



BERITA NEGARA REPUBLIK INDONESIA

No.1177, 2021

KEMENPAN-RB. Jafung Sandiman. Standar Kompetensi.

PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN
REFORMASI BIROKRASI REPUBLIK INDONESIA

NOMOR 44 TAHUN 2021

TENTANG

STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN
REFORMASI BIROKRASI REPUBLIK INDONESIA,

- Menimbang : a. bahwa untuk menyelenggarakan manajemen karier berbasis sistem merit dan meningkatkan profesionalitas Jabatan Fungsional Sandiman, serta mengembangkan kompetensi dan kinerja dalam pelaksanaan tugas Jabatan Fungsional Sandiman, perlu disusun standar kompetensi Jabatan Fungsional Sandiman;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan untuk melaksanakan ketentuan Pasal 2 ayat (2) Peraturan Menteri Pendayagunaan Aparatur Sipil Negara Nomor 38 Tahun 2017 tentang Standar Kompetensi Jabatan Aparatur Sipil Negara, perlu menetapkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tentang Standar Kompetensi Jabatan Fungsional Sandiman;

- 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);
3. Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);
4. Peraturan Pemerintah Nomor 11 Tahun 2017 tentang Manajemen Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 63, Tambahan Lembaran Negara Republik Indonesia Nomor 6037) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 17 Tahun 2020 tentang Perubahan atas Peraturan Pemerintah Nomor 11 Tahun 2017 tentang Manajemen Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 68, Tambahan Lembaran Negara Republik Indonesia Nomor 6477);
5. Keputusan Presiden Nomor 87 Tahun 1999 tentang Rumpun Jabatan Fungsional Pegawai Negeri Sipil, sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 116 Tahun 2014 tentang Perubahan Kedua atas Keputusan Presiden Nomor 87 Tahun 1999 tentang Rumpun Jabatan Fungsional Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 240);
6. Peraturan Presiden Nomor 47 Tahun 2021 tentang Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 126);
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 38 Tahun 2017 tentang Standar Kompetensi Jabatan Aparatur Sipil Negara (Berita Negara Republik Indonesia Tahun 2017 Nomor

- 1907);
8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 18 Tahun 2019 tentang Jabatan Fungsional Sandiman (Berita Negara Republik Indonesia Tahun 2019 Nomor 1010);
 9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 25 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Berita Negara Republik Indonesia Tahun 2019 Nomor 1593);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI TENTANG STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah profesi bagi Pegawai Negeri Sipil dan Pegawai Pemerintah dengan Perjanjian Kerja yang bekerja pada instansi pemerintah.
2. Pegawai Negeri Sipil yang selanjutnya disingkat PNS adalah warga negara Indonesia yang memenuhi syarat tertentu diangkat sebagai Pegawai ASN secara tetap oleh Pejabat Pembina Kepegawaian untuk menduduki jabatan pemerintahan.
3. Jabatan Fungsional Sandiman adalah jabatan yang mempunyai ruang lingkup, tugas, tanggung jawab dan wewenang untuk melakukan pengamanan informasi, pengamanan siber, dan persandian.
4. Pejabat Fungsional Sandiman yang selanjutnya disebut Sandiman adalah ASN yang diberi tugas, tanggung jawab dan wewenang untuk melaksanakan pekerjaan

Jabatan Fungsional Sandiman.

5. Kompetensi Teknis adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur dan dikembangkan yang spesifik berkaitan dengan bidang teknis jabatan.
6. Kompetensi Manajerial adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dikembangkan untuk memimpin dan/atau mengelola unit organisasi.
7. Kompetensi Sosial Kultural adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dan dikembangkan terkait dengan pengalaman berinteraksi dengan masyarakat majemuk dalam hal agama, suku dan budaya, perilaku, wawasan kebangsaan, etika, nilai-nilai, moral, emosi dan prinsip, yang harus dipenuhi oleh setiap pemegang Jabatan untuk memperoleh hasil kerja sesuai dengan peran, fungsi dan jabatan.
8. Standar Kompetensi Jabatan Fungsional Sandiman yang selanjutnya disebut Standar Kompetensi adalah deskripsi pengetahuan, keterampilan, dan perilaku yang diperlukan seorang Sandiman dalam melaksanakan tugas jabatan.

