan konseptual informasi seperti jumlah lantai, luasan, panjang serta pembagian denah bangunan, denah stasiun, dan denah ruang sudah dapat didefinisikan dan dipetakan dalam bentuk 3D *solid model* | Perencanaan |
| 3 | LOD 300 | Model yang sudah mencakup detail konstruksi, properti objek dan informasi spesifik seperti dimensi yang lebih akurat | Perencanaan |

| No. | LOD | Definisi | Tahap |
|---|---|---|---|
| 4 | LOD 350 | Model konstruksi sebagai referensi pelaksanaan konstruksi dan menjadi *output* yang harus dihasilkan saat pelaksanaan konstruksi dengan informasi yang dibutuhkan untuk keperluan konstruksi yang pemodelannya menghasilkan gambar konstruksi dan/atau *shop drawing*. | Pelaksanaan konstruksi |
| 5 | LOD 400 | Model konstruksi yang digunakan sebagai referensi pelaksanaan konstruksi untuk proses fabrikasi dengan menggunakan mesin / alat fabrikasi secara otomatis. Model BIM dengan LOD 400 memiliki standar komponen yang memungkinkan dilakukan fabrikasi oleh sebuah mesin/*equipment* khusus. | Pelaksanaan konstruksi |
| 6 | LOD 500 | Representasi atas *as-built* dari aset infrastruktur yang dibangun dan menjadi *output* yang harus dihasilkan saat serah terima paket pekerjaan dengan informasi yang dibutuhkan untuk keperluan operasional serta pemeliharaan yang pemodelannya didasari dari gambar *as-built drawing* dan kondisi terbangun di lapangan. | Pelaksanaan – pasca konstruksi |

(2) *Level of Information* atau Atribut Data

(a) LOI merupakan daftar informasi beserta konten yang dibutuhkan dan dipersyaratkan pada sebuah komponen/objek dalam Model BIM yang diinisiasi selama paket pekerjaan perencanaan dan dikembangkan pada pelaksanaan konstruksi. LOI merepresentasikan atribut dari sebuah objek BIM, dimana ada kategori dan konten tertentu yang harus teresedia sesuai persyaratan. Semakin tinggi LOI dari suatu model maka semakin rinci dan akurat informasi yang tersedia.

(b) LOI model BIM yang lebih detail dalam satu paket pekerjaan diatur lebih lanjut dalam peraturan teknis sesuai lingkup pekerjaan.

(c) Berikut daftar LOI yang minimum yang digunakan di setiap tahapan konstruksi:

Tabel 28 daftar LOI minimum yang digunakan di setiap tahapan konstruksi

| Tahap Konstruksi | LOD | LOI |
|---|---|---|
| Pra - Perencanaan Konseptual Design | LOD 100-200 | 1. Nama objek/barang<br>2. Parameter teknis |
| Perencanaan | LOD 300 | 1. Nama objek/barang<br>2. Parameter teknis<br>3. Kode rencana anggaran biaya (RAB)<br>4. Referensi standar<br>5. Spesifikasi material |
| Pelaksanaan Konstruksi | LOD 350 – 400 | 1. Seluruh LOI dari tahap perencanaan<br>2. Mata pembayaran<br>3. Informasi sistem objek<br>4. Merk<br>5. Nama *vendor*<br>6. Material a*pproval*<br>7. Rencana instalasi mulai<br>8. Rencana instalasi selesai<br>9. Realisasi instalasi mulai<br>10. Realisasi instalasi selesai<br>11. Persentase tingkat komponen dalam negeri (TKDN) |
| Pelaksanaan – Pasca Konstruksi | LOD 500 | 1. Nama objek/barang<br>2. Jenis barang milik negara (BMN)<br>3. Kode satuan kerja (satker)<br>4. Nama satuan kerja (satker)<br>5. Kode barang<br>6. Nomor urut pendaftaran (NUP)<br>7. Merk<br>8. Tipe<br>9. Kondisi<br>10. Tanggal perolehan<br>11. Tahun pengadaan<br>12. Lokasi aset<br>13. Koordinat lokasi aset<br>14. Nama *vendor/supplier*<br>15. Persentase tingkat komponen dalam negeri (TKDN) |

b) Ketentuan BIM 4D

BIM 4D merepresentasikan model 3D yang dilengkapi informasi jadwal pelaksanaan konstruksi, bersumber dari *master schedule* dari *project scheduling tools* yang terintegrasi dan menghasilkan simulasi tahapan dan alur konstruksi. Data BIM 4D memenuhi ketentuan sebagai berikut:

(1) Simulasi *master schedule* yang terhubung secara digital.
(2) Visualisasi realisasi progres yang terhubung secara digital.
(3) Pemodelan elemen model BIM 3D rencana dan realisasi.

c) Ketentuan BIM 5D
BIM 5D merepresentasikan model 3D yang dilengkapi dengan informasi biaya pada setiap objek. Detail informasi biaya dapat disusun menyesuaikan kebutuhan paket pekerjaan. Atribut biaya terpasang harus dipastikan tersedia pada *asset information model* sebagai informasi biaya atas barang/*equipment* terpasang. Data BIM 5D memenuhi ketentuan sebagai berikut:
(1) Biaya dan kuantifikasi objek disesuaikan dengan lingkup pekerjaan yang dapat terhubung dengan model 3D.
(2) Terhubung dengan Kurva S; dan
(3) Acuan klasifikasi objek BIM dalam pemodelan BIM 5D mengacu pada mata pembayaran.

d) Ketentuan BIM 6D
BIM 6D merepresentasikan model 3D yang dilengkapi dengan informasi dari *engineering analysis* dan/atau *sustainability*.

e) Ketentuan BIM 7D
BIM 7D merepresentasikan pemanfaatan model 3D berbasis *asset information model* (AIM) melalui ekstraksi informasi non-grafis, alfanumerik, dan tautan untuk pencatatan aset, sebagai penyusunan *master data asset* yang selanjutnya data dan informasi tersebut diteruskan untuk tahapan operasional dan pemeliharaan dengan menggunakan *computerized maintenance manajemen system* (CMMS) atau manajemen aset dan/atau sistem operasional bangunan lainnya.

f) Ketentuan BIM 8D
BIM 8D merepresentasikan model 3D yang digunakan untuk evaluasi keselamatan. Implementasi 8D memiliki cakupan yang luas dari tahapan desain, tahapan konstruksi, dan operasional.

5) *Common Data Environment* (CDE)
a) CDE merupakan media yang digunakan sebagai sarana penyimpanan, pengelolaan, dan berbagi data serta informasi digital infrastruktur secara terpusat dan terintegrasi.
b) CDE Kementerian dikelola secara bersama oleh Walidata Kementerian dan Koordinator Produsen data.

c) Penyediaan CDE paket pekerjaan menjadi tanggung jawab Koordinator Produsen Data berkoordinasi dengan Produsen Data;

d) Integrasi antara CDE paket pekerjaan dan CDE Kementerian harus dijaga secara konsisten untuk menjamin kesinambungan, keterpaduan, dan keterlacakan data infrastruktur secara menyeluruh.

e) Persyaratan CDE meliputi:
   (1) CDE menyimpan dan membaca data model BIM 3D (format *native file* dan format *industry foundation classes* (IFC)), data gambar 2D, dan data non-grafis.
   (2) CDE mampu untuk menunjang kolaborasi antar pihak yang terlibat dalam semua tahapan konstruksi yang menerapkan metode BIM, setidaknya terkait peninjauan, persetujuan, pembuatan isu, dan aktivitas lainnya. Jika integrasi tanda tangan secara digital belum bisa dilakukan pada CDE digunakan, maka proses persetujuan perlu disepakati Iebih lanjut mengenai isu integrasi tanda tangan digital tersebut antara pengguna jasa dengan penyedia jasa terkait.
   (3) CDE dapat mengatur tingkat partisipasi personal (hak akses) BIM dalam membuat, mengunggah, mengubah, dan mengatur informasi; dan
   (4) CDE menyimpan jejak riwayat secara digital yang terkait proses pembuatan dan pembangunan informasi penerapan BIM secara terintegrasi.

f) Struktur folder pada CDE untuk suatu paket pekerjaan sesuai dengan ISO 19650 terdiri atas:
   (1) *Work In Progress* merupakan folder penyimpanan data dan informasi digital infrastruktur yang digunakan selama proses pelaksanaan konstruksi oleh penyedia jasa. Informasi yang berada dalam folder ini bersifat sementara dan belum melalui proses verifikasi atau persetujuan, sehingga tidak boleh diakses atau dilihat di luar penyedia jasa.
   (2) *Shared* merupakan folder penyimpanan data dan informasi digital infrastruktur yang digunakan untuk mendukung proses pelaksanaan konstruksi secara kolaboratif antara Produsen Data dengan Tim Penyedia Jasa. Data dan informasi yang berada pada folder ini digunakan untuk tujuan koordinasi, kolaborasi, peninjauan, dan persetujuan dengan tetap memperhatikan pembatasan akses terkait keamanan.
   (3) *Published* merupakan folder penyimpanan data dan informasi digital infrastruktur yang telah disetujui melalui proses verifikasi dan otorisasi sesuai prosedur yang berlaku, sehingga dapat dijadikan acuan utama

dan sah dalam pengambilan keputusan maupun pelaksanaan pekerjaan.

(4) *Archive* merupakan folder penyimpanan akhir seluruh data dan informasi digital infrastruktur yang mempunyai fungsi sebagai arsip dan bukti dokumentasi terhadap seluruh proses pengelolaan dan perubahan data yang berpotensi digunakan untuk keperluan perancangan lanjutan, pelaksanaan konstruksi, maupun pengelolaan aset.

g) Struktur sub-folder, protokol hak akses, persyaratan format file, dan mekanisme persetujuan ditetapkan dan disesuaikan dalam Peraturan Teknis.

h) Apabila terdapat kebutuhan pembiayaan implementasi CDE, maka pembiayaan dilaksanakan sesuai peraturan yang berlaku.

6) Implementasi BIM berlandaskan pada prinsip informatif, kolaboratif, koordinatif, integratif, menyeluruh, interoperabel, transparan, otentik, keberlanjutan, mudah digunakan, dan andal. Prinsip-prinsip tersebut menjamin pengelolaan data yang akurat, keterpaduan antardisiplin, pertukaran informasi yang terbuka, keaslian data, efisiensi sumber daya, kemudahan akses, dan keandalan sistem dalam mendukung pengambilan keputusan di setiap tahapan pembangunan infrastruktur.

7) Pengelolaan Data Digital Infrastruktur mencakup seluruh tahapan hidup infrastruktur, yang meliputi:

a) Praperencanaan

Tahapan praperencanaan adalah semua kegiatan pendahuluan sebelum kegiatan *detail engineering design* (DED). Yang termasuk kegiatan praperencanaan adalah pra studi kelayakan, studi kelayakan (*feasibility study*), dan *basic design*.

b) Perencanaan Teknis

Tahapan perencanaan teknis adalah tahap pendetailan desain yang sudah ditetapkan dalam praperencanaan dengan mempertimbangkan keamanan infrastruktur dan bangunan pada saat pembangunan untuk mendapatkan perkiraan biaya pembangunan (*engineering estimate*) dan dokumen lelang konstruksi.

c) Pengadaan Lahan

Tahapan pengadaan lahan adalah kegiatan pembebasan lahan untuk pembangunan infrastruktur.

d) Pelaksanaan Konstruksi

Tahap kegiatan pembangunan fisik yang terdiri dari tiga (3) tahapan yakni tahapan prakonstruksi, tahapan konstruksi, dan tahapan pasca konstruksi. Tahapan prakonstruksi adalah masa untuk persiapan pembangunan seperti verifikasi desain terhadap kondisi aktual lapangan, penetapan zonasi pembangunan, teknologi kontruksi yang

dipakai, verifikasi spesifikasi pengujian laboratorium dan rencana mutu, verifikasi kuantitas pekerjaan untuk penetapan *mutual check* awal (MC-0). Tahapan konstruksi adalah tahapan untuk pembangunan fisik, dan tahapan pasca konstruksi adalah masa untuk serah terima bangunan.

e) Operasi dan Pemeliharaan
Tahap operasi dan pemeliharaan adalah masa pemanfaatan aset fisik.

8) Pemanfaatan teknologi digital dalam pengelolaan data digital infrastruktur

a) Klasifikasi pemanfaatan teknologi digital untuk pengelolaan data digital infrastruktur yang dapat digunakan untuk setiap tahapan konstruksi adalah:

Tabel 29 Klasifikasi pemanfaatan teknologi digital

| No. | Pemanfaatan Teknologi Digital | Deskripsi Singkat | Tahapan |
|---|---|---|---|
| 1 | Survei kondisi aktual | Kegiatan pengumpulan data eksisting menggunakan *survey* topografi, *drone*, citra satelit, LiDAR atau s*canning* untuk menghasilkan data dan informasi kondisi aktual. | Praperencanaan, Perencanaan, Pengadaan Lahan, Pelaksanaan Konstruksi |
| 2 | Analisis tapak | Kegiatan untuk mengkaji kondisi fisik, lingkungan, dan sosial suatu lokasi guna menentukan potensi, kendala, serta arahan pemanfaatan ruang sebelum perencanaan atau pembangunan dilakukan. | Praperencanaan, Perencanaan, Pengadaan Lahan |
| 3 | Studi kelayakan | Kajian yang dilaksanakan untuk menilai kelayakan pelaksanaan paket pekerjaan. | Praperencanaan |
| 4 | Pembuatan desain konseptual | Kegiatan penyusunan rancangan awal bangunan atau infrastruktur dalam bentuk 2D atau 3D dengan *level of detail* (LOD) 200 yang menggambarkan bentuk, ukuran, dan sistem utama secara konseptual. | Praperencanaan |
| 5 | *Engineering estimate* | Perkiraan biaya proyek berdasarkan dokumen teknis, kuantitas, spesifikasi, dan standar, baik berbasis 2D maupun 3D (BIM) untuk integrasi data. | Perencanaan |
| 6 | Pembuatan Desain Perencanaan (DED) | Penyusunan dokumen teknis lengkap yang memuat rancangan rinci, spesifikasi, kuantitas, dan gambar kerja dalam bentuk 2D atau 3D | Perencanaan |

| No. | Pemanfaatan Teknologi Digital | Deskripsi Singkat | Tahapan |
|---|---|---|---|
| | | (BIM) LOD 300 sebagai dasar pelaksanaan konstruksi. | |
| 7 | Analisis desain | Kajian teknis rancangan proyek untuk menilai performa, efisiensi, dan kepatuhan standar, termasuk analisis energi, sebagai dasar optimasi sebelum konstruksi. | Perencanaan |
| 8 | Deteksi konflik (*clash detection*) | proses identifikasi ketidaksesuaian atau benturan antar elemen dalam model 3D, untuk mencegah kesalahan saat konstruksi. | Perencanaan, Pelaksanaan |
| 9 | Visualisasi/ *mock-up* | Visualisasi model dalam bentuk *render/* animasi/ *prototype* untuk komunikasi desain. | Perencanaan |
| 10 | *Design communication* | Proses tinjauan dan persetujuan desain melalui pertukaran model antar pihak. | Perencanaan |
| 11 | Kolaborasi dan koordinasi dalam CDE | Proses bekerja bersama secara terpusat menggunakan *platform* CDE untuk mengelola, berbagi, dan memverifikasi data proyek sehingga semua tim memiliki informasi yang konsisten dan terintegrasi. | Seluruh Tahapan Konstruksi |
| 12 | Simulasi penjadwalan/ *scheduling (4d simulation)* | Proses menghubungkan model 3D dengan jadwal proyek untuk menguji, mengevaluasi, dan memvisualisasikan urutan kegiatan sebelum dan selama konstruksi, sehingga mempermudah koordinasi dan pengendalian | Pelaksanaan Konstruksi |
| 13 | Perencanaan logistik/ *logistic planning* | Proses merencanakan pergerakan material, peralatan, dan sumber daya di lokasi proyek untuk kelancaran konstruksi. | Pelaksanaan Konstruksi |
| 14 | Perencanaan keselamatan kerja/ *safety planning* | Proses menganalisis dan merencanakan langkah keselamatan di lokasi proyek menggunakan model 2D atau 3D (BIM) untuk mengidentifikasi risiko dan mencegah kecelakaan sebelum dan selama konstruksi. | Pelaksanaan Konstruksi |
| 15 | Pembuatan gambar kerja detail untuk | Proses menghasilkan gambar dan model rinci berbasis 2D atau 3D (BIM) dengan LOD | Pelaksanaan Konstruksi |

| No. | Pemanfaatan Teknologi Digital | Deskripsi Singkat | Tahapan |
|---|---|---|---|
| | konsruksi (*shop drawing*) | 350–400 yang memuat dimensi, sambungan, material, dan detail teknis lapangan. | |
| 16 | Peninjauan desain/*design review* | Proses memeriksa, mengevaluasi, dan memverifikasi rancangan proyek oleh tim internal atau *stakeholder* untuk memastikan kepatuhan terhadap standar, kriteria teknis, keselamatan, dan kelayakan sebelum pelaksanaan konstruksi. | Perencanaan dan Pelaksanaan Konstruksi |
| 17 | Fabrikasi | Proses mengubah desain menjadi komponen fisik dengan menggunakan dokumen 2D atau model 3D (BIM) LOD 400, yang siap dipasang di lokasi konstruksi sesuai spesifikasi dan toleransi desain. | Pelaksanaan Konstruksi |
| 18 | Pembuatan gambar *as-built* | Proses merekam dan memodelkan kondisi aktual infrastruktur atau bangunan beserta informasi aset ke dalam 2D atau 3D (BIM) setelah konstruksi selesai, untuk memastikan data sesuai realisasi di lapangan dan menjadi acuan operasional/*maintenance*. | Pelaksanaan Konstruksi |
| 19 | Manajemen aset/*asset management* 7D | Proses mengelola dan memelihara aset infrastruktur atau bangunan dengan menggunakan sistem manajemen, data aset, penjadwalan pemeliharaan untuk memastikan ketersediaan, kinerja, keamanan, dan umur pakai aset secara optimal. | Operasi dan Pemeliharaan |

b) Detail pemanfaatan teknologi dalam pengelolaan data digital infrastruktur suatu paket pekerjaan diatur lebih lanjut dalam peraturan teknis yang disesuaikan dengan lingkup pekerjaan.

9) Keamanan Data

Data yang diproses, dibangun, diterbitkan, dan disimpan berada pada CDE sesuai dengan ketentuan Manajemen Keamanan SPBE dan ketentuan:

a) Standar keamanan internasional

Standar keamanan internasional setidaknya memenuhi standar sertifikasi ISO 27001 untuk sistem keamanan. Standar keamanan lain dapat dilihat pada *security standards* pada perangkat lunak tersebut.

b) Enkripsi data dan privasi
Semua file yang ada pada media CDE tersimpan pada *cloud* (*cloud* Kementerian maupun ekosistem Pusat Data Nasional) yang sudah terenkripsi. Penyimpanan lanjutan menggunakan enkripsi lanjutan 256-bit (AES-256). Lalu lintas data yang bersifat krusial dikirim dengan enkripsi dengan teknologi *transfer layer security*.

c) Akses kontrol
Akses yang memiliki metode kendali akses berbasis peran yang membatasi akses tertentu ke sumber daya informasi. Otorisasi dalam aksesibilitas memerlukan persetujuan dari pengguna jasa yang bertanggung jawab atas kerahasiaan, integritas, dan ketersediaan.

d) Keamanan data fisik
Pusat Data dilindungi dari akses fisik yang membahayakan dengan rangkaian kontrol keamanan sesuai standar ISO 27001 dan ISO 20000-1.

10) Manajemen Risiko Pengelolaan Data Digital Infrastruktur
Manajemen risiko merupakan proses identifikasi, penilaian, pengelolaan, dan pengendalian terhadap potensi risiko yang dapat memengaruhi kualitas, keamanan, ketersediaan, dan keterpaduan data digital infrastruktur.

d. Daftar Data Yang Telah Ditentukan Dalam Forum Satu Data Kementerian

1) Data Digital Infrastruktur minimum untuk setiap tahapan konstruksi adalah sebagai berikut:

a) Tahapan Pra-perencanaan
Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(1) Data Kontur.
(2) Data *Orthophoto.*
(3) Rencana Tapak.
(4) Informasi Geometrik konseptual berupa pemodelan 3D LOD 200; dan
(5) Laporan kelayakan paket pekerjaan.

b) Tahap Perencanaan
Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(1) Data Kontur.
(2) Data *Orthophoto*.
(3) Data Hasil Investigasi Tanah.

(4) Gambar DED.
(5) Informasi Geometrik (DED) berupa permodelan 3D LOD 300 yang terkoneksi dengan gambar 2D.
(6) Infomasi *Engineering Estimate* sudah terkoneksi secara digital dengan kuantitas volume dalam BIM (5D).
(7) *Mock-Up* / Visualisasi; dan
(8) Laporan Konflik dan Model Koordinasi (*Clash Detection*).

c) Tahapan Pengadaan Lahan

Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(1) Data Batas Lahan; dan
(2) Data *Orthophoto*.

d) Tahapan Konstruksi

(1) Pra Konstruksi

Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(a) Informasi model 3D LOD 350-400 yang terkoneksi dengan jadwal dan progres pekerjaan; dan
(b) Informasi model 3D LOD 350-400 yang terkoneksi dengan biaya.

(2) Konstruksi

Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(a) Gambar *Shop Drawing*;
(b) Informasi geometrik *update* 3D LOD 350-400 yang terkoneksi dengan gambar 2D.
(c) Informasi geometrik *update* 3D LOD 350-400 yang terkoneksi dengan jadwal dan progres pekerjaan (4D).
(d) Informasi geometrik *update* 3D LOD 350-400 yang terkoneksi dengan biaya (5D).
(e) Dokumentasi pekerjaan di lapangan.
(f) *Reality Capture* baik menggunakan Lidar atau Fotogrametri sesuai dengan progres pekerjaan; dan
(g) Data hasil kontrol kualitas selama proses konstruksi.

(3) Pasca kontruksi

Data yang dihasilkan pada tahapan ini adalah sebagai berikut:
(a) Gambar *as-built drawing*.
(b) Informasi Geometrik berupa pemodelan 3D LOD 500.
(c) Data dan Informasi Aset.
(d) BIM *Library.*
(e) *Reality Capture* baik menggunakan Lidar atau Fotogrametri progres100%.
(f) Dokumentasi pekerjaan di lapangan; dan

(g) Data hasil kontrol kualitas selama proses konstruksi.

e) Tahapan Operasional dan Pemeliharaan

Data yang dihasilkan pada tahapan ini adalah sebagai berikut:

(1) Gambar a*s-built drawing update*.
(2) Informasi *update* 3D LOD 500; dan
(3) Data dan Informasi Aset *update*.

f) Data Tambahan

Data tambahan merupakan kumpulan dokumen pendukung yang diatur dalam Kerangka Acuan Kerja (KAK) paket pekerjaan untuk melengkapi keseluruhan tahapan paket pekerjaan. Jenis data tambahan yang dimaksud meliputi dokumen legal dan administratif, seperti *exchange information requirement* (EIR), *BIM execution plan* (BEP), surat izin pelaksanaan paket pekerjaan, dokumen kontrak dan adendum, berita acara hasil pekerjaan, laporan, notula, serta dokumen audit dan persetujuan resmi terkait paket pekerjaan.

e. Standar Data dan Meta Data

1) Persyaratan data digital infrastruktur minimum pada setiap tahapan kontruksi adalah sebagai berikut:

a) Praperencanaan

Tabel 30 Persyaratan data digital infrastruktur minimum pada tahap praperencanaan

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Data kontur | Data elevasi permukaan tanah hasil survei topografi atau pengolahan data LiDar, untuk analisis kemiringan lahan, perencanaan *drainase*, dan perhitungan volume tanah. | CAD dan/atau SHP | Semua paket |
| 2 | Data *Orthophoto* | Citra udara hasil pemotretan *drone* atau satelit yang telah terkoreksi geometrik, menampilkan kondisi aktual permukaan tanah dan objek secara spasial akurat, sebagai dasar pemetaan dan pemodelan (minimal resolusi 0,1 meter) | GeoTIFF | Semua paket |
| 3 | Rencana Tapak | Laporan analisis tapak, kontur, elevasi, dan batas lahan untuk menentukan potensi dan kendala tapak. | PDF, SHP, KML, dan/atau KMZ | Semua paket |
| 4 | Informasi Geometrik konseptual berupa | Model tiga dimensi awal yang menampilkan bentuk umum, dimensi, dan hubungan spasial antar elemen bangunan atau infrastruktur | *Native File* dan/atau IFC | Paket BIM |

| | | | | |
|---|---|---|---|---|
| | pemodelan 3D LOD 200 | untuk studi kelayakan desain, analisis ruang, dan komunikasi konsep antar-disiplin. | | |
| 5 | Laporan kelayakan paket pekerjaan | Laporan kajian kelayakan teknis, ekonomi, dan lingkungan berdasarkan model konseptual. | PDF | Semua paket |

b) Perencanaan

Tabel 31 Persyaratan data digital infrastruktur minimum pada tahap perencanaan

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Data kontur | Data elevasi permukaan tanah hasil survei topografi atau pengolahan data LiDar, untuk analisis kemiringan lahan, perencanaan *drainase*, dan perhitungan volume tanah. | CAD, SHP, KML dan/atau KMZ | Semua paket |
| 2 | Data *Ortophoto* | Citra udara hasil pemotretan *drone* atau satelit yang telah terkoreksi geometrik, menampilkan kondisi aktual permukaan tanah dan objek secara spasial akurat, sebagai dasar pemetaan dan pemodelan (minimal resolusi 0,1 meter) | GeoTIFF | Semua paket |
| 3 | Data hasil investigasi tanah | Hasil investigasi tanah yang mencakup parameter geoteknik untuk analisis pondasi dan perencanaan struktur bawah. | PDF, Data Tabular, dan/atau SHP | Semua paket |
| 4 | Gambar DED | Gambar perencanaan teknis rinci yang disusun berdasarkan hasil desain dasar (*preliminary design*) dan menjadi acuan utama dalam proses pelaksanaan konstruksi. | PDF dan/atau CAD | Semua Paket |
| 5 | Informasi Geometrik (DED) berupa permodelan 3D LOD 300 yang terkoneksi dengan gambar 2D. | Model 3D rinci multi-disiplin yaitu:<br>a. arsitektur<br>b. struktur<br>c. mekanikal, elektrikal, dan *plumbing* (MEP)<br>yang terkoneksi dengan gambar 2D sebagai dasar desain teknis. | *Native File* dan/atau IFC | Paket BIM |
| 6 | Infomasi *Engineering Estimate* sudah terkoneksi secara digital dengan | Informasi estimasi biaya pekerjaan yang sudah terhubung secara digital dengan model 3D, termasuk data volume dan item pekerjaan untuk pengendalian biaya. | *Native File*, IFC, dan/atau Data Tabular | Paket BIM |

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| | kuantitas volume dalam BIM (5D). | | | |
| 7 | Visualisasi / *Mock-Up* | Model representatif dengan tingkat detail tinggi untuk menunjukkan tampilan akhir desain secara visual dan realistis, digunakan untuk persetujuan desain dan komunikasi paket pekerjaan. | PDF, format gambar raster, dan/atau .mp4 | Semua paket |
| 8 | Laporan Konflik dan Model Koordinasi (*Clash Detection*) | Dokumen hasil analisis deteksi benturan antar disiplin (arsitektur, struktur, MEP, dan disiplin lainnya), beserta model koordinasi terintegrasi untuk perbaikan desain. | PDF dan/atau *Native File* | Paket BIM |

c) Pengadaan lahan

Tabel 32 Persyaratan data digital infrastruktur minimum pada tahap pengadaan lahan

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Data batas lahan | Data koordinat dan luas batas administrasi atau kepemilikan lahan sebagai dasar perencanaan dan pengelolaan kawasan paket pekerjaan. | SHP, PDF, CAD, KML, dan/atau KMZ | Semua Paket |
| 2 | Data *Orthophoto* | Citra udara yang telah terkoreksi geometrik dan memiliki sistem koordinat spasial, digunakan untuk pemetaan akurat kondisi eksisting lokasi paket pekerjaan (minimal resolusi 0,1 meter). | GeoTIFF | Semua Paket |

d) Konstruksi

(1) Pra Konstruksi

Tabel 33 Persyaratan data digital infrastruktur minimum pada tahap pra kontruksi

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Informasi model 3D LOD 350-400 yang terkoneksi dengan jadwal dan progres pekerjaan | Model tiga dimensi detail yang telah terintegrasi dengan jadwal pelaksanaan dan data progres aktual pekerjaan untuk memantau pelaksanaan konstruksi secara visual berbasis waktu. | *Native File* dan/atau IFC | Paket BIM |

| | | | | |
|---|---|---|---|---|
| 2 | Informasi model 3D LOD 350-400 yang terkoneksi dengan biaya | Model 3D yang telah terhubung dengan data estimasi dan realisasi biaya pekerjaan, digunakan untuk analisis pengendalian biaya konstruksi. | *Native File* dan/atau IFC | Paket BIM |

(2) Konstruksi

Tabel 34 Persyaratan data digital infrastruktur minimum pada tahap kontruksi

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Gambar *Shop Drawing*. | Gambar kerja teknis rinci yang digunakan sebagai acuan pelaksanaan di lapangan, disusun berdasarkan DED. | CAD dan/atau PDF | Semua Paket |
| 2 | Informasi *update* 3D LOD 350-400 yang terkoneksi dengan gambar 2D. | Model tiga dimensi terkini yang merepresentasikan perubahan desain dan telah terhubung dengan gambar 2D terbaru. | *Native File* dan/atau IFC | Paket BIM |
| 3 | Informasi *update* 3D LOD 350-400 yang terkoneksi dengan jadwal dan progres pekerjaan (4D) | Model ter-*update* yang mencerminkan perkembangan pekerjaan dan jadwal aktual konstruksi berdasarkan progres lapangan. | *Native File* dan/atau IFC | Paket BIM |
| 4 | Informasi *update* 3D LOD 350-400 yang terkoneksi dengan biaya (5D) | Model ter-*update* yang terhubung dengan estimasi dan realisasi biaya pekerjaan berdasarkan progres pelaksanaan. | *Native File* dan/atau IFC | Paket BIM |
| 5 | Dokumentasi pekerjaan di lapangan | Dokumentasi foto dan video pelaksanaan pekerjaan di lapangan sebagai bukti progres konstruksi. | PDF, JPG, dan/atau MP4 | Semua Paket |
| 6 | *Reality Capture* baik menggunakan Lidar atau Fotogrametri sesuai dengan progres pekerjaan | Data hasil pemindaian spasial (3D *scan*) atau pemotretan udara yang menggambarkan kondisi aktual pekerjaan di lapangan secara berkala. | LAS, OBJ, GeoTIFF, *Native File* dan/atau IFC | Semua Paket |
| 7 | Data hasil kontrol kualitas | Hasil uji mutu material seperti beton, baja, pondasi, dan komponen lainnya | PDF dan/atau | Semua Paket |

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| | selama proses konstruksi. | untuk memastikan kesesuaian spesifikasi teknis. | Data Tabular | |

(3) Pasca konstruksi

Tabel 35 Persyaratan data digital infrastruktur minimum pada tahap pasca kontruksi

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Gambar a*s-built Drawing* | Gambar akhir hasil pelaksanaan yang menunjukkan kondisi aktual konstruksi setelah selesai dibangun. | CAD dan/atau PDF | Semua Paket |
| 2 | Informasi geometrik berupa pemodelan 3D LOD 500. | Model tiga dimensi akhir (*as-built model*) yang merepresentasikan kondisi aktual infrastruktur secara lengkap untuk mendukung operasi dan pemeliharaan. | *Native File* dan/atau IFC | Paket BIM |
| 3 | Data dan Informasi Aset | Data identitas dan kondisi aset infrastruktur untuk pemeliharaan aset. | Data tabular PDF dan/atau SHP | Semua Paket |
| 4 | BIM *Library* | Kumpulan objek atau komponen standar BIM yang berisi parameter teknis. | *Native File* dan/atau IFC | Paket BIM |
| 5 | *Reality Capture* baik menggunakan LiDar atau Fotogrametri progres 100% | Data hasil pemindaian akhir (setelah pekerjaan selesai) untuk validasi model *as-built* dan dokumentasi paket pekerjaan akhir. | LAS, OBJ, GeoTIFF, *Native File*, dan/atau IFC | Semua Paket |
| 6 | Dokumentasi pekerjaan di lapangan | Dokumentasi foto dan video pelaksanaan pekerjaan di lapangan sebagai bukti progres konstruksi. | Format gambar raster dan/atau MP4 | Semua Paket |
| 7 | Data hasil kontrol kualitas selama proses konstruksi | Laporan akhir hasil pengujian material dan struktur sebagai bagian dari proses serah terima pekerjaan. | PDF dan/atau Data Tabular | Semua Paket |

(4) Operasional dan Pemeliharaan

Tabel 36 Persyaratan data digital infrastruktur minimum pada tahap operasional pemeliharaan

| No. | Jenis Data | Deskripsi | Format | Keterangan |
|---|---|---|---|---|
| 1 | Gambar *As-Built Drawing update* | Gambar hasil pembaruan berdasarkan kondisi akhir paket pekerjaan setelah penyesuaian atau perbaikan pasca konstruksi. | CAD dan/atau PDF | Semua Paket |
| 2 | Informasi *update* 3D LOD 500 | Model *as-built* yang diperbarui untuk mencerminkan kondisi aktual terkini dari infrastruktur yang telah selesai dibangun. | *Native File* dan/atau IFC | Paket BIM |
| 3 | Data dan Informasi Aset *update* | Data pemutakhiran aset infrastruktur meliputi perubahan fungsi, kondisi, atau lokasi untuk mendukung operasi dan pemeliharaan berkelanjutan. | Data tabular, PDF, dan/atau SHP | Semua Paket |

2) Metadata dan Struktur Data

Tabel 37 Metadata dan Struktur Data

| No. | Atribut | Deskripsi | Contoh pengisian | Jenis | Maks. Jumlah Karakter |
|---|---|---|---|---|---|
| 1 | Nama Objek/ Barang | Nama atau identifikasi utama dari elemen atau komponen infrastruktur yang dimodelkan | Panel Listrik Utama Gedung A | Teks | 50 |
| 2 | Parameter Teknis | Informasi teknis utama dari objek, meliputi dimensi, kapasitas, atau spesifikasi kerja | Panjang 25 m, Lebar 6 m, Kapasitas 10 ton | Teks/angka | 50 |
| 3 | Kode RAB | Kode kegiatan atau item pekerjaan sesuai daftar Rencana Anggaran Biaya paket pekerjaan | JAL-04-01 | Teks | 20 |
| 5 | Referensi Standar | Acuan standar atau regulasi teknis yang digunakan dalam desain atau pelaksanaan | SNI 1725:2016 | Teks | 100 |
| 6 | Spesifikasi material | Jenis dan mutu material utama yang | Beton fc'=25 MPa | Teks | 255 |

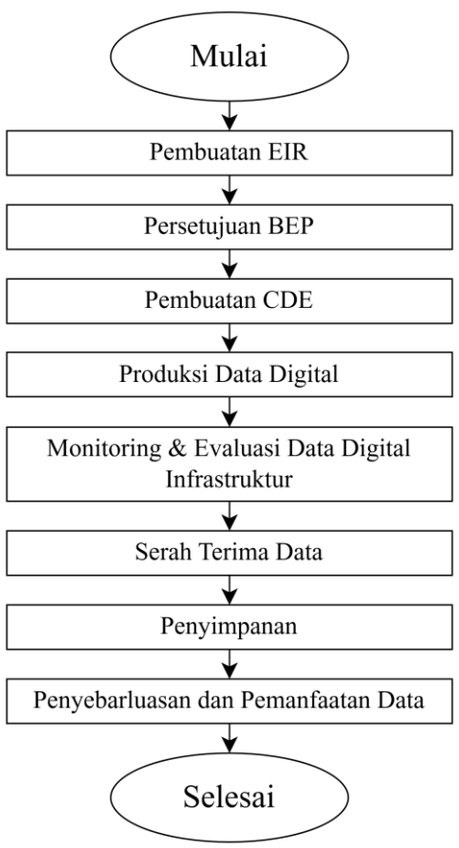
| No. | Atribut | Deskripsi | Contoh pengisian | Jenis | Maks. Jumlah Karakter |
|---|---|---|---|---|---|
| | | digunakan dalam objek atau komponen | | | |
| 7 | Mata Pembayaran | Nomor atau kode pembayaran sesuai dokumen kontrak atau daftar kuantitas pekerjaan | 1.3.02.001 – Pekerjaan Beton Bertulang | Teks | 255 |
| 8 | Informasi Sistem Objek | Klasifikasi sistem atau subsistem tempat objek tersebut berada (mis. struktur, MEP, arsitektur, utilitas) | Jaringan Air Limbah | Teks | 255 |
| 9 | Merk | Nama merk dagang dari material, peralatan, atau komponen yang digunakan | Daikin / Fuji / Toto | Teks | 255 |
| 10 | Nama *Vendor/Supplier* | Nama penyedia atau pemasok material atau komponen | PT Krakatau Steel | Teks | 255 |
| 12 | Material *Approval* | Status persetujuan material dari pengguna jasa atau konsultan pengawas | Disetujui/Menunggu Persetujuan/Revisi | Teks (*Boolean*) | 25 |
| 13 | Rencana Instalasi Mulai | Tanggal yang direncanakan untuk memulai pemasangan material, peralatan, atau komponen sesuai jadwal kerja | 15-07-2025 | Tanggal (DD-MM-YYYY) | 10 |
| 14 | Rencana Instalasi Selesai | Tanggal yang direncanakan untuk menyelesaikan seluruh kegiatan instalasi sesuai jadwal perencanaan | 15-07-2025 | Tanggal (DD-MM-YYYY) | 10 |
| 15 | Realisasi Instalasi Mulai | Tanggal aktual dimulainya kegiatan instalasi di lapangan berdasarkan laporan pelaksanaan pekerjaan | 15-07-2025 | Tanggal (DD-MM-YYYY) | 10 |
| 16 | Realisasi Instalasi Selesai | Tanggal aktual selesainya kegiatan instalasi di lapangan berdasarkan hasil pemeriksaan atau laporan penyelesaian pekerjaan | 15-07-2025 | Tanggal (DD-MM-YYYY) | 10 |

| No. | Atribut | Deskripsi | Contoh pengisian | Jenis | Maks. Jumlah Karakter |
|---|---|---|---|---|---|
| 17 | Persentase TKDN | Persentase komponen TKDN pada aset. | 90% / 70% | Angka | 10 |
| 18 | Jenis BMN | Jenis Barang Milik Negara sesuai klasifikasi aset | Peralatan/Mesin | Teks | 255 |
| 19 | Kode Satker | Kode satuan kerja pengelola atau pemilik aset | 0330xxxxxx | Teks | 255 |
| 20 | Nama Satker | Nama lengkap satuan kerja pengelola aset atau pekerjaan | Balai Besar Wilayah Sungai Brantas | Teks | 255 |
| 21 | Kode Barang | Kode klasifikasi barang sesuai daftar BMN (kodefikasi SIMAK BMN) | 3.05.02.04.002 | Angka | 30 |
| 22 | Nomor Urut Pendaftaran (NUP) | Nomor unik aset di dalam satu satuan kerja | 16 | Angka | 30 |
| 23 | Tipe | Tipe atau model dari peralatan atau komponen teknis | Type T-25C | Teks | 255 |
| 24 | Kondisi | Status fisik barang saat ini (Baik/Rusak Ringan/Rusak berat) | Baik | Teks dan/ boolean | 10 |
| 25 | Tanggal perolehan | Tanggal pertama kali aset diperoleh atau diterima | 15-07-2025 | Tanggal (DD-MM-YYYY) | 10 |
| 26 | Tahun Pengadaan | Tahun aset diperoleh berdasarkan kontrak atau pembelian | 2025 | Angka | 4 |
| 27 | Lokasi Aset | Alamat lengkap terdiri dari Jalan, RT, RW, Kelurahan, Kecamatan, Kab/Kota, Provinsi | Jl. Pattimura No. 20 RT 02, RW 01, Selong, Kec. Kebayoran Baru, Kota Jakarta Selatan, DKI Jakarta | Teks | 255 |
| 28 | Koordinat Lokasi Aset | Informasi posisi geografis suatu aset yang dinyatakan dalam sistem koordinat geografis dengan referensi datum geodetik WGS 1984, menggunakan format derajat | 6.076,95.012 | Angka | 20 |

| No. | Atribut | Deskripsi | Contoh pengisian | Jenis | Maks. Jumlah Karakter |
|---|---|---|---|---|---|
| | | desimal (3 angka belakang koma) yang terdiri atas nilai lintang dan bujur. | | | |

f. Jadwal pemutakhiran data atau rilis data
Jadwal pemutakhiran dan rilis data digital infrastruktur bersifat dinamis, mengikuti perkembangan tahapan paket pekerjaan serta sesuai dengan kebijakan Forum Satu Data Kementerian dan produsen data.

g. Prosedur Pengelolaan Data dan informasi Digital Infrastruktur
1) Prosedur Pengelolaan Data dan Informasi Digital Infrastruktur untuk paket pekerjaan yang mengimplementasikan BIM mencakup Pembuatan EIR, Persetujuan BEP, Pembuatan CDE, Produksi Data Digital, Monitoring dan Evaluasi Data Digital Infrastruktur, Serah Terima Data, Penyimpanan, Penyebarluasan dan Pemanfaatan Data, sebagaimana tercantum dalam gambar berikut:




Gambar 16 Prosedur Pengelolaan Data dan informasi Digital Infrastruktur

2) Apabila paket pekerjaan pekerjaan tidak menerapkan BIM, maka penyusunan EIR dan BEP tidak diperlukan.

3) Prosedur pengelolaan data digital infrastruktur secara detail adalah sebagai berikut :

a) Penyusunan EIR

(1) Langkah penyusunan EIR mencakup

(a) Produsen data menetapkan kebutuhan data dan informasi yang harus tersedia.

(b) Produsen data mendefinisikan format, struktur, tingkat kedetailan/LOD, standar penamaan, jadwal pengiriman data, serta menyusun dokumen EIR.

(2) Ketentuan EIR

EIR berisikan kebutuhan informasi minimum data digital infrastruktur minimal mencakup:

(a) Ruang lingkup model BIM dan jenis data yang harus disediakan.

(b) Model BIM minimal yang harus dapat digunakan untuk:

i. Visualisasi 3D lintas disiplin.

ii. Deteksi benturan antar elemen (*clash detection*); dan

iii. Perkiraan kebutuhan biaya paket pekerjaan (*engineering estimate*).

(c) Daftar kebutuhan informasi.

(d) Standar format file dan metadata wajib.

(e) Target LOD dan LOI per tahapan.

(f) Jadwal pengiriman data dan hasil BIM pada tiap tahapan konstruksi; dan

(g) Persyaratan keamanan dan hak akses data.

b) Persetujuan BEP

(1) Langkah persetujuan BEP mencakup

(a) Penyedia Jasa menyusun pra-BEP sebagai respon dari EIR.

(b) Produsen Data memilih BEP yang paling sesuai dengan kebutuhan dalam pelaksanaan BIM.

(c) Produsen Data dan penyedia jasa terpilih meninjau dan menyepakati *post* BEP sebagai panduan dalam pelaksanaan BIM dalam paket pekerjaan.

(2) Ketentuan BEP mencakup:

(a) Tujuan dan ruang lingkup BIM.

(b) Peran dan tanggung jawab tim BIM.

(c) *Level of Detail* (LOD) dan *Level of Information* (LOI).

(d) Standar, prosedur, dan format data.

(e) Pengaturan *Common Data Environment* (CDE).

(f) Jadwal pengiriman model dan dokumen BIM.

(g) Proses *Quality Assurance* (QA)/ *Quality Control* (QC) dan validasi model.

(h) Proses koordinasi antar disiplin.

(i) Keamanan dan kontrol akses data.
(j) Dokumentasi dan arsip digital proyek.

c) Pembuatan CDE
Langkah pembuatan CDE mencakup:
(1) Koordinator Produsen Data berkoordinasi dengan Produsen Data dalam hal menyediakan CDE untuk seluruh data digital paket pekerjaan.
(2) Produsen Data mengatur hak akses, alur kerja, dan versi data.
(3) Koordinator Produsen Data menjamin keterlacakan dan keamanan data selama paket pekerjaan berlangsung.

d) Produksi Data Digital
Langkah produksi data digital mencakup:
(1) Produsen Data melaksanakan pembuatan dan pengumpulan data digital sesuai EIR dan BEP termasuk proses pemodelan BIM, digitalisasi gambar 2D, pengumpulan data lapangan, dan integrasi spasial sesuai dengan standar data dan meta data.
(2) Hasil produksi harus memenuhi standar format dan struktur data yang telah ditetapkan.

e) *Monitoring* dan Evaluasi Data Digital
Langkah Monitoring dan Evaluasi Data mencakup:
(1) Koordinator Produsen data membuat *Key Performance Indicator* (KPI) untuk pengelolaan data digital infrastruktur.
(2) Koordinator Produsen data melakukan pemeriksaan data sesuai KPI yang dibuat.
(3) Koordinator Produsen Data membuat Berita Acara Hasil Monitoring dan evaluasi data digital.

f) Serah Terima Data
(1) Serah Terima Data mencakup penyerahan data secara resmi dengan disertai data hasil tahap pascakonstruksi dan operasi dan pemeliharaan.
(2) Proses ini memastikan tanggung jawab dan status validasi data terdokumentasi dengan jelas.

g) Penyimpanan Data
Data disimpan pada CDE dan dikelola secara bersama oleh Wali Data kementerian serta Koordinator Produsen Data.

h) Penyebarluasan dan Pemanfaatan Data
Langkah Penyebarluasan dan Pemanfaatan Data mencakup
(1) Data digital yang telah tervalidasi dapat diakses untuk keperluan perencanaan, pelaksanaan, pengawasan, dan operasi-pemeliharaan.
(2) Penyebarluasan dilakukan melalui sistem integrasi.
(3) Pemanfaatan data harus memperhatikan hak akses dan ketentuan keamanan informasi.

10. Data dan informasi lainnya yang dikelola oleh Kementerian
    Pengaturan data dan informasi lainnya yang dikelola oleh Kementerian mengikuti ketentuan peraturan perundang-undangan yang berlaku.

D. MANAJEMEN ASET TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK)

1. Perencanaan Aset TIK
    a. Perencanaan aset TIK dilakukan pada anggaran tahun sebelumnya, kecuali untuk kebutuhan TIK yang bersifat mendesak dapat dibuat perencanaannya pada tahun anggaran yang berjalan dengan mendapat persetujuan Tim Pengarah SPBE.
    b. Pusdatin membuat perencanaan aset TIK Kementerian berdasarkan arsitektur SPBE dan Peta Rencana SPBE Kementerian.
    c. Unit Organisasi, Unit Kerja, dan UPT membuat perencanaan aset TIK berdasarkan arsitektur SPBE dan Peta Rencana SPBE Unit Organisasi.
    d. Unit Organisasi, Unit Kerja, dan UPT melakukan koordinasi dengan Pusdatin dalam membuat perencanaan aset TIK untuk menghindari duplikasi pengadaan aset TIK.
    e. Pusdatin melakukan kompilasi seluruh perencanaan aset TIK di Kementerian, serta memastikan tidak terjadi duplikasi perencanaan aset TIK yang bisa berbagi-pakai di Kementerian sebelum menjadi rencana kerja TIK Kementerian tahun berikutnya dan menjadi Daftar Isian Pelaksanaan Anggaran (DIPA).
    f. Sebelum ditetapkan menjadi DIPA, rencana kerja TIK Unit Organisasi, Unit Kerja, dan UPT harus mendapatkan persetujuan dari Pusdatin.
    g. Perencanaan aset TIK harus menjelaskan fungsi-fungsi utama, justifikasi bisnis dan teknis dari aset yang akan diadakan, manfaat (*outcome*), keluaran (*output*), strategi pengadaan, perkiraan anggaran, serta sumber daya manusia dan waktu yang diperlukan, pada setiap Kerangka Acuan Kerja (KAK).

2. Pengadaan Aset TIK
    a. Setiap kegiatan pengadaan aset TIK didahului dengan rencana kebutuhan aset TIK.
    b. Pengadaan aset TIK dilakukan berdasarkan DIPA dan sesuai dengan ketentuan peraturan perundang-undangan.
    c. Pengadaan aset TIK yang melibatkan pihak di luar Kementerian, baik badan usaha maupun individual, untuk tenaga ahli diwajibkan memiliki sertifikat keahlian yang sesuai dengan kebutuhan.
    d. Pengadaan, penerimaan, verifikasi, pengujian, dan pencatatan semua aset TIK dilakukan dengan cara yang terkontrol, termasuk pelabelan fisik sesuai dengan ketentuan peraturan perundang-undangan.

e. Menyetujui pembayaran dan menyelesaikan proses dengan penyedia barang/jasa sesuai dengan kondisi kontrak yang disepakati.
f. Melakukan penempatan & pengalokasian aset TIK sesuai dengan standar siklus hidup pengelolaan barang milik negara, termasuk manajemen perubahan dan pengujian penerimaan.
g. Melakukan realokasi aset ketika tidak lagi diperlukan karena perubahan peran pengguna, pergandaan aset dalam suatu layanan, atau penghapusan/berhentinya suatu layanan.

3. Pengelolaan Aset TIK Vital
   a. Aset TIK Vital disepakati dan ditetapkan bersama antara Unit Organisasi dengan Pusdatin.
   b. Identifikasi aset TIK vital dapat merujuk pada kebutuhan kapabilitas layanan, ketersediaan layanan (*Service Level Agreement* - SLA) dan ketentuan lain sesuai dengan peraturan perundang-undangan yang berlaku.
   c. Pengelolaan Aset TIK Vital mempertimbangkan risiko kegagalan atau kebutuhan untuk penggantian setiap aset TIK vital secara teratur.
   d. Pengelolaan Aset TIK Vital dikomunikasikan dengan pengguna yang terpengaruh (misalnya pembatasan kinerja) dari aktivitas pemeliharaan.
   e. Menggabungkan *downtime* yang direncanakan dalam jadwal produksi keseluruhan serta menjadwalkan kegiatan pemeliharaan untuk meminimalkan dampak gangggua pada layanan yang didukung oleh aset TIK vital.
   f. Memelihara ketahanan aset TIK dengan menerapkan pemeliharaan preventif yang teratur serta memantau kinerja dan jika diperlukan, memberikan aset TIK alternatif dan/atau cadangan untuk meminimalkan kemungkinan kegagalan.
   g. Menetapkan rencana pemeliharaan preventif untuk semua perangkat keras, mempertimbangkan analisis biaya/manfaat, rekomendasi pihak di luar Kementerian, risiko gangguan layanan, personel yang berkualifikasi, dan faktor-faktor terkait lainnya.
   h. Menetapkan perjanjian pemeliharaan yang melibatkan akses pihak di luar Kementerian ke fasilitas TIK Kementerian untuk aktivitas di lokasi dan di luar lokasi berupa kontrak layanan formal yang berisi atau merujuk pada semua kondisi keamanan dan privasi yang dipersyaratkan, termasuk prosedur otorisasi akses.
   i. Memastikan bahwa layanan akses jarak jauh dan profil pengguna hanya aktif bila diperlukan.
   j. Memantau kinerja aset TIK vital dengan memeriksa tren insiden dan jika diperlukan, pengelola mengambil tindakan untuk memperbaiki atau mengganti aset TIK terkait.

4. Pengelolaan Nilai Aset TIK
   a. Meninjau seluruh aset TIK secara berkala dan mempertimbangkan apakah aset TIK tersebut masih selaras dengan kebutuhan Kementerian.
   b. Melakukan asesmen terkait biaya pemeliharaan dengan mempertimbangkan kewajaran, dan identifikasi opsi biaya yang lebih rendah, termasuk penggantian dengan alternatif baru.
   c. Mempertimbangkan nilai aset TIK dan strategi penggantian aset TIK untuk menentukan opsi biaya terendah.
   d. Melakukan pengukuran kapasitas dan pemanfaatan aset TIK untuk mengidentifikasi aset TIK yang kurang bermanfaat atau terjadi pergandaan yang tidak perlu, sehingga dapat dipertimbangkan untuk dihapus atau diganti dalam rangka pengurangan efisiensi biaya.
   e. Meninjau seluruh aset TIK untuk mengidentifikasi peluang yang dapat menurunkan biaya pengadaan, dukungan, dan pemeliharaan sesuai dengan ketentuan peraturan perundang-undangan.
   f. Melakukan kajian untuk mengidentifikasi peluang pemanfaatan teknologi baru.

5. Pengelolaan Lisensi
   a. Mengelola daftar lisensi perangkat lunak yang dibeli beserta perjanjian lisensinya.
   b. Secara berkala, melakukan audit untuk mengidentifikasi semua komponen (*instances*) perangkat lunak berlisensi yang digunakan.
      1) Membandingkan jumlah *instances* perangkat lunak yang digunakan dengan jumlah lisensi yang dimiliki dan memastikan penggunaan lisensi sesuai dengan kontrak.
      2) Ketika jumlah *instances* lebih rendah dari jumlah lisensi yang dimiliki, tentukan apakah mempertahankan atau menghentikan lisensi dengan mempertimbangkan pemeliharaan, pelatihan dan biaya lain yang tidak perlu.
      3) Ketika jumlah *instances* lebih tinggi dari jumlah lisensi yang dimiliki, lakukan *uninstall instances* yang tidak lagi diperlukan, dan kemudian jika perlu beli lisensi tambahan untuk mematuhi perjanjian lisensi.
   c. Secara teratur, mempertimbangkan apakah nilai yang lebih baik dapat diperoleh dengan *upgrade* produk dan lisensi terkait.

6. Pencatatan Aset TIK
   a. Mengidentifikasi semua aset TIK yang dimiliki dalam daftar aset TIK termasuk catatan status saat ini dan melaporkan aset TIK sesuai dengan ketentuan peraturan perundang-undangan.
   b. Mengidentifikasi persyaratan hukum, peraturan, atau kontrak yang perlu dipatuhi ketika mengelola aset TIK sesuai dengan ketentuan peraturan perundang-undangan.

c. Melakukan verifikasi untuk memastikan bahwa penggunaan aset TIK sesuai dengan tujuannya.
d. Memastikan pertanggungjawaban pada semua aset TIK.
e. Memverifikasi keberadaan semua aset TIK yang dimiliki dengan melakukan pemeriksaan dan rekonsiliasi persediaan fisik dan logis secara teratur, termasuk penggunaan alat bantu untuk mengetahui status dan keberadaan perangkat lunak.
f. Memeriksa secara teratur untuk memastikan apakah setiap aset TIK masih memberikan nilai dan memperkirakan masa pakai aset TIK sesuai dengan ketentuan peraturan perundang-undangan.

7. Penghapusan Aset TIK
   a. Merencanakan, memberikan wewenang dan menerapkan kegiatan terkait penghapusan aset TIK serta mengelola daftar aset TIK yang sesuai dengan kebutuhan layanan dan ketentuan peraturan perundang-undangan.
   b. Menghapus aset TIK yang sudah tidak bermanfaat karena penghapusan/penghentian/penggabungan layanan terkait, teknologi yang sudah usang, kurangnya pengguna, atau dampak lingkungan akibat penggunaan teknologi tersebut.
   c. Menghapus aset TIK dengan aman sesuai dengan ketentuan keamanan informasi SPBE dan peraturan perundangan-undangan.
   d. Penghapusan aset TIK dari daftar Barang Milik Negara (BMN) sesuai dengan ketentuan peraturan perundangan-undangan.

E. MANAJEMEN SUMBER DAYA MANUSIA (SDM)

1. Perencanaan Komptensi SDM
   a. Pusdatin bersama Unit Datin melakukan inventarisasi SDM SPBE yang telah dimiliki dan menganalisis kebutuhan kompetensi SDM SPBE di masa mendatang dengan mengacu kepada pada inisiatif SPBE saat ini, target arsitektur SPBE, kebutuhan operasional sehari-hari, dan Peta Rencana SPBE Kementerian.
   b. Pusdatin bersama Unit Datin mereviu hasil inventarisasi kompetensi dan analisis kebutuhan kompetensi SDM SPBE, untuk:
      1) Kebutuhan pengembangan kompetensi yang bersifat umum yang diperlukan oleh lintas unit organisasi, Pusdatin mengusulkan kepada Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum untuk menyelenggarakan pengembangan kompetensi SDM SPBE sesuai ketentuan peraturan perundang-undangan.
      2) Kebutuhan pengembangan kompetensi yang bersifat spesifik untuk kebutuhan Unit Organisasi dikelola dan dilaksanakan oleh Unit Datin sesuai ketentuan peraturan perundang-undangan.
   c. Pusdatin memantau pelaksanaan pengembangan kompetensi SDM SPBE yang bersifat umum dan lintas organisasi.

d. Unit Datin memantau pelaksanaan pengembangan kompetensi SDM SPBE yang bersifat spesifik untuk kebutuhan Unit Organisasi.
e. Unit Datin menyampaikan laporan evaluasi pelaksanaan pengembangan kompetensi SDM SPBE Unit Organisasi masing-masing secara periodik kepada Pusdatin.
f. Pusdatin mengkompilasi laporan perencanaan dan pelaksanaan pengembangan kompetensi SDM SPBE Kementerian.
g. Pusdatin menyampaikan laporan evaluasi pelaksanaan pengembangan kompetensi SDM SPBE Kementerian secara periodik kepada Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum tembusan tim koordinasi SPBE Kementerian sebagai masukan untuk perbaikan berkelanjutan.

2. Pengembangan, Pembinaan, dan Pendayagunaan SDM
   a. Pengembangan, pembinaan, dan pendayagunaan SDM meliputi:
      1) Pengembangan kepemimpinan SPBE di Kementerian melalui komitmen, keteladanan, dan arahan dari pimpinan.
      2) Peningkatan literasi digital pegawai di Kementerian menggunakan program d*igital ecolab* yang terdiri dari *internalisasi utilisasi* perangkat, internalisasi kolaborasi digital, internalisasi keamanan digital, dan *internalisasi literasi* data dan informasi. Penerapan program d*igital ecolab* akan diatur sesuai ketentuan peraturan perundang-undangan.
      3) Peningkatan kapasitas SDM dengan menetapkan standar kompetensi teknis SPBE, mengembangkan kompetensi teknis SDM, mengembangkan pola karir dan remunerasi SDM.
      4) Kompetensi teknis SPBE yang dimaksud poin tiga (3) minimal mencakup bidang Proses Bisnis pemerintahan, arsitektur SPBE, data dan informasi, Keamanan SPBE, Aplikasi SPBE, dan Infrastruktur SPBE.
      5) Model Pengembangan Kompetensi SDM SPBE mengacu pada model *corporate university* sesuai dengan ketentuan peraturan perundang-undangan.
      6) Pengembangan Kompetensi SDM SPBE memanfaatkan Portal Pembelajaran Digital Kementerian Komunikasi dan Digital sesuai ketentuan peraturan perundang-undangan.
   b. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum bersama dengan Pusdatin melakukan identifikasi keterampilan dan kompetensi SDM yang ada, serta kesenjangan antara keterampilan yang tersedia dan yang dibutuhkan.
   c. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum bersama dengan Pusdatin membuat rencana pengembangan yang akan dilakukan, seperti pelatihan kepemimpinan (*soft skills*), dan peningkatan kapasitas SDM.
   d. Unit Organisasi melaksanakan pengembangan SDM bidang pekerjaan umum bersama dengan Pusdatin mengkaji materi dan program pelatihan secara rutin untuk memastikan keterkaitannya dengan perubahan dan dampaknya terhadap pengetahuan, keterampilan, dan kemampuan yang diperlukan.

e. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum menyediakan fasilitas repositori pengetahuan yang bisa diakses oleh seluruh pegawai untuk mendukung pengembangan keterampilan dan kompetensi.
f. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum mengembangkan dan memberikan program pelatihan berdasarkan persyaratan di Unit Organisasi, Unit Kerja, dan UPT, termasuk persyaratan untuk pengetahuan organisasi, kontrol internal, perilaku etis, keamanan, dan privasi.
g. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum bersama dengan Pusdatin menilai perkembangan keterampilan dan kompetensi pegawai.
h. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum menyampaikan hasil penilaian perkembangan keterampilan dan kompetensi pegawai kepada Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian, Pimpinan Unit Organisasi, Unit Kerja, dan UPT.
i. Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian mengkaji perkembangan keterampilan dan kompetensi pegawai untuk pembinaan karir, pelaksanaan penempatan, mutasi, rotasi, dan promosi pegawai.
j. Pimpinan Unit Organisasi, Unit Kerja, dan UPT melakukan penilaian dan mengusulkan penghargaan terhadap kinerja pegawai.
    1) Menetapkan sasaran kinerja pegawai yang selaras dengan tujuan Unit Organisasi, Unit Kerja, dan UPT dan TIK berbasis SMART (*specific, measurable, achievable, relevant and time-bound*) yang mencerminkan kompetensi inti, nilai-nilai organisasi, dan keterampilan yang diwajibkan untuk peran pegawai tersebut.
    2) Memberikan masukan secara berkala kepada Pusdatin dan Unit Kerja yang mengelola kepegawaian di Unit Organisasi, Unit Kerja, dan UPT masing-masing mengenai capaian kinerja pegawai yang berada di bawah tanggung jawabnya.
    3) Mengelola informasi yang bersifat pribadi dalam proses evaluasi kinerja sesuai dengan ketentuan peraturan perundang-undangan;
    4) Menyusun hasil evaluasi kinerja pegawai sesuai dengan sasaran kinerja yang disepakati.
    5) Menyediakan rencana jenjang karir jabatan secara formal dan pengembangan keahlian berdasarkan hasil evaluasi untuk mendorong pengembangan kompetensi pegawai/personil sehingga mengurangi ketergantungan pada personil tertentu.
    6) Mengusulkan penghargaan untuk pegawai yang memiliki komitmen, peningkatan kompetensi, dan keberhasilan pencapaian sasaran kinerja kepada Unit Kerja di sekretariat jenderal yang melakukan pengelolaan kepegawaian.

7) Menerapkan dan mengkomunikasikan proses disiplin kepada pegawai.

k. Pimpinan Unit Organisasi, Unit Kerja, dan UPT melakukan tindakan yang tepat terkait perubahan tugas dan fungsi terhadap personil SPBE, serta menyiapkan pegawai/personil cadangan melalui berbagi pengetahuan (*knowledge sharing*), dan pelatihan.

l. Unit Organisasi yang melaksanakan pengembangan SDM bidang pekerjaan umum menguji kemampuan pegawai/personil cadangan secara berkala.

m. Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian mengevaluasi persyaratan kepegawaian secara berkala atau jika terjadi perubahan yang bersifat mayor dan memastikan bahwa setiap Unit Organisasi/UPT/Unit Kerja memiliki sumber daya yang tepat dan memadai untuk mendukung tujuan dan sasaran organisasi, pengendalian dan Proses Bisnis, serta pengelolaan inisiatif SPBE.

n. Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian melakukan proses penerimaan pegawai/personil SPBE sesuai dengan ketentuan peraturan perundang-undangan.

o. Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian menetapkan pengaturan sumber daya yang fleksibel, seperti *outsourcing*, tenaga kontrak, vendor, pihak di luar Kementerian, untuk mendukung perubahan kebutuhan Layanan SPBE.

p. Unit Kerja di Sekretariat Jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian bersama Unit Organisasi/UPT/Unit Kerja melakukan pemeriksaan latar belakang (*background check*) dalam proses penerimaan pegawai SPBE dan vendor/pihak di luar Kementerian dan meningkatkan frekuensi pemeriksaan ini harus bergantung pada sensitivitas dan/atau kekritisan fungsi.

3. Pengelolaan Pegawai/Personil Kontrak

a. Unit Kerja di sekretariat jenderal yang mempunyai tugas melaksanakan pembinaan dan pengelolaan kepegawaian, organisasi, dan tata laksana Kementerian menerapkan kebijakan dan prosedur pegawai/personil kontrak.

b. Pimpinan Unit Organisasi, Unit Kerja, dan UPT melakukan kesepakatan perjanjian formal bahwa pegawai/personil kontrak harus mematuhi kebijakan SPBE yang berlaku di Kementerian, termasuk manajemen keamanan informasi, kontrol akses fisik dan logis, penggunaan fasilitas, dan perjanjian kerahasiaan informasi.

c. Pimpinan Unit Organisasi, Unit Kerja, dan UPT mengkomunikasikan kepada pegawai/personil kontrak bahwa manajemen berhak untuk memantau dan memeriksa semua penggunaan sumber daya TIK,

termasuk surat elektronik, komunikasi suara, semua program, dan *file* data.

d. Pimpinan Unit Organisasi, Unit Kerja, dan UPT mengkomunikasikan definisi yang jelas tentang peran dan tanggung jawab pegawai/personil kontrak, termasuk kewajiban untuk mendokumentasikan pekerjaan dengan standar, dan format yang disepakati.
e. Pimpinan Unit Organisasi, Unit Kerja, dan UPT mengkaji pekerjaan pegawai/personil kontrak dan menjadi dasar untuk kesepakatan pembayaran.
f. Pimpinan Unit Organisasi, Unit Kerja, dan UPT menetapkan semua pekerjaan yang dilakukan oleh pihak di luar Kementerian dalam sebuah kontrak formal.
g. Pimpinan Unit Organisasi, Unit Kerja, dan UPT meninjau secara berkala untuk memastikan bahwa pengelolaan pegawai/personil kontrak telah sesuai dengan Pedoman Manajemen Keamanan terkait pegawai/personil kontrak.

F. MANAJEMEN PENGETAHUAN

1. Manajemen pengetahuan SPBE adalah proses yang dilakukan untuk mendokumentasi pengalaman dan pengetahuan dalam perencanaan, implementasi, dan evaluasi SPBE guna meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE.
2. Manajemen pengetahuan SPBE bertujuan untuk mendorong dan meningkatkan budaya pembelajaran dengan menyebarkan dan membagikan pengetahuan yang relevan dengan tugas Kementerian sehingga dapat meningkatkan efisiensi operasional melalui penggunaan modal intelektual yang tepat.
3. Manfaat manajemen pengetahuan SPBE antara lain:
   a. Menghindari perbedaan pengetahuan dan pemahaman atas objek pengetahuan tertentu.
   b. Memperkecil dampak risiko dari penurunan atau hilangnya pengetahuan karena individu yang kompeten pensiun, meninggal, atau rotasi/mutasi.
   c. Menghindari hilangnya pengetahuan yang berharga dan mempercepat akses terhadap pengetahuan di Kementerian.
   d. Menghindari terjadinya permasalahan yang berulang.
   e. Meningkatkan kinerja pegawai dan Kementerian yang disebabkan karena tidak memiliki pengetahuan yang cukup.
   f. Mendorong pengembangan inovasi, perubahan positif, dan produktivitas; dan
   g. Meningkatkan efisiensi dari pemanfaatan sumber daya pengetahuan di Kementerian.
4. Pengetahuan dikelompokkan menjadi 2 (dua) kategori terdiri atas:
   a. Pengetahuan eksplisit; dan
   b. Pengetahuan implisit.

5. Pengetahuan eksplisit merupakan pengetahuan yang sudah didokumentasikan dan tersimpan dalam bentuk nyata pada suatu media tertentu berbentuk teks, gambar, suara, dan/atau audio visual yang dapat diakses dan dipahami oleh orang lain.
6. Pengetahuan implisit merupakan pengetahuan yang masih berada dalam pikiran individu sebagai hasil dari pengalaman, dan/atau proses pembelajaran.
7. Pengetahuan ditransformasikan melalui proses:
   a. Sosialisasi yang dilakukan melalui transformasi pengetahuan implisit ke pengetahuan implisit melalui diskusi atau berbagi pengetahuan dan pengalaman untuk menghasilkan pengetahuan baru.
   b. Eksternalisasi yang dilakukan melalui transformasi pengetahuan implisit pada setiap orang ke dalam bentuk pengetahuan eksplisit dan menyimpannya dalam suatu media tertentu yang memungkinkan untuk dikelola, diakses, dan didiseminasikan.
   c. Kombinasi yang dilakukan melalui transformasi pengetahuan yang mengombinasikan berbagai pengetahuan eksplisit yang berbeda untuk menghasilkan pengetahuan eksplisit baru; dan
   d. Internalisasi yang dilakukan melalui transformasi pengetahuan eksplisit ke pengetahuan implisit pada setiap orang.

8. Kementerian mendorong terjadinya transformasi pengetahuan untuk pelaksanaan manajemen pengetahuan SBPE.
9. Kerangka kerja manajemen pengetahuan SPBE digunakan untuk membantu Kementerian dalam mengintegrasikan manajemen pengetahuan SPBE dalam kegiatan dan pelaksanaan tugas dan fungsinya.
10. Kerangka kerja manajemen pengetahuan SPBE dikembangkan dan disesuaikan dengan karakteristik Kementerian.
11. Komponen kerangka kerja manajemen pengetahuan SPBE terdiri atas:
    a. Pembangunan budaya berbagi dan meningkatkan pengetahuan SPBE.
    b. Penyelenggaraan Proses Bisnis manajemen pengetahuan SPBE; dan
    c. Pembentukan struktur pengelola manajemen pengetahuan SPBE.

12. Pembangunan budaya berbagi dan meningkatkan Pengetahuan SPBE dilaksanakan dengan menyesuaikan nilai-nilai budaya Kementerian.
13. Pembangunan budaya berbagi dilakukan dengan berbagi pengetahuan antar setiap orang atau kelompok yang dimanfaatkan bersama untuk kepentingan Kementerian.
14. Pembangunan budaya meningkatkan pengetahuan SPBE dilakukan untuk mendorong pola pikir yang berorientasi pada pemecahan masalah, pembangunan kompetensi setiap orang, dan peningkatan kinerja Kementerian.
15. Dalam pembangunan budaya berbagi dan meningkatkan pengetahuan SPBE, dibutuhkan:
    a. Kepemimpinan digital dengan kriteria:
       1) Memberi contoh dengan terbuka berbagi pengalaman, *best practice,* dan *insight*.

2) Memiliki komitmen dalam mengelola pengetahuan.
3) Mampu memberikan arahan kebijakan yang jelas dan mudah dipahami.
4) Mampu memberikan dukungan secara konsisten dalam memanfaatkan teknologi informasi dan komunikasi untuk meningkatkan pengetahuan Kementerian terkait SPBE.
5) Mampu membangun kepercayaan dan mendorong pola pikir serta budaya kerja yang kolaboratif dan inovatif; dan
6) Menghargai keterbukaan, bukan hanya hasil kerja.

b. Sistem penghargaan terhadap kontribusi aparatur sipil negara dalam:
1) Pembangunan basis pengetahuan SPBE.
2) Berbagi pengetahuan SPBE secara aktif.
3) Berpartisipasi dalam memecahkan masalah dan menciptakan pengetahuan baru SPBE; dan
4) Membuat *sharing* pengetahuan sebagai bagian penilaian kinerja.

c. Ruang & media untuk berbagi
1) Membuat forum diskusi rutin (*knowledge cafe, brown bag session, sharing session*).
2) Memanfaatkan *platform* digital (intranet, *knowledge management system*, *chat group* khusus).

d. Budaya kolaboratif
1) Menekankan kerja tim daripada kompetisi internal.
2) Menghargai proses belajar bersama, bukan hanya hasil individual.

e. Dokumentasi & akses mudah
1) Membuat SOP, panduan atau *case study* yang mudah diakses.
2) Menyediakan repositori pengetahuan yang terstruktur.

f. Pelatihan & kesadaran
1) Memberikan *training* tentang pentingnya *knowledge sharing*.
2) Menumbuhkan *mindset* bahwa berbagi pengetahuan adalah investasi, bukan beban.

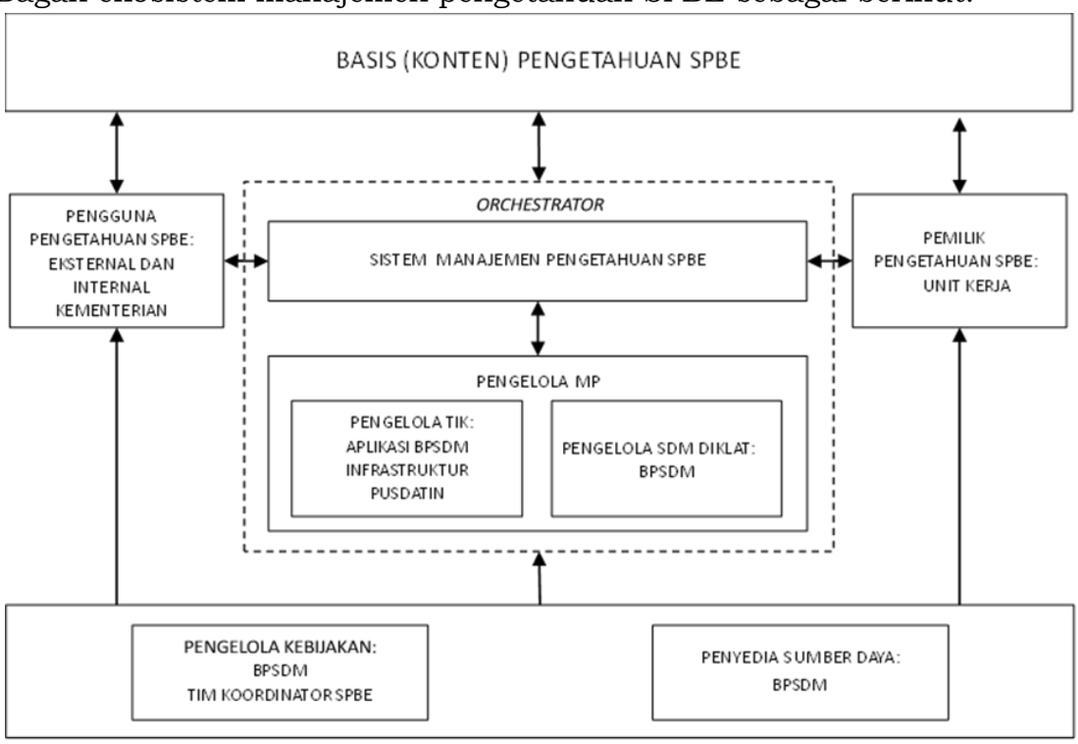
g. Integrasi dalam proses kerja
1) Membiasakan setiap proyek/kegiatan ditutup dengan *lessons learned*.
2) Membuat *mentoring* atau *buddy system* antara senior–junior.

h. Membangun kepercayaan
1) Lingkungan kerja harus aman secara psikologis (tidak takut salah atau dihakimi).
2) Budaya saling menghargai ide dan kontribusi.

16. Penyelenggaraan Proses Bisnis manajemen pengetahuan SPBE diterapkan dengan berpedoman pada:
    a. Siklus manajemen secara umum meliputi perencanaan, pelaksanaan, pemantauan dan evaluasi, dan perbaikan; dan
    b. Siklus manajemen pengetahuan SPBE meliputi pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi.
17. Penyelenggaraan Proses Bisnis manajemen pengetahuan SPBE dilaksanakan secara terpadu menggunakan teknologi dan sistem informasi manajemen pengetahuan SPBE yang terpusat dan terintegrasi.
18. Penyelenggaraan Proses Bisnis manajemen pengetahuan dilaksanakan dengan proses manajemen secara keseluruhan, menyatu dalam budaya, dan disesuaikan dengan Proses Bisnis Kementerian.
19. Pembentukan struktur pengelola manajemen pengetahuan SPBE terintegrasi dengan tim koordinasi SPBE Kementerian.
20. Ekosistem manajemen pengetahuan SPBE merupakan suatu tatanan utuh yang memungkinkan tumbuh dan berkembangnya pengetahuan SPBE yang berguna bagi berbagai pihak yang berkepentingan.
21. Ekosistem manajemen pengetahuan SPBE terdiri atas berbagai komponen pelaku dan subsistem yang saling berinteraksi satu sama lain dan dengan lingkungan sekitarnya.
22. Komponen pelaku dalam ekosistem manajemen pengetahuan SPBE Kementerian terdiri atas:
    a. Pengelola kebijakan.
    b. Pelaksana; dan
    c. Pendukung.
23. Subsistem dalam ekosistem manajemen pengetahuan SPBE terdiri atas:
    a. Basis (konten) pengetahuan SPBE; dan
    b. Sistem manajemen pengetahuan SPBE.
24. Pengelola kebijakan terdiri atas:
    a. Badan Pengembangan Sumber Daya Manusia (BPSDM) sebagai pembuat kebijakan terkait penerapan manajemen pengetahuan SPBE; dan
    b. Tim Koordinator SPBE sebagai pengawas penerapan manajemen pengetahuan SPBE sesuai dengan kebijakan yang telah ditetapkan.
25. Pelaksana terdiri atas:
    a. Pemilik pengetahuan SPBE adalah Unit Kerja yang ditetapkan oleh Menteri.
    b. Pengguna pengetahuan SPBE yang berasal dari internal atau eksternal Kementerian.
    c. Pengelola proses manajemen pengetahuan SPBE adalah BPSDM yaitu pihak yang mendorong interaksi dan kolaborasi untuk menjembatani kebutuhan pengetahuan antara pemilik dan pengguna pengetahuan SPBE.
    d. BPSDM, Pusdatin, dan Unit Kerja adalah penyedia teknologi dan komunikasi (TIK) untuk mendukung penerapan manajemen pengetahuan SPBE; dan

e. BPSDM sebagai pengelola kompetensi sumber daya manusia yang melaksanakan pengembangan kompetensi setiap orang khususnya untuk pendidikan dan pelatihan di Kementerian.

26. Penyedia teknologi dan komunikasi terdiri atas:
    a. Unit kerja sebagai penyedia dan pemelihara basis (konten) pengetahuan SPBE untuk dapat diakses dan digunakan oleh penggunanya.
    b. BPSDM sebagai pengelola aplikasi manajemen pengetahuan SPBE yang mendukung proses manajemen pengetahuan SPBE untuk:
        1) Pencarian pengetahuan SPBE yang dibutuhkan.
        2) Berbagi pengetahuan SPBE; dan
        3) Penciptaan pengetahuan baru SPBE.
    c. Pusdatin sebagai penyedia dan pemelihara infrastruktur TIK.
27. BPSDM merupakan penyedia sumber daya yang terdiri atas:
    a. Penyedia sumber daya manusia.
    b. Penyedia sarana dan prasarana; dan
    c. Penyedia anggaran.
28. Bagan ekosistem manajemen pengetahuan SPBE sebagai berikut:




Gambar 17 Bagan ekosistem manajemen pengetahuan SPBE

29. Proses manajemen pengetahuan SPBE terdiri dari pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam SPBE. Proses manajemen pengetahuan SPBE ini dikoordinasikan oleh BPSDM.
30. Proses manajemen pengetahuan SPBE dapat memanfaatkan teknologi informasi yang menghasilkan data, informasi, dan pengetahuan secara langsung seperti *online technology processing, internet of thing* (IoT), *artificial intelligence* (AI), dan teknologi informasi tingkat lanjut lainnya.
31. Pengumpulan
    a. Pengumpulan dilakukan dengan menyimpan pengetahuan SPBE dalam basis data pengetahuan SPBE secara terpusat.
    b. Pengumpulan dilakukan dengan cara secara formal dan secara informal.
    c. Proses pengumpulan pengetahuan SPBE secara formal terintegrasi dalam proses pencatatan atau dokumentasi dalam pengoperasian, pelayanan, dan pengembangan SPBE meliputi:
        1) Pencatatan penanganan insiden atau permasalahan sistem oleh petugas pelayanan SPBE.
        2) Dokumentasi pengembangan sistem; atau
        3) Dokumentasi hasil rapat yang menghasilkan keputusan pemecahan masalah.
    d. Proses pengumpulan pengetahuan SPBE secara informal dilakukan melalui diskusi, konsultasi, atau tanya jawab permasalahan dengan praktisi atau pakar terkait.
    e. Pengetahuan SPBE dalam bentuk tidak berwujud, implisit atau masih berupa data dan informasi atau pemahaman yang tidak terstruktur atau belum didefinisikan dalam bahasa formal yang terkumpul dari proses pengumpulan pengetahuan SPBE diubah menjadi pengetahuan SBPE dalam bentuk berwujud dan eksplisit.
    f. Pengetahuan SPBE dicatat, diartikulasi, dan direpresentasikan dengan baik agar dapat diserap dan digunakan kembali.

32. Pengolahan
    Untuk mengolah informasi menjadi pengetahuan dilakukan langkah-langkah berikut:
    a. Pengolahan dilakukan terhadap pengetahuan lama yang telah ada, diolah, dimodifikasi, atau dibentuk menjadi pengetahuan baru untuk mendukung pengambilan keputusan dan melakukan tindakan dalam SPBE.
    b. Pengolahan untuk pengetahuan SPBE eksplisit yang dikumpulkan dalam basis pengetahuan dilakukan kodifikasi, disusun, dan dilengkapi dengan metadata pengetahuan SPBE untuk memudahkan pencarian dan penggunaannya kembali.
    c. Contoh metadata pengetahuan SPBE digunakan untuk membangun basis data pengetahuan SPBE sebagai berikut:

Tabel 38 Contoh metadata pengetahuan SPBE

| NO. | METADATA | KETERANGAN |
|---|---|---|
| 1. | Nomor ID | Nomor ID pengetahuan SPBE |
| 2. | Judul | Judul atau *title* dari pengetahuan SPBE |
| 3. | Penulis | Penulis atau *author* adalah nama penulis, penyusun, atau pembuat pengetahuan SPBE |
| 4. | Instansi | Instansi penyedia pengetahuan atau berupa instansi dari penulis pada waktu membuat/ menulis pengetahuan |
| 5. | Deskripsi | Penjelasan secara naratif dari pengetahuan SPBE |
| 6. | Waktu | Waktu penerbitan atau publikasi dari pengetahuan SPBE |
| 7. | Format | Bentuk atau media penyimpanan dari pengetahuan SPBE, misalnya tulisan, gambar, audio, video |
| 8. | Lingkup | Lingkup SPBE atau kategori adalah pengelompokan pengetahuan SPBE sesuai aturan, kebijakan, atau rencana yang disepakati, misalnya arsitektur SPBE, pemantauan dan evaluasi SPBE, manajemen layanan SPBE, manajemen pengetahuan SPBE, Audit TIK, dan sebagainya |
| 9. | Label | Label atau *tags* (*taggings*) adalah frasa atau kata kunci dari pengetahuan SPBE untuk memudahkan pencarian kembali |
| 10. | Kontributor | Kontributor atau nama pendukung yang memberikan kontribusi pada penulis dalam menyusun pengetahuan SPBE. Kontributor bisa berjumlah lebih dari satu. |
| 11. | Status Publikasi | Publikasi untuk umum (masyarakat) atau terbatas untuk internal aparatur sipil negara dan pengguna pengetahuan SPBE |
| 12. | URL | Tautan lokasi pengetahuan SPBE |

Contoh pengisian metadata pengetahuan pada Aplikasi Manajemen Pengetahuan Karya Layanan Online PU (KLOP).

Tabel 39 Contoh pengisian metadata pengetahuan

| No. | METADATA | KETERANGAN |
|---|---|---|
| 1. | Nomor ID | -PA-0202-Ms-001 |
| 2. | Judul | Karya Layanan Online PU (KLOP) |
| 3. | Penulis | Badan Pengembangan Sumber Daya Manusia |
| 4. | Instansi | Kementerian Pekerjaan Umum |
| 5. | Deskripsi | Aplikasi layanan berbasis web yang digunakan untuk mengelola, memproses, dan memantau permohonan layanan *Knowledge Management System* dan *Learning Managemen System* |
| 6. | Waktu | 9 Desember 2024 |

| | | |
|---|---|---|
| 7. | Format | *Web-based* (*Responsive*) |
| 8. | Lingkup | Manajemen pengetahuan SPBE |
| 9. | Label | KLOP, pengetahuan, KMS, Kementerian Pekerjaan Umum |
| 10. | Kontributor | Unit organisasi, Tim Pokja Manajemen Pengetahuan Kementerian PU |
| 11. | Status Publikasi | Seluruh elemen masyarakat |
| 12. | URL | https://klop.pu.go.id |

d. Menampilkan pengetahuan berdasarkan kebutuhan Unit Organisasi, Unit Kerja, dan UPT atau pemangku kepentingan lain.
e. Mempublikasikan dan memberikan akses pengetahuan kepada para pemangku kepentingan yang relevan, berdasarkan peran dan hak akses yang diberikan.
f. Mengevaluasi kegunaan, relevansi dan nilai pengetahuan, memperbarui informasi yang masih memiliki relevansi dan nilai bagi Kementerian, mengidentifikasi informasi terkait yang tidak lagi relevan dengan persyaratan atau diarsipkan sesuai dengan peraturan perundang-undangan.

33. Penyimpanan
a. Sumber data atau informasi harus disimpan di media yang aman sesuai dengan klasifikasinya.
b. Pengetahuan harus disimpan secara terpusat dengan memanfaatkan teknologi komputasi awan untuk memudahkan penyediaan layanan berbagi pakai di fasilitas penyimpanan yang dikoordinasikan oleh Pusdatin.
c. Penyimpanan dibuat sesuai dengan kebutuhan, kapasitas, fungsi penyimpanan, ketepatan, dan kecepatan pencarian dan pengaksesan pengetahuan SPBE.
d. Arsip pengetahuan disimpan dan dipelihara dalam media dan tempat yang aman sampai pada masa berlakunya sesuai dengan ketentuan peraturan perundang-undangan.

34. Penggunaan

Penggunaan untuk mendukung efektivitas dan efisiensi dalam penyediaan dan penggunaan layanan SPBE, dan pengambilan keputusan terkait SPBE dilakukan langkah-langkah berikut:
a. Mengidentifikasi pengguna pengetahuan sesuai dengan klasifikasinya.
b. Mentransfer pengetahuan ke pengguna berdasarkan kebutuhannya secara efektif.
c. Menciptakan lingkungan, alat, dan bahan yang mendukung untuk berbagi dan transfer pengetahuan serta memastikan kontrol akses yang tepat sudah ada, sejalan dengan klasifikasi pengetahuan.
d. Mengukur penggunaan Aplikasi SPBE untuk manajemen pengetahuan dan evaluasi dampaknya terhadap Layanan SPBE dan pengambilan keputusan.

e. Meningkatkan informasi dan pengetahuan berdasarkan hasil evaluasi dampak terhadap Layanan SPBE dan pengambilan keputusan.

35. Alih Pengetahuan

Alih pengetahuan dan teknologi merupakan proses pemindahan pengetahuan dan tata cara terkait SPBE dari seseorang, sekelompok orang atau suatu unit kerja ke orang lain, kelompok orang lainnya atau ke unit kerja/organisasi/instansi lainnya untuk memastikan pengetahuan dan teknologi dapat diserap atau dipahami oleh penerimanya yang digunakan untuk mengambil keputusan atau melakukan tindakan. Alih pengetahuan terdiri dari:

a. Sosialisasi yang merupakan proses belajar dengan cara memperhatikan, meniru, dan berlatih. Sosialisasi dapat dilakukan dengan cara:
   1) Bekerja secara berdampingan; dan
   2) Berbagi pekerjaan dengan kondisi yang serupa.

b. Eksternalisasi yang merupakan proses transformasi pengetahuan dari bentuk tacit, ke bentuk eksplisit.
c. Internalisasi yang dilakukan secara perorangan dan dapat dibagikan ulang berdasarkan pengetahuan atau pengalaman yang dialami seseorang kepada orang lainnya, baik secara lisan maupun tulisan.

   Proses alih pengetahuan harus dilaksanakan oleh:
   1) Pihak Ketiga, dalam periode akhir pekerjaan yang dilakukan. Pekerjaan tidak dapat dinyatakan selesai sebelum alih pengetahuan dilaksanakan.
   2) Pegawai, dalam periode proses rotasi/mutasi dan dalam periode menjelang pensiun. Proses rotasi/mutasi atau pensiun tidak dapat dilanjutkan sebelum alih pengetahuan dilaksanakan.

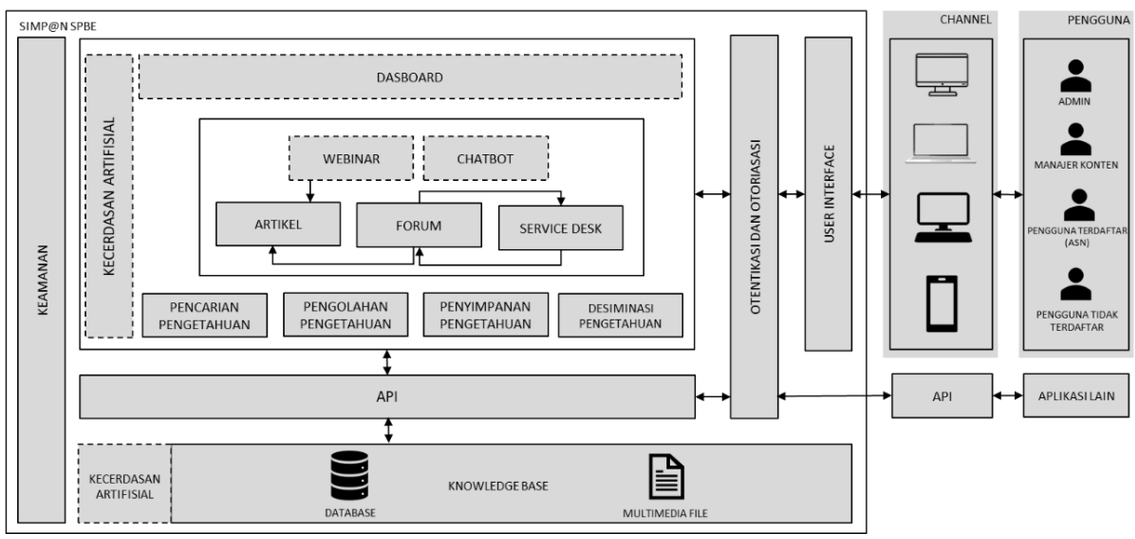
36. Pemantauan dan Evaluasi

a. Proses manajemen pengetahuan dipantau dan dievaluasi tingkat keberhasilannya secara berkala, minimal 1 (satu) kali dalam 1 (satu) tahun.
b. Proses manajemen pengetahuan SPBE dipantau dan dievaluasi oleh tim koordinasi SPBE.
c. Hasil pemantauan dan evaluasi menjadi acuan bagi Kementerian dalam melakukan perbaikan penerapan manajemen pengetahuan SPBE.
d. Pemantauan dan evaluasi dalam strategi implementasi manajemen pengetahuan SPBE dilakukan untuk mengukur:
   1) Tingkat kematangan penerapan manajemen pengetahuan SPBE; dan
   2) Efektivitas implementasi manajemen pengetahuan SPBE.
e. Tingkat kematangan penerapan manajemen pengetahuan SPBE diukur berdasarkan peraturan perundang-undangan.

37. Pengukuran tingkat kematangan penerapan manajemen pengetahuan SPBE menjadi acuan untuk mendukung perencanaan dan perbaikan penerapan manajemen pengetahuan SPBE selanjutnya.
38. Pengukuran efektivitas implementasi manajemen pengetahuan SPBE dilakukan melalui pengukuran kuantitatif sebagai indikator aktivitas proses:
    a. Pencarian pengetahuan SPBE.
    b. Penciptaan pengetahuan SPBE; dan
    c. Berdiskusi dan berbagi pengalaman.
39. Pengukuran aktivitas pencarian pengetahuan SPBE dilakukan untuk memberikan gambaran tentang kebutuhan pengetahuan SPBE oleh pengguna, berdasarkan:
    a. Jumlah permintaan pencarian pengetahuan SPBE; dan
    b. Pengetahuan SPBE yang paling banyak dicari atau diminta oleh pengguna pengetahuan SPBE.
40. Pengukuran aktivitas penciptaan pengetahuan SPBE dilakukan untuk memberikan gambaran tentang pengembangan basis pengetahuan SPBE di Kementerian paling sedikit berdasarkan:
    a. Jumlah dan penambahan artikel atau representasi pengetahuan SPBE baru yang terkumpul; dan
    b. Jumlah artikel atau representasi pengetahuan SPBE dari pakar atau ahli bidang tertentu, termasuk pegawai yang mendekati masa pensiun.
41. Pengukuran aktivitas berdiskusi dan berbagi pengalaman dilakukan untuk memberikan gambaran tentang efektivitas proses penciptaan pengetahuan yang dibutuhkan secara kolektif meliputi:
    a. Jumlah pertanyaan atau permasalahan SPBE yang disampaikan dalam diskusi.
    b. Jumlah jawaban, respon, atau komentar atas pertanyaan atau permasalahan SPBE yang dibahas dalam diskusi.
    c. Jumlah individu yang mengajukan pertanyaan terkait SPBE; dan
    d. Jumlah individu yang memberikan jawaban, respon, atau komentar terhadap pertanyaan terkait SPBE.
42. Pengukuran efektivitas implementasi manajemen pengetahuan SPBE merupakan pengukuran pemanfaatan manajemen pengetahuan SPBE yang dapat dikembangkan sesuai kebutuhan, kapasitas, kondisi penerapan, atau tingkat kematangan penerapan manajemen pengetahuan SPBE di Kementerian.
43. Alat bantu manajemen pengetahuan SPBE berbentuk sistem aplikasi yang dilengkapi dengan fitur untuk mendukung seluruh proses manajemen pengetahuan SPBE.
44. Alat bantu manajemen pengetahuan SPBE terdiri atas:
    a. Alat bantu proses pengumpulan berbentuk fitur aplikasi untuk memfasilitasi proses identifikasi, pencarian, dan pengumpulan pengetahuan SPBE.
    b. Alat bantu proses pengolahan berbentuk fitur aplikasi untuk memfasilitasi proses pengolahan pengetahuan dalam pemeliharaan dan penggunaan pengetahuan SPBE.

c. Alat bantu proses penyimpanan berbentuk fitur aplikasi untuk memfasilitasi proses penyimpanan pengetahuan SPBE yang dapat dilakukan secara terpusat di Pusat Data Nasional atau terdistribusi di Kementerian yang terhubung dengan Pusat Data Nasional; dan
d. Alat bantu proses penggunaan berbentuk fitur aplikasi untuk memfasilitasi proses pendayagunaan pengetahuan SPBE yang telah terkumpul.

45. Alat bantu proses alih pengetahuan dan teknologi berbentuk fitur aplikasi untuk memfasilitasi proses komunikasi dalam berbagi pengetahuan SPBE sehingga pengetahuan SPBE dapat terdayagunakan secara lebih efisien dan efektif.
46. Alat bantu manajemen pengetahuan SPBE harus memenuhi prinsip-prinsip SPBE dan mempunyai kemampuan untuk diintegrasikan dengan Aplikasi SPBE lainnya.
47. Kementerian telah memiliki sistem informasi manajemen pengetahuan SPBE.
48. Sistem informasi manajemen pengetahuan SPBE Kementerian harus terintegrasi dengan sistem informasi manajemen pengetahuan SPBE nasional.
49. Bagan arsitektur sistem informasi manajemen pengetahuan SPBE sebagai berikut:




Gambar 18 Bagan arsitektur sistem informasi manajemen pengetahuan SPBE

50. Sistem informasi manajemen pengetahuan SPBE minimal memuat modul:
    a. Artikel pengetahuan.
    b. Forum diskusi.
    c. *Service desk*; dan
    d. Pengelolaan pengguna pengetahuan SPBE.

51. Modul artikel pengetahuan digunakan sebagai media atau wadah untuk merepresentasikan pengetahuan eksplisit berupa narasi dalam bentuk teks, gambar, suara dan/atau audio visual untuk memudahkan penyimpanan dan pemahaman pengetahuan SPBE oleh pihak lain.
52. Modul forum diskusi digunakan sebagai media atau wadah bagi sekelompok orang untuk berinteraksi, bertanya jawab, dan berdiskusi tentang berbagai topik atau bidang terkait SPBE.
53. Modul pengelolaan pengguna pengetahuan SPBE digunakan sebagai media atau wadah untuk mengatur hak akses pengguna pengetahuan SPBE terhadap fitur yang ada dalam sistem informasi manajemen pengetahuan SPBE.
54. Dalam pelaksanaan manajemen pengetahuan SPBE, pimpinan Kementerian berkoordinasi dan dapat melakukan konsultasi dengan Badan Riset dan Inovasi Nasional jika diperlukan.
55. Koordinasi dan konsultasi manajemen pengetahuan SPBE dilakukan oleh BPSDM.
56. Koordinasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
57. Koordinasi dilakukan untuk:
    a. Pengembangan basis pengetahuan SPBE nasional; dan
    b. Pengembangan proses pengelolaan pengetahuan SPBE nasional.

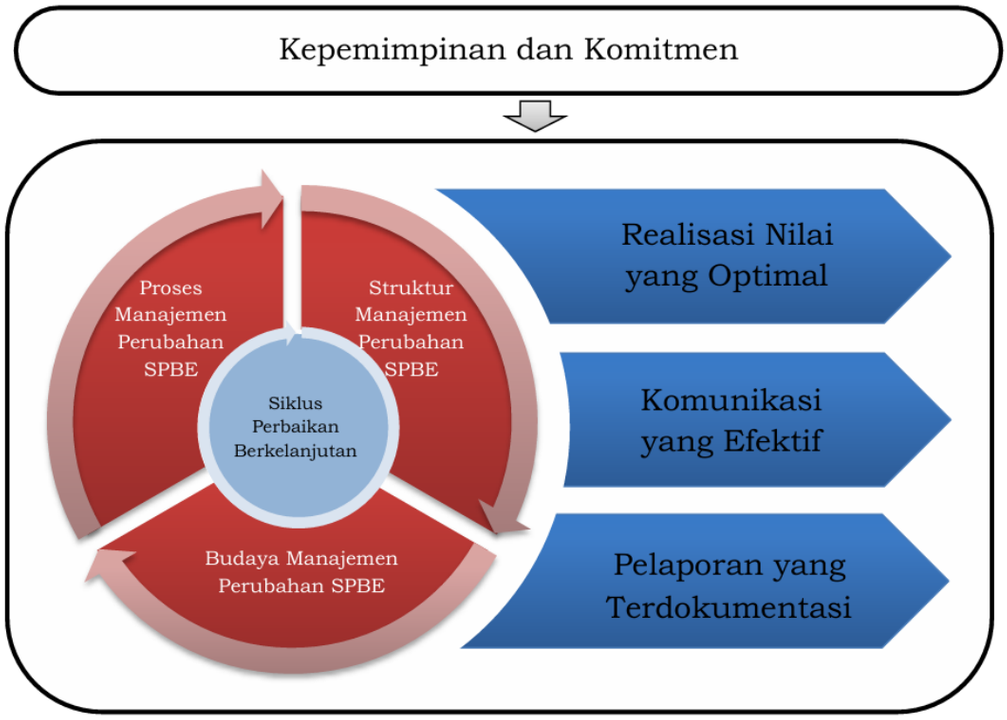
G. MANAJEMEN PERUBAHAN

1. Tujuan dan Lingkup Manajemen Perubahan SPBE

   Manajemen Perubahan SPBE bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE. Ruag lingkup Manajemen Perubahan SPBE mencakup
   a. Perubahan Aplikasi;
   b. Perubahan Perangkat Keras;
   c. Perubahan Perangkat Lunak;
   d. Perubahan Infrastruktur;
   e. Perubahan Proses Bisnis;
   f. Perubahan Lingkungan Organisasi;
   g. Perubahan Layanan;
   h. Perubahan Data;
   i. Perubahan Keamanan;
   j. Perubahan Arsitektur.

2. Kerangka Kerja Manajemen Perubahan

   Kerangka kerja Manajemen Perubahan SPBE mendeskripsikan komponen dasar yang digunakan sebagai landasan penerapan Manajemen Perubahan SPBE. Komponen dasar dari kerangka kerja ini terdiri atas prinsip mengenai kepemimpinan dan komitmen, serta proses dan tata kelola Manajemen Perubahan SPBE yang digambarkan sebagai berikut:




Gambar 19 Proses dan Tata Kelola Manajemen Perubahan SPBE

Komponen Kerangka Kerja manajemen Perubahan SPBE diuraikan sebagai berikut:

a. Kepemimpinan dan Komitmen

Kepemimpinan merupakan komponen kritikal untuk kesuksesan penerapan Manajemen Perubahan SPBE. Kepemimpinan dan komitmen dalam penerapan kerangka kerja ditunjukkan melalui Manajemen Perubahan SPBE, melalui:

1) Proses Manajemen Perubahan SPBE;
2) Struktur Manajemen Perubahan SPBE;
3) Budaya Manajemen Perubahan SPBE; dan
4) Siklus Perbaikan Berkelanjutan.

Tim koordinasi SPBE mendorong secara aktif penyelenggaraan kepemimpinan dan komitmen dalam manajemen perubahan yang menjamin keberlangsungan dan meningkatkan kualitas Layanan Berbasis Elektronik melalui pengendalian perubahan SPBE. Dengan demikian, sasaran utama dari Manajemen Perubahan SPBE yaitu Realisasi Nilai yang Optimal, Komunikasi yang Efektif, serta Pelaporan yang Terdokumentasi dapat tercapai

b. Siklus Perbaikan Berkelanjutan

Perbaikan berkelanjutan adalah pendekatan jangka panjang berkelanjutan yang dilakukan secara bertahap dan bertujuan untuk membuat perubahan dari waktu ke waktu. Siklus Perbaikan Berkelanjutan ini membantu memastikan Proses, Struktur, dan Budaya Manajemen Perubahan SPBE memenuhi tujuan SPBE.

1) Proses Manajemen Perubahan SPBE

Proses Manajemen Perubahan SPBE adalah serangkaian langkah perubahan yang dilakukan melalui aktivitas perencanaan, analisis, pengembangan, implementasi, serta pemantauan dan evaluasi

terhadap Perubahan SPBE.

2) Struktur Manajemen Perubahan SPBE
   Struktur Manajemen Perubahan SPBE merupakan struktur ex-officio yang menjalankan tugas dan tanggung jawab tambahan terkait Manajemen Perubahan SPBE.
3) Budaya Manajemen Perubahan SPBE
   Budaya Manajemen Perubahan SPBE merupakan perilaku kesadaran terhadap adanya kemungkinan terjadinya Perubahan SPBE, baik positif maupun negatif, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan Manajemen Perubahan SPBE Kementerian Pekerjaan Umum.

c. Sasaran Utama Manajemen Perubahan SPBE
   Pendekatan terstruktur yang dilakukan dalam Manajemen Perubahan SPBE merupakan pergeseran atau transisi dari keadaan sekarang ke keadaan masa depan yang diinginkan. Manajemen Perubahan SPBE memiliki sasaran utama yang di antaranya sebagai berikut:
   1) Realisasi Nilai yang Optimal
      Melalui pendekatan terstruktur yang dilakukan dalam Manajemen Perubahan SPBE, diharapkan hambatan menjadi lebih minim sehingga realisasi menjadi optimal.
   2) Komunikasi yang Efektif
      Komunikasi yang efektif diharapkan dapat terjalin melalui penerapan Manajemen Perubahan SPBE. Seluruh informasi yang tepat dan akurat serta keterlibatan berbagai pihak dalam rangka perubahan menjadi dampak adanya penerapan manajemen ini.
   3) Pelaporan yang Terdokumentasi
      Penerapan Manajemen Perubahan SPBE berimplikasi pada adanya pelaporan yang terdokumentasi. Dokumentasi yang berfungsi sebagai bukti dapat digunakan untuk memperoleh pemahaman yang lebih baik bagi Kementerian Pekerjaan Umum, serta menemukan kekurangan dan perbaikan melalui pelaporan yang dilakukan.

3. Proses Manajemen Perubahan
   a. Perencanaan Perubahan
      Merencanakan strategi manajemen perubahan, sebagai berikut:
      1) Menyusun rencana strategi dan implementasi perubahan sebelum mengimplementasikan Peta Rencana SPBE Kementerian berdasarkan arah pengembangan SPBE dan arsitektur SPBE Kementerian.
      2) Rencana strategi perubahan juga harus mencakup area perubahan yang diinginkan, tim pengelola perubahan, waktu yang dibutuhkan, serta rencana anggarannya.
      3) Setiap rencana perubahan yang bersifat strategis harus disampaikan pada tim koordinasi SPBE untuk diberikan pertimbangan dan persetujuan.

   b. Analisis Perubahan

Melakukan analisis perubahan SPBE sebagai berikut:

1) Melakukan pemetaan (*mapping*) terhadap para pemangku kepentingan dan melakukan asesmen atas pengaruh perubahan terhadap masing – masing pemangku kepentingan.
2) Melakukan asesmen terhadap:
   (a). Kesiapan perubahan, termasuk di dalamnya identifikasi penolakan terhadap perubahan;
   (b). Tingkat partisipasi/dukungan para pemangku kepentingan, kebutuhan akan komunikasi untuk manajemen perubahan, dan mengidentifikasikan penolakan terhadap perubahan;
   (c). Organisasi, termasuk struktur, peran (roles) dan tanggung jawabnya (responsibilities);
   (d). Kemampuan / kapabilitas dan skills proses, SDM, dan teknologi untuk melaksanakan perubahan.
3) Melakukan analisis dampak potensial dari perubahan pada:
   (a). Layanan administrasi pemerintahan saat ini;
   (b). Layanan publik saat ini;
   (c). Kebijakan dan prosedur;
   (d). Kapasitas, ketersediaan layanan, kesinambungan layanan, dan keamanan informasi.
4) Merumuskan manfaat (benefit) yang diperoleh dari hasil perubahan Layanan SPBE yang akan dilaksanakan.
5) Merumuskan mekanisme pelaksanaan perubahan SPBE termasuk tata kelola, manajemen, pemantauan dan evaluasi SPBE serta pelaporannya.

c. Pengembangan Perubahan SPBE
   Melakukan pengembangan perubahan SPBE sebagai berikut:

   1) Mengembangkan perubahan SPBE yang telah direncanakan dan dikaji yang meliputi Aplikasi SPBE, Infrastruktur SPBE, dan SDM yang dibutuhkan untuk meningkatkan kualitas Layanan SPBE.
   2) Melakukan pembangunan dan pengembangan Aplikasi SPBE.
   3) Menyediakan Infrastruktur SPBE sesuai dengan kebutuhan SPBE.
   4) Mengembangkan strategi dan rencana komunikasi.
   5) Mengembangkan strategi dan rencana pelatihan, termasuk menetapkan standar dan Indikator Kinerja Utama (IKU).

d. Implementasi Strategi dan Rencana Perubahan SPBE
   Melakukan implementasi strategi dan rencana perubahan SPBE sebagai berikut:

   1) Mengintegrasikan peta rencana strategis SPBE Kementerian dengan strategi perubahan dan strategi komunikasi.
   2) Menjalankan tiga tahapan proses komunikasi, yaitu sebelum pelaksanaan kegiatan, saat pelaksanaan kegiatan, dan saat kegiatan selesai dilaksanakan.

3) Melaksanakan pelatihan dan bimbingan teknis terkait dengan implementasi Layanan SPBE, termasuk menyiapkan materi pelatihannya.
4) Melaksanakan program pelatihan TOT (*Training of the Trainer*) untuk mempercepat implementasinya.
5) Memperbaharui strategi dan rencana perubahan.
6) Mengimplementasikan struktur organisasi yang baru, jika ada perubahan, termasuk peran dan tanggung jawabnya yang baru untuk mendukung perubahan.
7) Menerapkan aturan dan prosedur sesuai dengan perubahan yang terjadi.

Setiap implementasi strategi hanya dapat dilaksanakan sesuai keputusan tim koordinasi SPBE yang ditetapkan secara tertulis.

e. Pemantauan dan Evaluasi
Melakukan pemantauan dan evaluasi perubahan sebagai berikut:

1) Memantau dan mengevaluasi tingkat keberhasilan perubahan yang ditetapkan pada strategi perubahan dan rencana serta tindak lanjut perbaikan atas hasil pemantauan dan evaluasi pelaksanaan perubahan.
2) Kegiatan pemantauan dan evaluasi yang dilakukan adalah:

(a). Mengukur tingkat keberhasilan dari pelaksanaan rencana manajemen perubahan.
(b). Mengumpulkan dan menganalisis umpan balik dan mengevaluasi pelaksanaan manajemen perubahan.
(c). Mendiagnosis kembali kesenjangan dan mengelola penolakan yang terjadi dalam pelaksanaan manajemen perubahan.
(d). Melaksanakan tindakan perbaikan dan membuat langkah tindak lanjut untuk keberlanjutan proses perubahan.
(e). Memberikan penghargaan kepada pegawai yang berhasil mengimplementasikan perubahan dengan baik.

4. Struktur dan Budaya Manajemen Perubahan
a. Struktur Manajemen Perubahan
Struktur Manajemen Perubahan SPBE merupakan struktur *ex-officio* yang menjalankan tugas tambahan terkait Manajemen Perubahan SPBE. struktur Manajemen Perubahan SPBE terintegrasi dengan struktur manajemen perubahan yang telah ada tersebut untuk keterpaduan pelaksanaan manajemen perubahan secara menyeluruh.
Tim koordinasi SPBE secara aktif memberikan arahan dan mengoordinasikan pelaksanaan manajemen perubahan SPBE. Teknis pelaksanaan manajemen perubahan SPBE dilaksanakan oleh Koordinator Manajemen Perubahan bersama-sama dengan Unit Pelaksaa Manajemen Perubahan (UPMP), yaitu unit kerja pengampu tugas dan fungsi pada area perubahan terkait (misalnya pada area perubahan Proses Bisnis, Biro Kepegawaian dan Organisasi bertindak

sebagai UPMP). UPMP selanjutnya dapat menunjuk dan menetapkan Agen Perubahan. Agen Perubahan melaksanakan peran sebagai:

1) Katalis, yaitu meyakinkan pegawai yang ada di Kementerian tentang pentingnya perubahan menuju kondisi yang lebih baik (tujuan yang direncanakan).
2) Pemberi Solusi, yaitu memberikan alternatif solusi kepada pegawai Kementerian yang mengalami kendala dalam proses implementasi perubahan menuju tujuan akhir.
3) Mediator, yaitu membantu kelancaran proses perubahan, terutama menyelesaikan masalah yang muncul di dalam penerapan SPBE dan membina hubungan antar pihak yang ada di dalam dan di luar Kementerian terkait dalam proses perubahan.
4) Penghubung Sumber Daya, yaitu menghubungkan pegawai Kementerian kepada pemilik sumber daya atau pembuat kebijakan.

b. Budaya Manajemen Perubahan
Budaya Manajemen Perubahan SPBE merupakan perilaku ASN yang mengenal, memahami, dan mengakui kemungkinan terjadinya Perubahan SPBE, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan Manajemen Perubahan SPBE.
Aspek-aspek yang dapat mendukung budaya Manajemen Perubahan SPBE antara lain:

c. Kepemimpinan
Tim koordinasi SPBE harus dapat menunjukkan sikap kepemimpinan, yaitu konsisten dalam perkataan dan tindakan, mampu mendorong atau menggerakkan ASN dalam penerapan budaya Manajemen Perubahan SPBE, mampu menempatkan Manajemen Perubahan SPBE sebagai agenda penting di dalam setiap pengambilan keputusan yang terkait dengan penerapan SPBE, dan memiliki komitmen yang kuat menerapkan Manajemen Perubahan SPBE melalui penyediaan sumber daya yang cukup, baik anggaran, SDM, kebijakan, pedoman, maupun strategi penerapannya di Instansi Pusat dan Pemerintah Daerah.

d. Keterlibatan Semua Pihak
Budaya Manajemen Perubahan SPBE melibatkan semua ASN yang terkait secara langsung maupun tidak langsung dengan penerapan SPBE, baik ASN yang berada pada tim koordinasi SPBE, UPMP SPBE, maupun Agen Perubahan, karena mereka yang paling memahami terjadinya Perubahan SPBE dan cara penanganannya dalam level strategis maupun operasional.

e. Komunikasi
Komunikasi tentang pentingnya Manajemen Perubahan SPBE harus dapat disampaikan kepada setiap ASN yang terlibat dalam penerapan

SPBE melalui penyediaan saluran komunikasi yang variatif dan efektif. Tidak hanya tim koordinasi SPBE menyampaikan informasi terkait kebijakan Manajemen Perubahan SPBE kepada ASN, tetapi juga ASN dapat menyampaikan informasi Perubahan SPBE kepada pimpinan di setiap jenjang termasuk kepada tim koordinasi SPBE. Saluran komunikasi ini dapat diwujudkan melalui rapat-rapat pengambilan keputusan, berbagai pertemuan dalam proses Manajemen Perubahan SPBE, dan penyampaian informasi melalui saluran komunikasi elektronik seperti surat elektronik, sistem naskah dinas elektronik, sistem aplikasi manajemen perubahan, video conference, dan lain sebagainya.

f. Daya Responsif
   Dalam budaya sadar Perubahan SPBE, Perubahan SPBE ditangani kepada pihak yang bertanggung jawab agar mendapat penanganan yang cepat dan tepat. Sikap responsif ini sangat penting untuk mencegah ancaman yang dapat menghambat tercapainya tujuan penerapan SPBE ataupun meraih peluang untuk mempercepat tercapainya tujuan penerapan SPBE termasuk peningkatan kualitasnya. ASN yang responsif akan lebih siap beradaptasi terhadap perubahan dan penyelesaian masalah yang rumit dalam penerapan SPBE.
g. Sistem Penghargaan
   Tim koordinasi SPBE hendaknya memahami secara langsung permasalahan yang dialami oleh ASN pada pelaksanaan tugas UPMP SPBE dan Agen Perubahan, serta menjadikan pencapaian kinerja Perubahan SPBE sebagai salah satu indikator dalam pemberian penghargaan dan sanksi.
h. Integrasi Proses
   Proses Manajemen Perubahan SPBE hendaknya diintegrasikan dengan proses manajemen di Instansi Pusat dan Pemerintah Daerah sehingga tidak dipandang sebagai tambahan beban pekerjaan. Integrasi proses dapat dilakukan dengan menyelaraskan proses Manajemen Perubahan SPBE sebagai satu kesatuan dari setiap proses kegiatan, proses manajemen perubahan, dan proses manajemen kinerja Instansi Pusat dan Pemerintah Daerah.
i. Program Kegiatan Berkelanjutan
   Agar budaya Manajemen Perubahan SPBE dapat diterima oleh ASN, tim koordinasi SPBE hendaknya menyusun program kegiatan budaya Manajemen Perubahan SPBE secara sistematis dan terencana, seperti kegiatan edukasi, berbagi pengetahuan, dan kunjungan kerja/supervisi ke UPMP SPBE.

H. MANAJEMEN LAYANAN SPBE

1. Pelayanan Pengguna SPBE
   a. Layanan *Service Desk*
      1) Untuk layanan administrasi pemerintahan berbasis elektronik, Unit Kerja yang menyelenggarakan urusan Layanan SPBE harus menyediakan fungsi *Service Desk* dan ditetapkan oleh Pimpinan Unit Kerja.
      2) Untuk layanan publik berbasis elektronik, Sekretariat Jenderal menyediakan *Service Desk* sebagai *single point of contact*.
      3) Unit Kerja yang menyelenggarakan urusan layanan publik berbasis elektronik harus mendukung *Service Desk* dalam hal melakukan pengelolaan insiden, permintaan, dan perubahan Layanan SPBE dari pengguna SPBE sesuai dengan tugas dan fungsinya.
      4) *Service Desk* mempunyai tugas memberikan layanan kepada pengguna SPBE dengan memberikan solusi yang sesuai dengan kesepakatan tingkat layanan (*service level agreement*) dan/atau target indikator kinerja (*key performance indicator* – KPI) untuk mengatasi insiden dan permintaan Layanan SPBE dari pengguna SPBE.
      5) *Service Desk* untuk layanan publik berbasis elektronik melakukan pengelolaan insiden, dan/atau permintaan layanan SPBE meliputi penerimaan dan pencatatan pelaporan, analisis, penyelesaian, dan/atau eskalasi penyelesaiannya, serta pemantauan dan menginformasikan statusnya kepada pengguna SPBE.
      6) Aspek pelaporan ke Unit Datin/Pusdatin pada pelaksanaan *service desk*.

   b. Pengelolaan Insiden Layanan SPBE
      1) Setiap insiden harus dicatat dan dikelola untuk memastikan bahwa insiden tersebut dapat diselesaikan dalam jangka waktu sesuai dengan kesepakatan tingkat layanan SPBE.
      2) Kesepakatan tingkat layanan SPBE didokumentasikan dan dikomunikasikan pada pengguna SPBE.
      3) Insiden diprioritaskan berdasarkan klasifikasi tinggi, sedang atau rendah yang disepakati untuk memastikan bahwa insiden dengan dampak layanan tertinggi diselesaikan terlebih dahulu.
      4) Unit Kerja harus merancang pengelolaan insiden untuk menyediakan manajemen dan alokasi sumber daya yang tepat.
      5) Insiden dengan dampak rendah harus dikelola secara efisien untuk memastikan mereka tidak mengonsumsi terlalu banyak sumber daya.
      6) Insiden dengan dampak yang lebih tinggi memerlukan lebih banyak sumber daya dan manajemen yang lebih kompleks.
      7) Insiden dapat didiagnosis dan diselesaikan oleh orang-orang dalam banyak kelompok fungsi yang berbeda, tergantung pada kompleksitas masalah atau kategori/jenis insiden dan kategori

insiden dapat dibagi atas insiden data, Aplikasi SPBE, Infrastruktur SPBE, dan keamanan informasi.

8) Penanganan insiden bisa melalui proses sebagai berikut:
   a) Beberapa insiden akan diselesaikan oleh pengguna sendiri, secara mandiri menggunakan alat pertolongan yang disediakan (*self-help*) atau FAQ dan penggunaan catatan swadaya khusus harus ditangkap untuk digunakan dalam kegiatan pengukuran dan peningkatan.
   b) Beberapa insiden akan diselesaikan oleh petugas *Service Desk*;
   c) Insiden yang lebih kompleks dapat dieskalasi ke tim pendukung (*support*) untuk penyelesaian dan dalam hal insiden disebabkan oleh permasalahan teknis pada Aplikasi SPBE dan/atau Infrastruktur SPBE, pimpinan Unit Datin berkoordinasi dengan Pusdatin.
   d) Insiden dapat dieskalasi ke pihak di luar Kementerian yang memberikan dukungan untuk produk dan Layanan SPBE.
   e) Untuk kasus insiden ekstrim, rencana pemulihan bencana dapat digunakan untuk menyelesaikan suatu insiden, misal pindah sistem ke Pusat Pemulihan Bencana *(disaster recovery center*).
9) Jika insiden terjadi berulang-ulang karena belum diketahui masalahnya (*unknown error*), maka insiden ini harus ditindaklanjuti dalam pengelolaan masalah.
10) Melakukan penutupan insiden.

c. Pengelolaan Masalah

Langkah untuk mengelola masalah adalah sebagai berikut:

1) Melakukan identifikasi dan mencatat masalah, dengan cara antara lain:
   a) Melakukan analisis tren dari catatan insiden.
   b) Mendeteksi insiden yang terjadi berulang oleh pengguna, petugas *Service Desk*, dan staf dukungan teknis.
   c) Selama penanganan insiden besar (major), mengidentifikasi risiko yang dapat terulang kembali; dan
   d) Menganalisis informasi yang diterima dari pihak di luar Kementerian, pengembang perangkat lunak internal, tim pengujian dan tim proyek, atau sumber informasi lain.
2) Melakukan pengendalian masalah meliputi analisis masalah, dan mendokumentasikan penyelesaian masalah serta kesalahan yang diketahui, dengan cara tahapan sebagai berikut:
   a) Melakukan analisis masalah untuk mencari sumber penyebabnya dan memprioritaskan analisis masalah yang paling besar risiko yang ditimbulkannya, yaitu berdasarkan potensi dampak terhadap Layanan SPBE dan probabilitasnya terjadinya.
   b) Melakukan identifikasi komponen yang salah/*error* atau sumber penyebabnya.

c) Menemukan *workaround* yang bisa dilakukan untuk mengatasi insiden di masa mendatang, berdasarkan pada pemahaman tentang masalah tersebut ketika masalah tidak dapat diselesaikan dengan tuntas; dan
d) Masalah yang sudah diketahui dan ada solusinya harus didokumentasikan dalam sebuah pengetahuan.

3) Melakukan pengendalian kesalahan (*error*) yang telah diidentifikasi dan melakukan identifikasi potensi permanen solusi yang dapat menghasilkan permintaan perubahan untuk implementasi solusi permanennya. Kegiatan pengendalian kesalahan terdiri atas tahapan sebagai berikut:
a) Menilai kembali status kesalahan yang diketahui dan belum diselesaikan, termasuk dampak keseluruhan pada pengguna SPBE, ketersediaan dan biaya resolusi permanen, dan efektivitas penyelesaian masalah.
b) Melakukan identifikasi potensi permanen solusi dengan mempertimbangkan biaya, risiko, dan manfaatnya.
c) Mengajukan permintaan perubahan (*change request*) untuk implementasi solusi permanen berdasarkan pertimbangan yang dilakukan.
d) *Workaround* insiden yang efektif dapat menjadi cara permanen untuk menangani beberapa masalah ketika menyelesaikan masalah secara tuntas (permanen) tidak tersedia atau tidak hemat biaya. Efektivitas penyelesaian masalah harus dievaluasi setiap kali pemecahan masalah digunakan, karena penyelesaian mungkin ditingkatkan berdasarkan penilaian.

d. Pengelolaan Permintaan Layanan SPBE

Permintaan Layanan SPBE mengacu pada layanan yang sudah tersedia dalam katalog layanan (*service catalogue*) SPBE. Katalog Layanan SPBE memuat informasi antara lain:
1) Nama Layanan SPBE.
2) Deskripsi layanan dan ringkasan karakteristik/spesifikasi layanan.
3) Khusus layanan publik, jangka waktu atau kesepakatan tingkat layanan untuk memenuhi layanan SPBE.
4) Informasi tata cara permohonan layanan SPBE; dan
5) Nomor kontak penanggung jawab layanan jika ada kendala/insiden yang bersifat darurat ketika *Service Desk* tidak bisa dihubungi.

Pengelolaan permintaan dilakukan dengan cara:
1) *Service Desk* menerima permintaan layanan dari pengguna. Permintaan dicatat dan dilakukan validasi.
2) Mengajukan persetujuan kepada pihak yang berwenang untuk permintaan yang sudah divalidasi.

3) Permintaan ditinjau oleh pihak yang berwenang. Jika permintaan disetujui maka segera dipenuhi permintaan sesuai dengan permintaan layanannya.
4) Melakukan penutupan permintaan layanan dan mencatat semua perubahan item konfigurasi jika ada; dan
5) Melakukan evaluasi dan perbaikan atas proses yang terjadi sehingga memungkinkan dilakukan pemenuhan permintaan lebih cepat.

e. Pengelolaan Akses Pengguna

Pengelolaan akses pengguna dilakukan dengan cara sebagai berikut:

1) Permintaan akses pengguna disampaikan melalui *Service Desk* sesuai dengan proses pengelolaan permintaan Layanan SPBE; dan
2) Khusus untuk pengguna pegawai Kementerian, identitas dan status pengguna mengacu pada sistem basis data kepegawaian Kementerian dan jika status kepegawaian sudah tidak aktif lagi maka otomatis akses pengguna pegawai yang bersangkutan menjadi tidak aktif.

f. Pengendalian Perubahan Layanan SPBE

Langkah-langkah untuk mengendalikan perubahan Layanan SPBE adalah sebagai berikut:

1) Setiap perubahan Layanan SPBE dapat diajukan atas permintaan pengguna atau permintaan tim teknis karena usulan perbaikan atas permasalahan yang terjadi. Pengguna atau tim teknis harus mengajukan permintaan perubahan kepada penanggung jawab layanan pada Unit Kerja yang bersangkutan untuk mendapatkan persetujuan terlebih dahulu.
2) Formulir permintaan perubahan antara lain memuat:
   a) Identitas pemohon.
   b) Ruang lingkup perubahan (aplikasi/infrastruktur/.....).
   c) Alasan permohonan; dan
   d) Kajian implikasi atau risikonya jika perubahan ini tidak dilakukan.
3) Pimpinan Unit Kerja yang bersangkutan berkoordinasi dengan Unit Datin dan/atau Pusdatin terkait dengan perubahan konfigurasi Aplikasi dan Infrastruktur Layanan SPBE untuk mengkaji risiko dan mendapatkan pertimbangan teknis sebelum menyetujui permintaan perubahan yang diajukan.
4) Perubahan yang berdampak pada kebutuhan anggaran/ operasional kementerian, dan/atau layanan publik harus diketahui oleh Pimpinan Unit Kerja.
5) Permintaan perubahan yang sudah disetujui, segera ditugaskan kepada tim pelaksana perubahan dan menetapkan jadwal implementasi perubahan sesuai dengan kewenangan yang diberikan.

6) Perubahan yang dilakukan harus diuji terlebih dahulu untuk memastikan bahwa perubahan yang dilakukan tidak berdampak negatif terhadap pelayanan SPBE secara keseluruhan.
7) Pelaksanaan perubahan, pengujian dan rilis hasil perubahan Aplikasi SPBE terhadap Layanan SPBE sesuai dengan ketentuan peraturan perundang-undangan.
8) Unit Kerja yang menyelenggarakan urusan layanan bertanggung jawab untuk memastikan bahwa setiap perubahan terhadap aset TIK yang dikelolanya sudah melalui proses penilaian, persetujuan, pengujian, implementasi dan peninjauan yang terkontrol.
9) Setiap perubahan konfigurasi pada aset TIK harus dicatat, dan diperbarui sesuai dengan peraturan perundang-undangan.

2. Pengoperasian Layanan SPBE
Kegiatan Pengoperasian Layanan SPBE sebagai berikut:
a. Perencanaan dan Pemantauan Kapasitas
1) Melakukan perencanaan kapasitas infrastruktur TIK dengan memperhatikan rencana pembangunan dan/atau pengembangan sistem informasi sesuai dengan arsitektur dan Peta Rencana SPBE Kementerian.
2) Unit Datin berkoordinasi dengan Pusdatin dalam:
a) penyediaan kapasitas sumber daya Infrastruktur SPBE yang memadai sesuai kebutuhan,
b) pelaksanaan pemantauan penggunaan kapasitas, dan
c) pelaksanaan evaluasi kecukupan kapasitas secara berkala sesuai dengan ambang batas (*threshold*) yang ditetapkan.
3) Jika ambang batas sudah tercapai, maka perlu dilakukan tindakan untuk meningkatkan kapasitas yang tersedia sesuai dengan kebutuhan pengguna di masa depan.
4) Hasil pemantauan dan pengukuran dianalisis dan dievaluasi untuk menilai tingkat ketersediaan kapasitas dan utilisasi Infrastruktur SPBE dan Aplikasi SPBE (misalnya jumlah pengguna, pertumbuhan pengguna, jumlah transaksi per hari, dan sebagainya) dan menyiapkan rencana aksi jika ada hal-hal yang perlu ditindaklanjuti.
5) Hasil analisis dan evaluasi kapasitas Infrastruktur SPBE dan Aplikasi SPBE didokumentasikan dan dilaporkan kepada Kepala Pusdatin secara periodik untuk mendapatkan masukan dan arahan.
6) Unit Organisasi, Unit Kerja, dan UPT mengutamakan pemanfaataan infrastruktur bagi pakai nasional.
a) Menggunakan PDN sebagai layanan utama atau *mirroring* dalam hal penggunaan layanan di luar PDN
b) Menggunakan layanan komputasi awan yang ditetapkan oleh Pusdatin, dalam hal dilakukan penggunaan layanan komputasi awan di luar yang ditetapkan harus dikoordinasikan dengan Pusdatin.

b. Operasional Infrastruktur SPBE dan Aplikasi SPBE
   1) Lingkup tanggung jawab dalam pengelolaan infrastruktur jaringan di kampus Kantor Pusat Kementerian:
      a) Pusdatin mengelola konfigurasi logis dari *firewall – end user* serta pengadaan perangkat keras dari *firewall* dan *backbone* s.d distribution *switch* gedung,
      b) Pusdatin melaksanakan pemantauan dan pengawasan seluruh infrastruktur jaringan di kampus Kementerian PU Pusat, dan Unit Datin melaksanakan pemantauan dan pengawasan di lingkungan unit organisasinya.
      c) Unit Datin bertanggung jawab atas pengadaan dan pengelolaan perangkat keras jaringan dan seluruh perangkat pendukung pada layer *switch access* dan *access point* di luar ketentuan pada poin a dan b.
      d) Unit Datin berkoordinasi dengan Pusdatin dalam pelaksanaan poin c.
      e) Pemantauan dan optimalisasi jaringan di lingkungan Kampus Kementerian PU Pusat dikoordinasikan secara terpusat oleh Pusdatin.
   2) Pengelolaan infrastruktur jaringan di luar kampus Kementerian dilaksanakan oleh Unit kerja/UPT terkait dan berkoordinasikan dengan Unit Datin dan Pusdatin.
   3) Setiap unit organisasi, unit kerja/UPT yang bertanggung jawab dalam pengelolaan fasilitas, Infrastruktur SPBE, dan Aplikasi SPBE harus memastikan ketersediaan sumber daya manusia sebagai petugas pengelola.
   4) Setiap petugas pengelola fasilitas, Infrastruktur SPBE, dan Aplikasi SPBE harus mempunyai kompetensi yang sesuai dengan bidang tugasnya dan dalam hal kompetensi internal tidak tersedia, maka pengelolaan dapat dilakukan secara alih daya (*outsource*) ke pihak di luar Kementerian sesuai ketentuan peraturan perundang-undangan.
   5) Setiap petugas pengelola fasilitas, Infrastruktur SPBE, dan Aplikasi SPBE harus mendapat pelatihan untuk setiap penambahan sistem baru yang dikelola.
   6) Pengelola operasional harus memastikan penempatan perangkat di dalam ruang perangkat sesuai dengan ketentuan.
   7) Pengelola operasional harus memelihara dokumentasi sistem dan Infrastruktur SPBE pendukung yang dikelolanya mencakup antara lain:
      a) Dokumentasi petunjuk penggunaan sistem (*user manual*).
      b) Dokumentasi petunjuk pendukung teknis (*technical manual*).
      c) Prosedur pengoperasian dan pemulihan (*recovery*) jika diperlukan; dan
      d) Nama-nama dan nomor kontak petugas pendukung teknis.
   8) Penyusunan prosedur operasional mencakup antara lain:

a) Standar Teknis, yang memuat ketentuan teknis pengelolaan sistem, dan infrastruktur perangkat keras/perangkat lunak pendukung operasional Layanan SPBE.
b) Prosedur Operasional Standar, yang memuat standar alur kerja pengelolaan sistem, dan infrastruktur perangkat keras/perangkat lunak pendukung operasional Layanan SPBE.
c) Instruksi teknis (*working instruction*) yang menjadi acuan dalam pelaksanaan pengoperasian perangkat sistem, dan infrastruktur perangkat keras/perangkat lunak pendukung operasional Layanan SPBE; dan
d) Formulir atau dokumen pendukung yang diperlukan untuk mempermudah pelaksanaannya seperti *checklist*, surat, dan laporan.

9) Setiap perangkat harus diberi label/identitas yang jelas sesuai dengan ketentuan peraturan perundang-undangan mengenai aset (*asset naming convention*) serta topologi atau arsitektur teknis (*configuration item naming convention*) terkait.
10) Fungsi pencatatan (*logging*) yang ada di perangkat harus diaktifkan dan *file* hasil pencatatan (*log file*) harus disimpan selama jangka waktu tertentu sesuai dengan kebutuhan atau ketentuan peraturan perundang-undangan.
11) Melakukan pemantauan, pengukuran dan pelaporan dari ketersediaan Infrastruktur SPBE dan Aplikasi SPBE termasuk kesiapan pemulihan dari kegagalan Layanan SPBE sehingga dapat pulih dan berjalan normal dalam waktu yang singkat.
12) Petugas kendali operasional menjalankan tugas-tugas rutin yang telah ditentukan sesuai dengan prosedur, antara lain:
    a) Pemantauan kinerja sistem.
    b) Pemantauan kapasitas sistem (*processor, memory, disk*, dan *bandwidth*).
    c) Pemantauan jaringan komunikasi data.
    d) Pemantauan *job* yang sedang berjalan.
    e) Pemantauan aktivitas orang selain yang bertugas di lokasi kendali operasional SPBE.
    f) Pelaksanaan proses *batch*; dan
    g) Pelaksanaan pencadangan (*backup*) data, pengamanan media pencadangan, dan serah terima media pencadangan ke pihak terkait.
13) Petugas kendali operasional mencatat setiap kegiatan yang terjadi selama jadwal tugasnya sesuai dengan standar teknis & prosedur Layanan Service Desk.
14) Aktivitas proses operasional, pemantauan Infrastruktur SPBE dan proses *batch* sebaiknya diotomasikan untuk efektivitas dan efisiensi proses dan telah melalui serangkaian proses uji coba yang memadai sebelum diimplementasikan.

c. Pemeliharaan Infrastruktur SPBE dan Aplikasi SPBE
   1) Pengelola operasional melakukan pemeliharaan secara teratur sesuai dengan ketentuan dengan mempertimbangkan hasil analisis biaya dan manfaat, rekomendasi dari pihak di luar Kementerian, risiko-risiko kegagalan sistem, dan faktor terkait lainnya.
   2) Pengelola operasional melakukan reviu terhadap pencatatan sistem (*system logs,* jika ada) untuk mendeteksi gejala-gejala kegagalan sistem.
   3) Pemberian akses kepada pihak di luar Kementerian untuk pelaksanaan pemeliharaan sistem harus sesuai dengan ketentuan peraturan perundang-undangan.
   4) Operasionalisasi sistem harus mempertimbangkan metode pemeliharaan rutin yang optimal guna menghindari terjadinya *downtime* pada sistem.
   5) Kegiatan pemeliharaan yang dapat mengganggu kegiatan pengguna sistem harus dilakukan pada saat sistem tidak digunakan, yaitu di luar waktu jam Layanan SPBE.
   6) Jika kegiatan pemeliharaan yang dimaksud pada butir 5 di atas harus dilakukan di dalam waktu jam Layanan SPBE, maka harus dilakukan pemberitahuan kepada pengguna Layanan SPBE sebagai berikut:
      a) Alasan pemeliharaan harus dilakukan.
      b) Perkiraan lama masa pemeliharaan; dan
      c) Langkah-langkah alternatif yang mungkin dapat dilakukan oleh pengguna layanan.
   7) Perubahan terhadap sistem yang dilakukan saat pemeliharaan harus tercatat sesuai dengan ketentuan peraturan perundang-undangan.

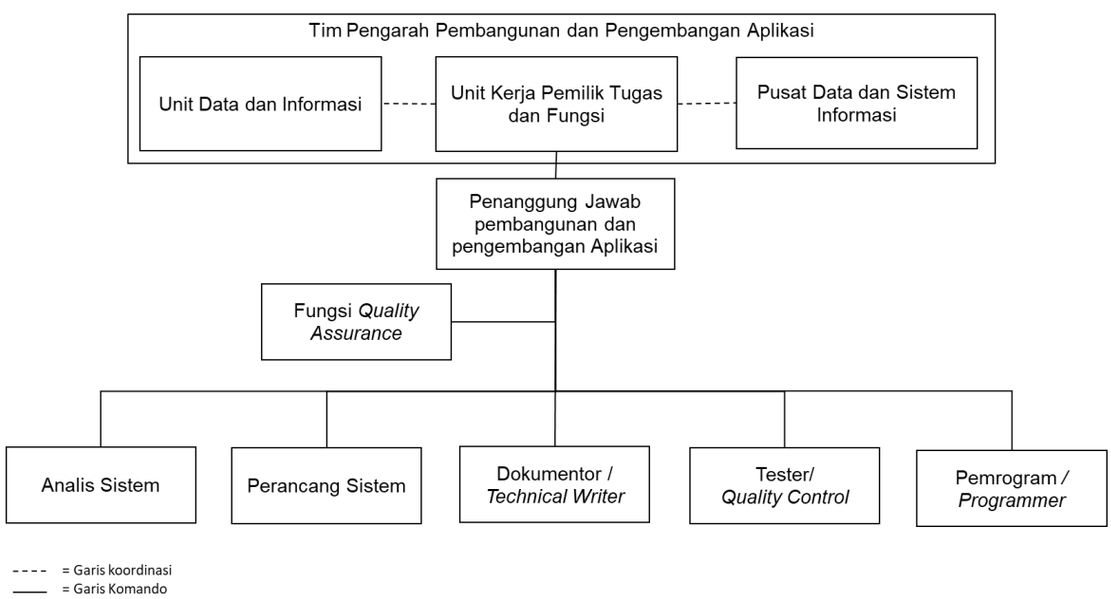
d. Pemantauan dan Evaluasi Layanan Pihak di luar Kementerian
   1) Pengguna dan pihak di luar Kementerian/penyedia jasa harus menyepakati prosedur pelaporan gangguan dan eskalasinya secara berjenjang.
   2) Pihak di luar Kementerian/penyedia jasa harus memberikan laporan secara berkala untuk diperiksa oleh pengguna barang dan/atau jasa.
   3) Kinerja pihak di luar Kementerian/penyedia jasa dalam mencapai tingkat layanan yang disepakati dalam kontrak harus ditinjau secara berkala.
   4) Tingkat layanan yang tidak tercapai harus dilaporkan dan ditindaklanjuti untuk perbaikan.
   5) Kegagalan pencapaian tingkat layanan secara berturut-turut harus ditindaklanjuti antara lain dengan:
      a) Pembuatan rencana perbaikan oleh pihak di luar Kementerian/penyedia jasa.
      b) Pengenaan denda atau penyesuaian biaya layanan;

c) Pemutusan hubungan kontrak dengan pihak di luar Kementerian/penyedia jasa; dan
d) Dimasukkan dalam daftar hitam sesuai ketentuan peraturan perundang-undangan.

6) Pencapaian tingkat layanan secara konsisten harus ditindaklanjuti antara lain dengan:
a) Peningkatan target tingkat layanan, jika memungkinkan; dan
b) Pengurangan biaya layanan, jika memungkinkan.

7) Khusus untuk pihak di luar Kementerian/penyedia barang dan/atau jasa kritikal, harus dilakukan analisis risiko berupa evaluasi kelangsungan usahanya untuk memastikan kemampuannya dalam menyediakan dukungan Layanan SPBE.

3. Pengoperasian Aplikasi SPBE
a. Tim Pembangunan dan Pengembangan Aplikasi SPBE
Untuk pembangunan dan pengembangan Aplikasi SPBE:
1) Aplikasi layanan publik, aplikasi teknis, dan aplikasi pendukung, tim pembangunan dan pengembangan Aplikasi SPBE ditetapkan oleh Pimpinan Unit Kerja/UPT Pemilik Layanan SPBE; dan
2) Aplikasi tingkat Kementerian, tim pengembangan Aplikasi SPBE ditetapkan oleh kepala Pusdatin.
3) Struktur organisasi tim pembangunan dan pengembangan Aplikasi SPBE setidaknya memiliki fungsi-fungsi seperti pada gambar di bawah ini:




Gambar 20 Struktur Organisasi Tim Pembangunan dan Pengembangan Aplikasi SPBE

a) Tim Pengarah Pembangunan dan Pengembangan Aplikasi
Tim Pengarah Pembangunan dan Pengembangan Aplikasi terdiri atas:
(1) Unit Datin.
(2) Unit Kerja Pemilik Tugas dan Fugsi.

(3) Pusat Data dan Sistem Informasi.

Unit Kerja Pemilik Tugas dan Fugsi bertindak sebagai Ketua Tim Pengarah Pembangunan dan Pengembangan Aplikasi.

Tim Pengarah Pembangunan dan Pengembangan Aplikasi memiliki tanggungjawab:

(1) Mengawasi, mengarahkan dan memastikan keberhasilan pelaksanaan pembangunan dan pengembangan aplikasi agar tetap selaras dengan kebutuhan Unit Organisasi, Unit Kerja, dan UPT.
(2) Menetapkan arah dan kebijakan, termasuk arahan strategis dalam pelaksanaan pembangunan dan pengembangan aplikasi
(3) Melakukan monitoring dan evaluasi proses pembangunan dan pengembangan aplikasi
(4) Menetapkan keputusan kunci (*decision-making authority*) selama proses pembangunan dan pengembangan aplikasi
(5) Menjamin manfaat pembangunan dan pengembangan aplikasi terhadap kebutuhan Unit Organisasi, Unit Kerja, dan UPT.
(6) Memberikan solusi terhadap eskalasi kendala/ masalah yang tidak dapat diselesaikan pada tingkat Tim Pembangunan dan Pengembangan Aplikasi.

b) Penanggung Jawab Pembangunan dan Pengembangan Aplikasi

Penanggung Jawab Pembangunan dan Pengembangan Aplikasi dapat diperankan oleh pemilik Layanan SPBE atau yang mewakili, memiliki tanggung jawab:

(1) Memastikan proses pembangunan dan pengembangan aplikasi berjalan sesuai dengan rencana yang dijadwalkan dan sumber daya yang ditetapkan.
(2) Mengelola personil yang terlibat dalam tim pengembang aplikasi.
(3) Bertindak sebagai penghubung antara tim pengembang aplikasi dengan pemilik Layanan SPBE, Tim Pengarah Pembangunan dan Pengembangan Aplikasi, dan pihak terkait lainnya.
(4) Bertindak sebagai Manajer Proyek pembangunan dan pengembangan aplikasi dengan menerapkan *best practices* dalam pengelolaan proyek.
(5) Memastikan ketersediaan dan penerapan *tools* sesuai dengan kerangka kerja pembangunan/pengembangan aplikasi yang ditetapkan oleh Pusdatin.
(6) Memastikan ketersediaan peran dan fungsi sekurang-kurangnya sebagaimana pada struktur organisasi tim pembangunan dan pengembangan aplikasi. Penanggung jawab pembangunan dan pengembangan aplikasi dapat

menambahkan fungsi-fungsi pada tim pembangunan dan pengembangan aplikasi apabila diperlukan.

(7) Menyampaikan laporan status pembangunan dan pengembangan aplikasi kepada Tim Pengarah Pembangunan dan Pengembangan Aplikasi; dan

(8) Melakukan eskalasi permasalahan kepada Tim Pengarah Pembangunan dan Pengembangan Aplikasi jika terdapat kendala/masalah yang tidak dapat diselesaikan pada tingkat Tim Pembangunan dan Pengembangan Aplikasi.

c) *Quality Assurance* (QA)

Fungsi QA dapat merangkap sebagai Tester untuk jenis *integration testing* dan *system testing*. Fungsi QA harus bersifat independen.

Tugas dan tanggung jawab QA antara lain:

(1) Memastikan bahwa *output* setiap fase pembangunan dan pengembangan aplikasi telah memenuhi kriteria yang ditetapkan untuk tiap fasenya.

(2) Untuk pembangunan dan pengembangan aplikasi oleh pihak di luar Kementerian/penyedia jasa, maka Kepala Datin atau Kepala Pusdatin membentuk tim pendamping pembangunan dan pengembangan aplikasi sebagai fungsi QA internal Kementerian untuk memastikan bahwa pembangunan dan pengembangan Aplikasi SPBE yang dilakukan oleh pihak di luar Kementerian/penyedia jasa berjalan sesuai dengan ketentuan peraturan perundang-undangan.

d) Analis Sistem

Tugas dan tanggung jawab Analis Sistem antara lain:

(1) Mengumpulkan kebutuhan pengguna (*user requirement)* dari Pemilik Layanan SPBE dan pihak terkait lainnya sesuai dengan Proses Bisnis yang telah ditetapkan.

(2) Menyusun *user requirement* dan mendefinisikan *Software Requirement Specification* (SRS) secara rinci sesuai dengan kriteria yang ditetapkan.

(3) Melakukan dokumentasi *user requirement* dan SRS sesuai dengan standar yang ditetapkan sebagaimana terlampir; dan

(4) Melakukan analisis dan rekomendasi permintaan perubahan serta melakukan pembaruan dokumentasi karena perubahan yang terjadi.

e) Perancang Sistem

Tugas dan tanggung jawab Perancang Sistem antara lain:

(1) Melakukan perancangan sistem sesuai dengan dokumen SRS, terdiri atas perancangan umum dan perancangan rinci, sesuai dengan standar yang ditetapkan.

(2) Melakukan koordinasi dengan Tim Keamanan Teknologi Informasi terkait dengan penerapan standar teknis dan prosedur keamanan yang relevan.

(3) Mendokumentasikan hasil rancangan sistem dalam *Software Description Design* (SDD) sebagaimana terlampir; dan
(4) Melakukan analisis dan rekomendasi permintaan perubahan serta melakukan pembaruan dokumentasi karena perubahan yang terjadi.

f) Dokumentor/*Technical Writer*
Tugas dan tanggung jawab Dokumentor/*Technical Writer* antara lain:
(1) Melaksanakan penulisan dokumen teknis untuk setiap fase pembangunan dan pengembangan aplikasi sesuai dengan standar penulisan dokumen yang ditetapkan.
(2) Melaksanakan penyusunan dokumen petunjuk pengguna (*admin & user manual*) aplikasi, dokumen tahapan penanganan masalah (*exception* atau *known error)*, serta dokumentasi rencana pemeliharaan beserta pembaruannya jika terjadi perubahan.
(3) Melaksanakan pengendalian dan pengelolaan dokumentasi teknis pembangunan dan pengembangan aplikasi;
(4) Melaksanakan koordinasi dengan Analis Sistem, Perancang Sistem, Pemrogram, dan pihak terkait lainnya dalam pelaksanaan pengendalian dan pengelolaan dokumentasi teknis; dan
(5) Melakukan koordinasi dengan QA untuk memastikan Analis Sistem, Perancang Sistem, Pemrogram, dan pihak terkait lainnya mendokumentasikan pekerjaannya sesuai dengan standar yang ditetapkan.

g) *Tester*
*Tester* dapat merupakan bagian dari QA, dengan tugas dan tanggung jawab antara lain:
(1) Melakukan koordinasi dengan seluruh pihak terkait dalam pembangunan dan pengembangan aplikasi untuk pelaksanaan pengujian aplikasi sesuai dengan jenis pengujiannya.
(2) Menyusun *test plan, test scenario*, dan *test case* untuk *integration testing* dan *system testing*.
(3) Menyusun *test plan, test scenario*, dan *test case* untuk *User Acceptance Testing* (UAT) bersama dengan pemilik Layanan SPBE atau yang mewakili.
(4) Melakukan pengujian sesuai dengan *test plan, test scenario,* dan *test case* yang telah disusun.
(5) Melakukan *integration testing* dan *system testing*; dan
(6) Mendokumentasikan hasil pengujian dalam dokumen tahap pengujian sebagaimana terlampir.

h) Pemrogram/*Programmer*
Tugas dan tanggung jawab Pemrogram/*Programmer* antara lain:

(1) Melakukan pengkodean atau konfigurasi aplikasi yang dibuat sesuai dengan SDD rinci.
(2) Menerapkan prinsip-prinsip *secure coding* dalam pengkodean aplikasi.
(3) Menggunakan repositori terpusat yang ditetapkan Pusdatin pada proses pengkodean pembangunan dan pengembangan aplikasi.
(4) Melakukan unit *testing* untuk setiap modul yang dibuat.
(5) Melakukan *bug fixing* terhadap hasil *unit testing;* dan
(6) Melakukan dokumentasi hasil pengkodean atau konfigurasi aplikasi.

b. Pembangunan dan pengembangan Aplikasi SPBE yang dilakukan oleh pihak di luar Kementerian/penyedia jasa melalui proses tender/pengadaan, tim pembangunan dan pengembangan Aplikasi SPBE dibentuk oleh penyedia jasa pihak di luar Kementerian/penyedia jasa dengan struktur organisasi yang sesuai dengan standar yang berlaku di Kementerian.
c. Ketentuan Pembangunan dan Pengembangan Aplikasi SPBE
   1) Persyaratan Umum
      a) Pembangunan dan pengembangan Aplikasi SPBE dilakukan dengan mengacu pada Arsitektur SPBE dan Peta Rencana SPBE Kementerian.
      b) Pembangunan dan pengembangan Aplikasi SPBE harus dikoordinasikan secara berjenjang dengan Unit Datin serta Pusdatin sejak tahap perencanaan.
      c) Aplikasi SPBE menggunakan standar desain yang mudah diakses (desain responsif) melalui berbagai perangkat (misalnya *desktop*, *mobile device*).
      d) Aplikasi SPBE mengutamakan penggunaan kode sumber terbuka dengan mempertimbangkan aspek-aspek keamanan, kinerja, dukungan teknis, keberlanjutan, serta biaya/manfaat.
      e) Aplikasi SPBE harus menyediakan fitur interoperabilitas untuk integrasi antar Aplikasi SPBE.
      f) Aplikasi SPBE mengoptimalkan penggunaan teknologi komputasi awan dan standar teknologi terbuka. Penggunaan teknologi awan dikoordinasikan oleh Unit Datin dan Pusdatin.
      g) Pemanfaatan lisensi secara optimal pada Aplikasi SPBE dengan mempertimbangkan jumlah dan jenis pengguna, jumlah perangkat, jumlah sumber daya, ukuran data, dan wilayah geografis.
      h) Aplikasi SPBE yang dicatatkan sebagai barang milik negara mengikuti ketentuan peraturan perundang-undangan.
      i) Memenuhi ketentuan Audit TIK sesuai dengan ketentuan peraturan perundang-undangan, memperhatikan rekomendasi hasil Audit TIK, dan hasil evaluasi terhadap

penyelenggaraan Aplikasi SPBE sebelum melakukan pembangunan dan pengembangan Aplikasi SPBE.

j) Memenuhi ketentuan standar teknis dan prosedur keamanan Aplikasi SPBE sesuai dengan ketentuan peraturan perundang-undangan.

2) Persyaratan Pemanfaatan Infrastruktur

a) Aplikasi SPBE dikelola, diproses, dan disimpan di Pusat Data Nasional, dan/atau infrastruktur lain dengan persetujuan Pusdatin.

b) Aplikasi SPBE menggunakan jaringan intra pemerintah, dan/atau jaringan intra Kementerian.

c) Aplikasi SPBE menggunakan Sistem Penghubung Layanan pemerintah, dan/atau Sistem Penghubung Layanan Kementerian.

3) Siklus Pembangunan dan Pengembangan Aplikasi SPBE

a) Proses pembangunan dan pengembangan Aplikasi SPBE Kementerian menggunakan pendekatan *Secure Software Development Life Cycle* (S-SDLC) yang terdiri atas tahap-tahap sebagai berikut:

(1) Perencanaan (*planning*).
(2) Analisis (*analysis*).
(3) Perancangan (*design*).
(4) Pengkodean (*coding*).
(5) Pengujian (*testing*).
(6) Implementasi (*implementation).*
(7) Reviu pasca implementasi *(post implementation review);* dan
(8) Pemeliharaan (*maintenance*).

b) Dalam pemilihan metodologi pembangunan dan pengembangan Aplikasi SPBE harus mempertimbangkan jenis Layanan SPBE. Metodologi pembangunan dan pengembangan Aplikasi SPBE dapat menggunakan kerangka kerja *spiral, rapid application development, waterfall, agile development cycle*, atau kerangka kerja lainnya.

c) Siklus pembangunan dan pengembangan Aplikasi SPBE dapat dilaksanakan dengan berpedoman pada Standar Nasional Indonesia yang disesuaikan dengan karakteristik Aplikasi SPBE.

d) Pembangunan dan pengembangan Aplikasi SPBE Kementerian dapat menggunakan *Computer Aided Software Engineering* (CASE) *Tool*.

e) Pusdatin menyiapkan kriteria yang objektif dan dapat diterima pada setiap tahap dalam pembangunan dan pengembangan Aplikasi SPBE.

f) Pusdatin menyiapkan standar penulisan dokumen dalam setiap tahap dalam pembangunan dan pengembangan

Aplikasi SPBE.

g) Setiap tahap pembangunan dan pembangunan Aplikasi SPBE didokumentasikan sesuai dengan standar penulisan dokumen.

h) Permintaan perubahan dalam setiap tahap pembangunan dan pengembangan Aplikasi SPBE sesuai dengan ketentuan peraturan perundang-undangan.

i) Untuk pengembangan jenis Aplikasi SPBE teknis dan jenis aplikasi pendukung maka dokumentasi sekurang-kurangnya adalah *software spesification requirements* dan dokumen pengujian *User Acceptance Test* (UAT).

4) Tahap Perencanaan

a) Setiap perencanaan pembangunan dan pengembangan Aplikasi SPBE dilakukan mengikuti ketentuan peraturan perundang-undangan.

b) Penyusunan perencanaan dilakukan oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor berkoordinasi dan berkonsultasi dengan Pusdatin secara berjenjang melalui Unit Datin.

c) Penyusunan perencanaan

(1) Berdasarkan pendefinisian kebutuhan Aplikasi SPBE, Arsitektur SPBE Kementerian, dan Peta Rencana SPBE Kementerian.

(2) Pendefinisian Kebutuhan Aplikasi SPBE

(a) Disusun oleh Unit Kerja atau Unit Organisasi pemilik layanan dan berkoordinasi dengan Pusdatin secara berjenjang melalui Unit Datin jika diperlukan.

(b) Dapat direviu secara berkala atau sewaktu-waktu sesuai kebutuhan oleh tim koordinasi SPBE;

(c) Paling sedikit memuat:

i. Dasar hukum kewenangan untuk membangun dan mengembangkan Aplikasi SPBE yang diusulkan.

ii. Uraian permasalahan dan kebutuhan yang melatarbelakangi pembangunan dan pengembangan Aplikasi SPBE, termasuk hasil audit dan/atau evaluasi terhadap Aplikasi SPBE.

iii. Pihak yang terkait dalam Penyelenggaraan Aplikasi SPBE.

iv. Maksud dan tujuan pemanfaatan Aplikasi SPBE.

v. Ruang lingkup Aplikasi SPBE.

vi. Analisis biaya dan manfaat.

vii. Analisis risiko.

viii. Target waktu kesiapan penerapan Aplikasi

SPBE.

ix. Sasaran pengguna.

x. Lokasi implementasi.

(3) Memperhatikan skalabilitas dan performa untuk mengakomodasi pertumbuhan jumlah akses dan data.

(4) Menggunakan komponen-komponen yang bersifat modular pada data, logika komputasi, dan antarmuka.

(5) Menggunakan kode sumber:

(a) Mempertimbangkan keandalan, performa, keberlangsungan, dan keamanan Aplikasi SPBE.

(b) Menerapkan versi terkini dan stabil dari Kode Sumber.

(c) Mencatat perubahan Kode Sumber dalam arsip rekam jejak dalam *source code repository* Kementerian untuk menjaga keterlacakan.

(6) Menggunakan Komponen Umum Aplikasi yang terdapat pada daftar Komponen Umum Aplikasi yang disediakan oleh Kementerian.

(7) Berbasis layanan bersifat arsitektur layanan *(service-oriented architecture).*

(8) Perencanaan dapat direviu secara berkala atau sewaktu-waktu sesuai kebutuhan oleh tim koordinasi SPBE.

(9) Perencanaan paling sedikit memuat uraian:

(a) Ruang lingkup fungsi dan fitur aplikasi berdasarkan pendefinisian kebutuhan aplikasi yang diusulkan, arsitektur SPBE, dan peta rencana.

(b) Proses Bisnis dan layanan yang terkait.

(c) Kerangka kerja pembangunan dan pengembangan Aplikasi SPBE.

(d) Pemilihan pelaksana pembangunan dan pengembangan Aplikasi SPBE yaitu oleh:

i. Swakelola; atau

ii. Pihak ketiga.

(e) Jadwal dan periode pelaksanaan.

(f) Rencana aksi.

(g) Pemenuhan persyaratan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan.

(h) Sumber daya yang dibutuhkan, meliputi:

i. Manusia.

ii. Anggaran; dan

iii. Sarana pendukung lainnya.

(i) Indikator keberhasilan, yang merupakan faktor-faktor penentu keberhasilan dari penerapan siklus pembangunan dan pengembangan Aplikasi SPBE.

(j) Mekanisme alih pengetahuan dan teknologi.

(k) Mekanisme pemantauan dan pelaporan.

5) Tahap Analisis
   a) Pendefinisian Kebutuhan Pengguna
      (1) Tim Pembangunan dan Pengembangan Aplikasi SPBE melakukan *review* terhadap *user requirement* yang dibuat oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor dan memastikan bahwa semua kriteria *user requirement* yang baik telah dipenuhi.
      (2) Tim Pembangunan dan Pengembangan Aplikasi SPBE dapat melakukan kajian lebih mendalam terhadap *user requirements* yang disampaikan oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor apabila kurang jelas; dan
      (3) *User requirements* ini harus disepakati antara pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor dengan Tim Pembangunan dan Pengembangan Aplikasi SPBE.
   b) Pendefinisian Kebutuhan Aplikasi SPBE
      (1) Tim Pembangunan dan Pengembangan Aplikasi SPBE melakukan analisis terhadap *software requirement* yang dibuat dan memastikan bahwa semua kriteria *software requirement* yang baik telah dipenuhi serta memenuhi *user requirement.*
      (2) *Software Requirement* tersebut harus disepakati oleh Pemilik Proses Bisnis/Pengguna/ Unit Kerja/Unor dan Tim Pembangunan dan Pengembangan Aplikasi SPBE.

6) Tahap Perancangan
   a) Tim Pembangunan dan Pengembangan Aplikasi SPBE memastikan bahwa perancangan Aplikasi SPBE yang dihasilkan telah sesuai dengan *Software Requirement* yang disepakati dan semua kriteria perancangan yang baik telah dipenuhi.
   b) Perancangan aplikasi terdiri atas perancangan umum/konseptual dan perancangan rinci.
   c) Pengesahan perancangan aplikasi yang digunakan dalam pembangunan dan pengembangan Aplikasi SPBE disepakati oleh Tim Pembangunan dan Pengembangan Aplikasi SPBE dan Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor.
   d) Tahap perancangan paling kurang memuat:
      (1) Pemodelan perancangan aplikasi.
      (2) Alur proses Aplikasi SPBE.
      (3) Pemetaan dan keterhubungan fungsi dan basis data dalam Aplikasi SPBE.
      (4) Pemetaan hak akses dan peran untuk pengguna aplikasi.
      (5) Rancangan antarmuka pengguna dan navigasi dari layar ke layar sesuai dengan tingkatan pengguna.
      (6) Rancangan kendali internal yang diperlukan dalam

proses validasi, otorisasi, dan pencatatan aktivitas.

(7) Rancangan integrasi antara aplikasi dengan aplikasi lain; dan

(8) Rancangan kebutuhan penanganan keamanan aplikasi sesuai ketentuan peraturan perundang-undangan.

7) Tahap Pengkodean

a) Pelaksanaan Pengkodean (*coding*) aplikasi dan basis data sesuai dengan rancangan rinci yang telah disetujui.

b) Penulisan kode program (*source code*) disertai dengan penjelasannya.

c) Penulisan *variable* pengkodean dan atribut basis data sesuai dengan *naming convention* yang ditetapkan.

d) Kredensial harus disimpan di luar kode program (*source code*).

e) Pengendalian terhadap kode program (*source code*) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

8) Tahap Pengujian

a) Pengujian dilakukan dengan tahapan sebagai berikut:

(1) Menyusun perencanaan pengujian (*test plan*) yang terdiri atas penentuan jadwal pelaksanaan pengujian, penyiapan lingkungan dan sumber daya.

(2) Mengidentifikasi pengujian yang terdiri atas penentuan ruang lingkup dan kriteria pengujian.

(3) Menyusun rancangan pengujian yang terdiri atas penyiapan alur proses pengujian.

(4) Menetapkan skenario pengujian (*test scenario*) yang terdiri atas penentuan pengujian dengan menggunakan berbagai skenario yang berbeda dan data (*test case).*

(5) Melaksanakan pengujian; dan

(6) Melakukan evaluasi pengujian.

b) Pengujian terhadap suatu Aplikasi SPBE dilakukan secara bertingkat, sebagai berikut:

(1) Pengujian unit (*unit testing*) adalah pengujian masing-masing unit dalam komponen suatu rilis aplikasi untuk memastikan bahwa setiap unit/modul bekerja dengan baik sesuai dengan fungsinya.

(2) Pengujian integrasi (*integration testing*) merupakan pengujian integrasi dari unit-unit/modul dalam suatu aplikasi yang sudah teruji dalam pengujian unit (*unit testing*).

(3) Pengujian sistem (*system testing*) merupakan pengujian integrasi aplikasi yang dibangun/dikembangkan dengan perangkat keras/lunak lain untuk mengetahui apakah integrasi tersebut dapat berjalan dengan baik sesuai dengan kebutuhan.

(4) *User Acceptance Test* (UAT) merupakan uji penerimaan yang dilakukan oleh Pemilik Proses

Bisnis/Pengguna/Unit Kerja/Unor. Suatu aplikasi dikatakan dapat diterima apabila telah lulus dari UAT.

c) *Unit testing* dipersiapkan dan dilakukan oleh masing-masing *programmer* tim pengembangan dan pembangunan Aplikasi SPBE pada lingkungan pembangunan dan pengembangan Aplikasi SPBE (*development environment*).

d) *Integration testing* dipersiapkan dan dilakukan tim pembangunan dan pengembangan Aplikasi SPBE di lingkungan pembangunan dan pengembangan Aplikasi SPBE.

e) *System testing* dipersiapkan dan dilakukan oleh tim pembangunan dan pengembangan Aplikasi SPBE di lingkungan pengujian dengan mengacu kepada *software requirement* dan *system testing* harus mencakup tes fungsional, tes beban, tes regresi, dan tes keamanan. *System testing* wajib dilakukan untuk Aplikasi Layanan Publik dan Aplikasi Tingkat Kementerian.

f) Uji beban atau *stress test*, meliputi pengujian yang memastikan Aplikasi SPBE dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya.

g) Uji keamanan, meliputi pengujian yang memastikan Aplikasi SPBE dapat berfungsi sebagaimana mestinya dengan menjaga keamanan data dan informasi yang terkait dengannya sesuai dengan ketentuan peraturan perundangan undangan.

h) *User Acceptance Testing* dipersiapkan oleh tim pembangunan dan pengembangan Aplikasi SPBE dan dilakukan oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor terkait dan dilakukan di lingkungan (*environment*) pengujian yang mewakili lingkungan produksi, dengan mengacu kepada *user requirement*, kebutuhan aplikasi, dan perancangan sistem yang telah disepakati.

i) Setelah UAT disepakati oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor, maka aplikasi siap untuk memasuki tahap implementasi.

j) Evaluasi pengujian terdiri atas pelaksanaan penilaian terhadap:
   (1) kesesuaian proses pengujian yang sudah dilakukan dengan keseluruhan tahapan pengujian.
   (2) kesesuaian hasil pengujian dengan analisis kebutuhan, perancangan, dan kriteria pengujian; dan
   (3) mendokumentasikan keseluruhan tahapan pengujian.

9) Tahap Implementasi

a) Aplikasi yang dipasang pada lingkungan produksi merupakan Aplikasi SPBE yang sudah memenuhi persyaratan yang ditentukan oleh *Quality Assurance* dan

persyaratan yang ditetapkan oleh pengelola operasional/persyaratan *hosting* di Pusat Data Kementerian sesuai ketentuan peraturan perundang-undangan.

b) Pelatihan diberikan kepada pengelola operasional dan Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor sebelum dipasang di lingkungan produksi.

c) Aplikasi yang akan di *hosting* pada Pusat Data Kementerian harus memenuhi:
   (1) Persyaratan yang ditentukan oleh *Quality Assurance* Tim Pembangunan dan Pengembangan Aplikasi SPBE;
   (2) Persyaratan yang ditetapkan oleh pengelola operasional *hosting* di Pusat Data Kementerian merujuk kepada Pedoman Implementasi CICD Container atau Pedoman Implementasi CICD Non Container.
   (3) Menyertakan dokumen sebagai berikut:
      (a) Manual instalasi.
      (b) Buku petunjuk penggunaan sistem (*user manual*).
      (c) Buku petunjuk pendukung teknis (*technical manual*), dan penanganan masalah (*trouble shooting*).
      (d) Prosedur pengoperasian dan pemulihan (*recovery*) jika diperlukan.
      (e) Nama-nama dan nomor kontak petugas pendukung teknis.
      (f) Manual konfigurasi; dan
      (g) Formulir yang disebutkan dalam Pedoman Implementasi CICD Container atau Pedoman Implementasi CICD Non Container.
   (4) Untuk aplikasi yang dibangun/dikembangkan oleh pihak di luar Kementerian/penyedia jasa, selain persyaratan tersebut di atas pada poin 1-3, harus memenuhi persyaratan yang ditentukan oleh QA internal Kementerian, serta memenuhi persyaratan kesepakatan kontrak sesuai peraturan perundang-undangan.
   (5) setiap Aplikasi SPBE yang sudah diserahterimakan kepada tim pengelola operasional *hosting* di Pusat Data Kementerian harus dilaporkan statusnya kepada Pusdatin melalui Unit Datin.

10) Tahap Evaluasi Pasca Implementasi

a) Pelaksanaan Evaluasi Pasca Implementasi dilaksanakan oleh Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor berkoordinasi dengan Unit Datin.

b) Pelaksanaan evaluasi terhadap pencapaian tujuan pembangunan dan pengembangan Aplikasi SPBE sesuai dengan kebutuhan *user*.

c) Pelaksanaan evaluasi terhadap proses pelaksanaan

pembangunan dan pengembangan Aplikasi SPBE untuk bahan pembelajaran pada proses pembangunan dan pengembangan Aplikasi SPBE selanjutnya.

d) Pelaksanaan evaluasi dapat dilakukan dengan:
   (1) Menyusun kebijakan internal terkait evaluasi pembangunan dan pengembangan Aplikasi SPBE.
   (2) Melakukan pengukuran penilaian indikator keberhasilan sesuai dengan siklus pembangunan dan pengembangan Aplikasi SPBE.
   (3) Menyusun laporan hasil evaluasi.
   (4) Menyampaikan laporan hasil evaluasi kepada pimpinan Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor; dan
   (5) Melaksanakan tindak lanjut hasil evaluasi.

11) Tahap Pemeliharaan

Pemeliharaan Aplikasi SPBE dilakukan sesuai dengan Pemeliharaan Infrastruktur dan Aplikasi SPBE yang diatur dalam Pengoperasian Layanan SPBE. Pemeliharaan Aplikasi SPBE meliputi:

a) Pemeliharaan perfektif, yang merupakan penambahan atau penyempurnaan aplikasi yang meliputi penambahan fungsi baru, perbaikan antarmuka, perbaikan kinerja, perbaikan dokumentasi implementasi.
b) Pemeliharaan adaptif, yang merupakan adaptasi terhadap teknologi atau lingkungan operasional baru, dan penerapan protokol baru.
c) Pemeliharaan korektif, yang merupakan perbaikan terhadap permasalahan yang timbul setelah aplikasi digunakan; dan/atau
d) Pemeliharaan preventif, yang merupakan pemeriksaan aplikasi secara berkala untuk mengantisipasi permasalahan.

12) Persyaratan Data dan Informasi

a) Pembangunan dan pengembangan Aplikasi SPBE harus memenuhi persyaratan data dan informasi dalam rangka mewujudkan data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan pelaksanaan evaluasi dan pengendalian pembangunan nasional.
b) Persyaratan data dan informasi dalam pembangunan dan pengembangan Aplikasi SPBE yaitu:
   (1) memenuhi pedoman manajemen data SPBE sesuai dengan ketentuan peraturan perundang-undangan.
   (2) memenuhi peraturan perundang-undangan kebijakan satu data Indonesia; dan
   (3) Memenuhi keamanan data dan informasi sesuai dengan peraturan perundang-undangan.

13) Persyaratan interoperabilitas data

a) Pembangunan dan pengembangan Aplikasi SPBE harus

memenuhi persyaratan interoperabilitas data dalam rangka mendukung pertukaran data antar Aplikasi SPBE.

b) Persyaratan interoperabilitas dalam pembangunan dan pengembangan Aplikasi SPBE yaitu:
   (1) Memastikan Aplikasi SPBE yang dibangun dan dikembangkan memiliki interoperabilitas data melalui kemampuan antarmuka pemrograman aplikasi.
   (2) Memenuhi kebijakan interoperabilitas data sesuai dengan peraturan perundang-undangan; dan
   (3) Memenuhi keamanan data dan informasi sesuai dengan peraturan perundang-undangan.

14) Persyaratan keberlangsungan Layanan SPBE
   a) Pembangunan dan pengembangan Aplikasi SPBE harus memenuhi persyaratan keberlangsungan layanan.
   b) Pemenuhan Persyaratan keberlangsungan layanan dilakukan dengan cara menyediakan:
      (1) Pelayanan Pengguna SPBE sebagaimana diuraikan pada Bagian G butir (1).
      (2) Pengoperasian Layanan SPBE sebagaimana diuraikan pada Bagian G butir (2).
      (3) Aspek keamanan informasi dari Manajemen Keberlangsungan Layanan SPBE sebagaimana diuraikan pada Bagian A. Manajemen Keamanan Informasi SPBE butir (18).

15) Penerapan Manajemen SPBE
   Seluruh proses pembangunan dan pengembangan Aplikasi SPBE dilakukan dengan berpedoman pada Manajemen SPBE.

16) Dokumentasi atas Aplikasi SPBE
   Pemenuhan dokumentasi Aplikasi SPBE berdasarkan tahap pembangunan dan pengembangan Aplikasi SPBE yang terdiri atas:

   a) Dokumentasi perencanaan.
   b) Dokumentasi analisis kebutuhan.
   c) Dokumentasi perancangan, yang meliputi:
      (1) Dokumen perancangan umum (konseptual).
      (2) Dokumen perancangan detil yang meliputi teknis Aplikasi SPBE dan detail teknis basis data (*database*).
   d) Dokumentasi implementasi, yang meliputi:
      (1) Manual instalasi.
      (2) Buku petunjuk penggunaan sistem (*user manual*).
      (3) Buku petunjuk pendukung teknis (*technical manual*), dan penanganan masalah (*trouble shooting*).
      (4) Prosedur pengoperasian dan pemulihan (*recovery*) jika diperlukan.
      (5) Nama-nama dan nomor kontak petugas pendukung teknis;

(6) Manual konfigurasi; dan
(7) Formulir yang disebutkan dalam Pedoman Implementasi CICD Container atau Pedoman Implementasi CICD Non Container.

e) Dokumentasi tahap pengujian, yang meliputi:
(1) Dokumentasi pengujian integrasi yang terdiri atas *test plan, test scenario*, *test case*, hasil uji, dan tindak lanjutnya.
(2) Dokumentasi sistem testing terdiri atas *test plan, test scenario*, *test case*, tes fungsional, tes beban, tes regresi, tes keamanan, hasill uji, dan tindak lanjutnya.
(3) Dokumentasi *User Acceptance Testing* terdiri atas *test plan, test scenario*, *test case*, tes fungsional, hasill uji, dan tindak lanjutnya.

f) Dokumentasi pemeliharaan, yang meliputi:
(1) Pemeliharaan perfektif.
(2) Pemeliharaan adaptif.
(3) Pemeliharaan korektif; dan/atau
(4) Pemeliharaan preventif.

g) Dokumentasi evaluasi pasca implementasi (*post implementation review*).

d. Prosedur Pembangunan dan pengembangan Aplikasi SPBE
Pembangunan dan pengembangan Aplikasi SPBE harus sesuai dengan prosedur pembangunan dan pengembangan Aplikasi SPBE, yang meliputi tahapan:

1) Persiapan, yang mengacu pada tahap perencanaan sebagaimana diuraikan di atas.
2) Permohonan pertimbangan
a) Permohonan pertimbangan terdiri atas:
(1) Pertimbangan pembangunan dan pengembangan Aplikasi SPBE.
(2) Pertimbangan penggunaan aplikasi sejenis; dan
(3) Pertimbangan penggunaan kode sumber tertutup.

b) Permohonan pertimbangan pembangunan dan pengembangan Aplikasi Umum SPBE diajukan kepada menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi. c.q. Direktur Jenderal yang lingkup tugas dan tanggung jawabnya di bidang teknologi pemerintah digital dilakukan sebelum pembangunan dan pengembangan Aplikasi SPBE dilaksanakan serta dikoordinasikan melalui Pusdatin.

c) Dalam hal pembangunan dan pengembangan Aplikasi SPBE menggunakan kode sumber tertutup, permohonan pertimbangan melampirkan:
(1) Urgensi penggunaan kode sumber tertutup.
(2) Kajian biaya dan manfaat terhadap penggunaan kode sumber tertutup.

3) Pelaksanaan

a) Pelaksanaan pembangunan dan pengembangan Aplikasi SPBE terdiri atas:
   (1) Skema pembangunan dan pengembangan Aplikasi SPBE melalui Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi, Swakelola Kementerian, atau Pihak Ketiga.
   (2) Pelaksanaan manajemen proyek teknologi informasi.
   (3) Pelaksanaan alih teknologi melalui sosialisasi, bimbingan teknis, pelatihan, konsultasi, fasilitasi, dan pendampingan. yang meliputi:
      (a) Alih pengetahuan dan keterampilan untuk pengoperasian, pemeliharaan, dan pembaruan Aplikasi SPBE.
      (b) Alih penguasaan teknologi dasar untuk mendesain Aplikasi SPBE secara mandiri.
      (c) Alih penguasaan teknologi menyeluruh untuk pengembangan Aplikasi SPBE secara mandiri.
   (4) konsultasi dan/atau koordinasi
      (a) Konsultasi dan/atau koordinasi terkait keterpaduan pembangunan dan pengembangan Aplikasi SPBE dilaksanakan dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi.
      (b) Konsultasi dan/atau koordinasi terkait keamanan pembangunan dan pengembangan Aplikasi SPBE dilaksanakan dengan kepala lembaga yang menyelenggarakan urusan pemerintahan di bidang keamanan siber.

b) Pembangunan dan pengembangan Aplikasi SPBE dilaksanakan dengan prinsip-prinsip manajemen proyek teknologi informasi, yang bertujuan untuk:
   (1) Menyelesaikan pekerjaan tepat waktu.
   (2) Mengelola risiko yang mungkin timbul.
   (3) Mengelola tim pelaksanaan pekerjaan.
   (4) Membuat perencanaan yang tepat; dan
   (5) Menjaga penggunaan anggaran yang efisien.

c) Manajemen proyek teknologi informasi sebagaimana dimaksud dilakukan dengan meliputi tahapan sebagai berikut:
   (1) Inisiasi.
   (2) Perencanaan.
   (3) Pelaksanaan proyek.
   (4) Pemantauan dan evaluasi; dan
   (5) Penutupan proyek.

4) Pendaftaran dan penyimpanan
   a) Pendaftaran Aplikasi SPBE dan penyimpanan Kode Sumber Aplikasi SPBE dilaksanakan melalui tahapan:

(1) Pendaftaran pejabat pendaftar Aplikasi SPBE; dan
(2) Mengisi formulir pendaftaran atas Aplikasi SPBE yang dikelola Kementerian.

b) Pejabat pendaftar Aplikasi SPBE harus didaftarkan ke Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informasi, untuk pejabat pendaftar aplikasi baru atau pejabat pendaftar aplikasi pengganti.

c) Pejabat pendaftar Aplikasi SPBE merupakan aparatur sipil negara yang menduduki jabatan setingkat pejabat pimpinan tinggi pratama di bidang pengelolaan teknologi informasi dan komunikasi, atau sekurang-kurangnya jabatan fungsional ahli madya yang memiliki kompetensi di bidang teknologi informasi dan komunikasi di Pusdatin.

d) Formulir pendaftaran pejabat pendaftar Aplikasi SPBE dan formulir pendaftaran atas Aplikasi SPBE yang dikelola Kementerian mengacu pada peraturan perundang-undangan.

e) Pejabat Pendaftar Aplikasi SPBE menyimpan dokumentasi Aplikasi SPBE yang meliputi:
(1) Kode sumber Aplikasi SPBE
(a) Kode Sumber Aplikasi SPBE yang sudah menerapkan layanan mikro *(microservices)* disimpan dalam bentuk per komponen aplikasi.
(b) Kode Sumber Aplikasi SPBE yang belum menerapkan layanan mikro *(microservices)* disimpan dalam bentuk kompresi.
(2) Skema basis data, yang merupakan bahasa pemrograman yang dapat dimanfaatkan untuk membuat dan mendefinisikan struktur dari suatu objek dalam basis data.
(3) Dokumentasi siklus pembangunan dan pengembangan Aplikasi SPBE, yang terdiri dari:
(a) Dokumentasi perencanaan.
(b) Dokumentasi analisis kebutuhan (SRS).
(c) Dokumentasi perancangan (SDD).
(d) Dokumentasi implementasi.
(e) Dokumentasi pengujian.
(f) Dokumentasi pemeliharaan; dan
(g) Dokumentasi evaluasi pasca implementasi.

5) Penetapan dan hak cipta
a) Penetapan Aplikasi Khusus ditetapkan dalam bentuk Keputusan Menteri.
b) Hak cipta atas setiap Aplikasi SPBE yang dibangun menjadi milik Kementerian.

e. Pengelolaan Penjaminan Kualitas (*Quality Assurance*)
1) Untuk setiap kegiatan pembangunan dan pengembangan Aplikasi

SPBE harus ada fungsi *Quality Assurance*.

2) Pelaksana *Quality Assurance* adalah pihak yang memiliki kapabilitas untuk memeriksa pekerjaan pihak lain dalam kegiatan pembangunan dan pengembangan Aplikasi SPBE, untuk menjaga objektivitas.
3) *Quality Assurance* secara objektif mengevaluasi pelaksanaan seluruh proses yang telah ditentukan dalam suatu pembangunan dan pengembangan Aplikasi SPBE yang meliputi pelaksanaan prosedur dan penggunaan standar.
4) *Quality Assurance* secara objektif mengevaluasi proses dan produk yang dihasilkan dalam setiap tahap pada pembangunan dan pengembangan Aplikasi SPBE, baik yang berupa dokumen maupun Aplikasi SPBE.
5) *Quality Assurance* mengkomunikasikan permasalahan kualitas kepada pihak-pihak terkait dan memastikan permasalahan ketidakpatuhan proses (*non-compliance*) dan ketidaksesuaian produk (*non-conformance*) dapat diselesaikan.
6) Kegiatan *Quality Assurance* harus dicatat dan catatan tersebut dikelola dengan baik.

f. Pengelolaan Perubahan

1) Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor atau tim teknis mengajukan permintaan perubahan melalui formulir permintaan perubahan kepada tim pembangunan dan pengembangan Aplikasi SPBE.
2) Untuk setiap perubahan yang diajukan Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor atau tim teknis harus diketahui dan disetujui oleh Pimpinan Unit Kerja di masing-masing Unit Kerja.
3) Tim pembangunan dan pengembangan Aplikasi SPBE melakukan analisis dampak dari permintaan perubahan yang diajukan terutama terkait dengan jadwal, SDM, pergeseran prioritas pengerjaan modul-modul aplikasi.
4) Secara bertingkat, tim pembangunan dan pengembangan Aplikasi SPBE memeriksa dan menyetujui permintaan perubahan, serta menyampaikan hasilnya kepada Pemilik Proses Bisnis/Pengguna/Unit Kerja/Unor atau tim teknis.
5) Dalam hal permintaan perubahan disetujui, maka tim pembangunan dan pengembangan Aplikasi SPBE akan:

a) Menindaklanjuti permintaan perubahan tersebut sesuai dengan sumber daya yang ditetapkan.
b) Melakukan pembaruan terhadap konfigurasi aplikasi; dan
c) Melakukan perekaman dalam repositori Kementerian untuk setiap perubahan yang dilakukan termasuk pembaruan konfigurasi aplikasi.

6) Tim pembangunan dan pengembangan Aplikasi SPBE melalui penanggungjawab pembangunan dan pengembangan aplikasi dapat melakukan konsultasi dan/atau eskalasi kepada Kepala Unit

Datin/Kepala Pusdatin terkait hasil analisis dampak permintaan perubahan.

g. Pengelolaan Situs Web
   1) Situs Web Kementerian merupakan bagian dari Aplikasi SPBE.
   2) Situs Web Kementerian terdiri atas:
      a) Situs web utama; dan
      b) Situs web Unit Organisasi.
   3) Situs web utama merupakan situs resmi Kementerian dan menggunakan domain Kementerian.
   4) Sistem situs web utama dibangun, dikembangkan, dan dipelihara oleh Pusdatin.
   5) Pembangunan dan/atau pengembangan situs web Unit Organisasi dikoordinasikan oleh Pusdatin.
   6) Situs web Unit Organisasi yang dibangun dan/atau dikembangkan oleh masing-masing Unit Organisasi, harus mendapat persetujuan dari Pusdatin.
   7) Situs web Unit Organisasi merupakan subdomain dari domain Kementerian.
   8) *Platform* Situs Web
      a) Dalam pembangunan dan pengembangan Situs web, dapat menggunakan platform berlisensi terbuka (*open source*) dan/atau berlisensi berbayar (*licensed*) untuk sistem operasi, basis data, bahasa pemrograman, dan *web server.*
      b) Dalam pemilihan *platform*, harus memperhatikan kemudahan memperoleh dukungan layanan purnajual dan mengembangkan situs web tersebut.
      c) Situs web yang dikembangkan harus dapat diakses pada semua perangkat (*gadget*) dan peramban (*browser*) yang umum digunakan oleh masyarakat.
      d) Penempatan (*hosting*) situs web Kementerian disediakan oleh Pusdatin.
      e) Penempatan (*hosting*) situs web Unit Organisasi dikoordinasikan dengan Pusdatin melalui Unit Datin.
      f) Pengujian keamanan terhadap situs web yang dikembangkan oleh Unit Organisasi dilaksanakan oleh Unit Datin dan melaporkan hasil pengujian keamanan kepada Pusdatin.
   9) Penataan Konten
      Konten yang wajib tersedia di situs web Kementerian dan Unit Organisasi mengacu pada ketentuan yang ditetapkan oleh Unit Kerja di sekretariat jenderal yang memiliki tugas melaksanakan penyelenggaraan dan pembinaan komunikasi publik Kementerian.
   10) Tata Kelola Situs Web
      a) Situs web di lingkungan Kementerian terdiri atas situs Kementerian, Unit Organisasi, BPJT dan LPJK.
      b) Situs web UPT merupakan portal layanan yang diintegrasikan dengan Portal Layanan publik Kementerian (sahabat.pu.go.id) dan diakses melalui situs Unit Organisasi.

c) Penyelenggara Situs Web

Penyelenggara situs web terdiri atas:

(1) Pusdatin, berperan sebagai:
   (a) Penanggung jawab Infrastruktur SPBE pendukung situs web Kementerian dan Unit Organisasi.
   (b) Penanggung jawab sistem situs web Kementerian.
   (c) Penanggung jawab sistem situs web Sekretariat Jenderal.
   (d) Pengelola tayangan yang terdiri atas:
      i. Pengumuman.
      ii. Agenda kegiatan Kementerian; dan
      iii. Tayangan informasi Kementerian di luar berita dan publikasi.

(2) Unit Kerja di Sekretariat Jenderal yang bertanggung jawab terhadap Komunikasi Publik, berperan sebagai:
   (a) Penanggung jawab konten situs web Kementerian yang terdiri atas:
      i. Berita utama Kementerian.
      ii. Galeri foto dan video Kementerian.
      iii. Saran dan Pengaduan.
      iv. Layanan Informasi Publik; dan
      v. Pelayanan Publik.
   (b) Penanggung jawab konten situs web Sekretariat Jenderal yang terdiri atas:
      i. Berita Sekretariat Jenderal Kementerian; dan
      ii. Galeri foto dan video Sekretariat Jenderal Kementerian.
   (c) Kontributor konten lainnya.

(3) Unit Organisasi
   (a) Penanggung jawab Infrastruktur SPBE pendukung situs web, dalam hal tidak menggunakan fasilitas yang disediakan oleh Pusdatin.
   (b) Penanggung jawab sistem situs web Unit Organisasi.
   (c) Penanggung jawab konten situs web Unit Organisasi; dan
   (d) Kontributor konten situs web Kementerian.

(4) Unit Kerja/UPT
   (a) Kontributor konten situs web Unit Organisasi.
   (b) Matriks tugas dan tanggung jawab pemeliharaan situs web Kementerian dan Unit Organisasi adalah sebagai berikut:

Tabel 40 Matriks Tugas dan Tanggung Jawab Pemeliharaan Situs Web

| | | Tugas | Pelaksana |
|---|---|---|---|
| *Top Level Management* and *Policy maker* / Pembuat kebijakan | | | |
| 1. | Pengelola *web* utama (*Webmaster*) | Menentukan kebijakan, mengelola dan menjaga situs web | Pusdatin |
| 2. | Administrator *web* (*Web Administrator*) | Proses manajemen | Pusdatin<br>Unit Datin |
| 3 | Administrator Konten (*Content Administrator*) | Penentuan kebijakan konten | Unit Kerja di Sekretariat Jenderal yang bertanggung jawab terhadap komunikasi publik |
| *Content Management* / Pengelola konten *web* | | | |
| 4. | Penulis (*Author*) | Membangun konten situs web | Unit Kerja yang bertanggung jawab terhadap komunikasi publik |
| 5. | Penyunting (*Editor*) | Merawat konten situs web | Unit Kerja yang bertanggung jawab terhadap komunikasi publik |
| *Web Development* / Pengembang *website* | | | |
| 6 | Pengembang *web* (*Web Developer*) | Membangun, mengembangkan, dan memperbaiki situs web: | Penanggungjawab : |
| | | Kementerian | Pusdatin |
| | | Unit Organisasi | Unit Datin |
| a. | Desain Komunikasi Visual *web* (*Visual Narrative Design*) | Desain situs web, membuat grafis, gambar, tipografi, animasi, dan multimedia | Penanggungjawab : |
| | | Kementerian | Pusdatin |
| | | Unit Organisasi | Unit Datin |
| b. | Pemogram *web* (*Web Programmer*) | Membuat aplikasi | Pusdatin dan Unit Datin |
| c. | Administrator Basis Data (*Database Administrator*) | Merancang basis data (*database*) aplikasi | Pusdatin dan Unit Datin |

(5) Pengelola *web* utama (*webmaster*)

Pengelola *web* utama (*webmaster*) bertanggung jawab sebagai berikut:

(a) Merencanakan, mengembangkan, mengelola, dan mengevaluasi situs web secara berkelanjutan.

(b) Menyusun prosedur operasional standar pengelolaan situs web.
(c) Menetapkan persyaratan teknis situs web.
(d) Menentukan situs terkait; dan
(e) Memberikan pelayanan dan perawatan yang berkaitan dengan situs web.

(6) Administrator web (*web administrator*)
Administrator *web* (*web administrator*) bertanggung jawab sebagai berikut:
(a) Membantu webmaster dalam merencanakan, mengembangkan, mengelola, dan mengevaluasi situs web secara berkelanjutan serta menyusun prosedur operasional standar.
(b) Mengelola hak akses pengguna ke situs web.
(c) Melakukan koordinasi dengan Unit Organisasi dan Unit Kerja terkait dalam pengelolaan situs web.
(d) Melakukan cadangan (*back up*) sistem dan data.

(7) Administrator konten (*content administrator*) bertanggung jawab sebagai berikut:
(a) Membuat, menyiapkan, dan mengelola konten baru untuk setiap Unit Organisasi dan Unit Kerja.
(b) Menyusun prosedur operasional standar penyusunan konten situs web.

(8) Penulis (*author*)
Penulis (a*uthor*) bertanggung jawab menyusun konten situs web.

(9) Penyunting (*editor*)
Penyunting (*editor*) bertanggung jawab atas kelayakan konten situs web.

(10) Pengembang *web* (*web developer*)
Pengembang *web* (*web developer*) bertanggung jawab sebagai berikut:
(a) Merencanakan dan membangun dalam pengembangan situs web.
(b) Membuat petunjuk teknis penggunaan situs web.
(c) Pengembang *web* (*web developer*) terdiri atas:
i. Desain Komunikasi Visual web (*Visual Narrative Design*).
Desain Komunikasi Visual web (*Visual Narrative Design*) bertanggung jawab sebagai berikut:
i) Membuat rancangan dan menentukan struktur bagian-bagian situs web yang akan dibuat.
ii) Menentukan skema/hierarki tautan (*link*) yang akan dibuat, dan layanan yang akan diberikan ke publik serta menentukan pola situs web; dan

iii) Menciptakan hasil visualisasi dari suatu ide ke dalam bentuk grafis, gambar, tipografi, animasi, dan multimedia.

ii. Pemrogram *web* (*web* programmer)

Pemrogram *web (web programmer*) bertanggung jawab sebagai berikut:

i) Membuat dan melakukan pengaturan (setup) layanan interaktif dalam lingkungan situs web; dan

ii) Menjalankan program-program yang ada dalam situs web.

iii) Administrator basis data (*database administrator*);

Administrator basis data (*database administrator*) bertanggung jawab merancang dan mengelola sistembasis data (*database*).

h. Pengelolaan Nama Domain

1) Pengelolaan nama domain dan subdomain di Kementerian dilaksanakan oleh Pusdatin.
2) Nama domain digunakan pada situs web utama dengan nama pu.go.id.
3) Unit Kerja di Kementerian yang akan menggunakan subdomain, harus mendapat persetujuan dari Pusdatin.
4) Standar Nama Domain dan Subdomain
   a) Pengelolaan Penamaan Domain
      (1) Pengelolaan Penamaan Domain meliputi:
         (a) Pendaftaran.
         (b) Penggunaan.
         (c) Penonaktifan.
         (d) Perpanjangan.
         (e) Penunjukan pejabat.
         (f) Perubahan nama domain; dan
         (g) *Server* nama domain.
      (2) Setiap aplikasi yang menggunakan nama domain/sub domain Kementerian harus mengikuti ketentuan pembangunan dan pengembangan aplikasi Kementerian.
      (3) Nama domain yang dimaksud di atas dibiayai oleh anggaran Kementerian.
   b) Pengelolaan Penamaan Subdomain;
      (1) Unit Datin bertanggung jawab dalam memantau dan mengawasi penggunaan subdomain di Unit Organisasinya.
      (2) Unit Datin bertanggung jawab dalam hal pengajuan, penambahan, perubahan, dan penghapusan subdomain di Unit Organisasinya.

(3) Domain dan subdomain yang sudah dibuat menjadi milik Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari Pusdatin.

(4) Setiap pengajuan nama subdomain oleh Unit Datin harus disampaikan kepada Pusdatin disertai dengan data penanggung jawab situs web atau aplikasi berbasis web dan menyerahkan seluruh Dokumen atas Aplikasi SPBE.

(5) Yang berhak mendapatkan nama subdomain:
   (a) Situs web Unit Organisasi.
   (b) Kegiatan Kementerian.
   (c) Aplikasi Layanan Publik.
   (d) Aplikasi Tingkat Kementerian.
   (e) Aplikasi Teknis; dan
   (f) Aplikasi Pendukung.

(6) Permohonan mendapatkan nama subdomain.
   Untuk mendapatkan nama subdomain, Unit Organisasi/Unit Kerja harus mengajukan permohonan melalui portal layanan internal kepada Pusdatin dengan mencantumkan:
   (a) Nama subdomain yang diusulkan dan alamat IP (*IP Address*).
   (b) Peruntukan penggunaan nama subdomain yang diusulkan; dan
   (c) Pejabat Penanggung jawab nama subdomain yang diusulkan.

(7) Nama subdomain yang diajukan harus terdiri dari karakter yang dapat berupa nama, singkatan nama atau akronim dari nama resmi instansi, nomenklatur pelayanan publik, nama kegiatan Kementerian, dan aplikasi berbasis *web*.
   (a) Penataan subdomain untuk situs *web* Unit Organisasi:
   *nama Unit Organisasi*.pu.go.id
   (b) Penataan subdomain untuk kegiatan Kementerian:
      i. Kegiatan skala nasional/internasional:
      *kegiatan*.pu.go.id
      ii. Kegiatan internal Kementerian tingkat Unit Organisasi:
      *nama Unit Organisasi*.pu.go.id/*kegiatan*
   (c) Penataan subdomain untuk aplikasi berbasis *web*:
      i. Digunakan oleh publik:
      *aplikasi*.pu.go.id
      ii. Digunakan di lingkungan Kementerian:
      *aplikasi*.pu.go.id
      iii. Digunakan di lingkungan Unit Organisasi:
      *aplikasi.nama Unit Organisasi*.pu.go.id
   (d) Nama subdomain Unit Organisasi di Kementerian:

i. Sekretariat Jenderal:
*setjen.pu.go.id*
ii. Inspektorat Jenderal:
*itjen.pu.go.id*
iii. Ditjen Sumber Daya Air:
*sda.pu.go.id*
iv. Ditjen Bina Marga:
*binamarga.pu.go.id*
v. Ditjen Cipta Karya:
*ciptakarya.pu.go.id*
vi. Ditjen Prasarana Strategis:
*djps.pu.go.id*
vii. Ditjen Bina Konstruksi:
*binakonstruksi.pu.go.id*
viii. Ditjen Pembiayaan Infrastruktur Pekerjaan Umum:
*pembiayaan.pu.go.id*
ix. Badan Pengembangan Infrastruktur Wilayah:
*bpiw.pu.go.id*
x. Badan Pengembangan Sumber Daya Manusia:
*bpsdm.pu.go.id*
xi. Badan Pengatur Jalan Tol:
*bpjt.pu.go.id*
xii. Lembaga Pengembangan Jasa Konstruksi:
*Lpjk.pu.go.id*

5) Aplikasi yang tidak relevan dengan substansi aplikasi tidak diperkenankan menggunakan subdirektori dari domain aplikasi tersebut.
6) Jika terdapat perubahan nomenklatur dan/atau struktur organisasi, Unit Organisasi dapat mengajukan perubahan dan/atau penambahan nama subdomain dengan mengajukan permohonan kepada Pusdatin melalui Unit Datin.
7) Pusdatin menyediakan sertifikat *Transport Layer Security* (TLS) bagi pengguna subdomain Kementerian (xx.pu.go.id) kecuali untuk aplikasi berbasis *web* yang digunakan di lingkungan Unit Organisasi.

i. Pengelolaan Surat Elektronik
1) Surat elektronik dikelola oleh Pusdatin.
2) Akun surat elektronik resmi Kementerian menggunakan alamat nama_akun@pu.go.id.
3) Akun surat elektronik resmi Kementerian digunakan untuk urusan kedinasan oleh Pegawai yang bekerja di Kementerian.
4) Pengelolaan Surat Elektronik
a) Setiap Unit Organisasi/Unit Kerja/UPT bertanggung jawab dalam memantau dan mengevaluasi penggunaan surat

elektronik resmi Kementerian di lingkungan unitnya berkoordinasi dengan Pusdatin.

b) Setiap Unit Organisasi/Unit Kerja/UPT bertanggung jawab dan mengetahui serta melaporkan kegiatan terkait perubahan akun surat elektronik resmi Kementerian di lingkungan unitnya kepada Pusdatin, dalam hal ini meliputi penambahan, perubahan, dan penghapusan akun surat elektronik resmi Kementerian.

c) Setiap pengajuan nama akun surat elektronik resmi Kementerian harus disampaikan kepada Pusdatin disertai dengan data penanggung jawab akun surat elektronik resmi Kementerian.

d) Untuk pengguna akun organisasi dan jabatan yang dipindahtugaskan keluar Kementerian atau pensiun atau meninggal, unit pengelola kepegawaian pada masing-masing Unit Kerja/UPT harus menyerahkan akun surat elektronik resmi Kementerian kepada Pusdatin ditembuskan kepada Unit Kerja di Sekretariat Jenderal yang melakukan pengelolaan kepegawaian.

5) Format penamaan akun surat elektronik resmi Kementerian dikoordinasikan dengan Pusdatin.

6) Tata Cara Mendapatkan Akun Surat Elektronik Resmi Kementerian:

a) Yang berhak mendapatkan akun surat elektronik resmi Kementerian:
   (1) Unit Organisasi/Unit Kerja/UPT di Kementerian.
   (2) Aparatur Sipil Negara (ASN).
   (3) Kegiatan/Aplikasi di Unit Kerja; dan
   (4) Pegawai lainnya di Kementerian.

b) Pengajuan untuk mendapatkan akun surat elektronik resmi Kementerian.

   Untuk mendapatkan nama akun surat elektronik resmi Kementerian, Unit Organisasi/Unit Kerja/UPT harus mengajukan permohonan kepada Pusdatin dengan mencantumkan:
   (1) Nama akun yang diusulkan; dan
   (2) NIP/NRP/NIK pengguna atau penanggung jawab akun surat elektronik resmi Kementerian yang diusulkan.

c) Nama akun surat elektronik resmi Kementerian yang diajukan harus terdiri dari karakter yang dapat berupa nama, singkatan nama atau akronim.

d) Dalam pengajuan akun surat elektronik resmi Kementerian, sekurang-kurangnya mencantumkan nama pegawai, nama Unit Organisasi/Unit Kerja/UPT, NIP/NRP/NIK, jabatan, dan nama akun surat elektronik yang diinginkan.

e) Pusdatin menentukan persetujuan akun surat elektronik resmi Kementerian yang diajukan dengan mempertimbangkan sumber daya yang tersedia.

7) Akun surat elektronik resmi Kementerian yang dimaksud di atas dibiayai oleh anggaran Kementerian.
8) Tata cara pemanfaatan akun surat elektronik resmi Kementerian, pergantian *password*, dan tata cara lainnya yang lebih detil dan teknis akan di tuangkan dalam aturan pelaksanaan sebagai turunan dari Peraturan Menteri ini.

MENTERI PEKERJAAN UMUM
REPUBLIK INDONESIA,

ttd.

DODY HANGGODO