BAB II

KEDUDUKAN, JENJANG, DAN KOMPETENSI

Pasal 2

- (1) Sandiman berkedudukan sebagai pelaksana teknis di bidang keamanan informasi, keamanan siber, dan persandian.
- (2) Sandiman sebagaimana dimaksud pada ayat (1) merupakan jabatan karier PNS.
- (3) Sandiman sebagaimana dimaksud pada ayat (2) berkedudukan di bawah dan bertanggung jawab secara langsung kepada Pejabat Pimpinan Tinggi Pratama, Pejabat Administrator, atau Pejabat Pengawas yang

memiliki keterkaitan dengan pelaksanaan tugas Jabatan Fungsional Sandiman, serta ditetapkan dalam peta jabatan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 3

- (1) Jabatan Fungsional Sandiman merupakan jabatan fungsional kategori keterampilan dan kategori keahlian.
- (2) Jenjang Jabatan Fungsional Sandiman kategori keterampilan sebagaimana dimaksud pada ayat (1), dari jenjang terendah sampai jenjang tertinggi, terdiri atas:
 - a. Sandiman terampil;
 - b. Sandiman mahir; dan
 - c. Sandiman penyelia.
- (3) Jenjang Jabatan Fungsional Sandiman kategori keahlian sebagaimana dimaksud pada ayat (1), dari jenjang terendah sampai jenjang tertinggi, terdiri atas:
 - a. Sandiman ahli pertama;
 - b. Sandiman ahli muda;
 - c. Sandiman ahli madya; dan
 - d. Sandiman ahli utama.

Pasal 4

- (1) Sandiman dalam menjalankan tugas jabatan harus memenuhi Standar Kompetensi.
- (2) Standar Kompetensi sebagaimana dimaksud pada ayat (1) meliputi:
 - a. identitas jabatan;
 - b. kompetensi jabatan; dan
 - c. persyaratan jabatan.
- (3) Standar Kompetensi sebagaimana dimaksud pada ayat (2) menjadi acuan paling sedikit untuk:
 - a. perencanaan Sandiman;
 - b. pengadaan Sandiman;
 - c. pengembangan karier Sandiman;
 - d. pengembangan Sandiman;
 - e. penempatan Sandiman;

- f. promosi dan/atau mutasi Sandiman;
- g. uji kompetensi Sandiman;
- h. sistem informasi manajemen Sandiman; dan
- i. kelompok rencana suksesi (*talent pool*) Sandiman.

Pasal 5

- (1) Identitas jabatan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a, paling sedikit terdiri atas:
 - a. nama jabatan;
 - b. uraian/ikhtisar jabatan; dan
 - c. kode jabatan.
- (2) Kompetensi jabatan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b, terdiri atas:
 - a. Kompetensi Teknis;
 - b. Kompetensi Manajerial; dan
 - c. Kompetensi Sosial Kultural.
- (3) Persyaratan jabatan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf c, paling sedikit terdiri atas:
 - a. pangkat;
 - b. kualifikasi pendidikan;
 - c. jenis pelatihan;
 - d. ukuran kinerja jabatan; dan
 - e. pengalaman kerja.

Pasal 6

- (1) Kompetensi Teknis Jabatan Fungsional Sandiman sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a terdiri atas:
 - a. Kompetensi Teknis bersifat umum; dan
 - b. Kompetensi Teknis bersifat khusus.
- (2) Kompetensi Teknis Jabatan Fungsional Sandiman bersifat umum sebagaimana dimaksud pada ayat (1) huruf a meliputi:
 - a. manajemen keamanan siber dan persandian; dan
 - b. advokasi kebijakan keamanan siber.
- (3) Kompetensi Teknis Jabatan Fungsional Sandiman bersifat khusus sebagaimana dimaksud pada ayat (1)

huruf b meliputi:

- a. manajemen risiko keamanan siber;
 - b. penilaian keamanan teknologi informasi;
 - c. intelijen siber;
 - d. *monitoring* keamanan jaringan;
 - e. audit keamanan informasi;
 - f. penyediaan layanan keamanan informasi;
 - g. pengelolaan Computer Security Incident Response Team (CSIRT);
 - h. manajemen insiden siber;
 - i. manajemen krisis siber;
 - j. forensik digital;
 - k. investigasi siber;
 - l. *data science* keamanan siber dan sandi negara;
 - m. analisis kriptografi;
 - n. rekayasa kriptografi;
 - o. rancang bangun perangkat keamanan teknologi informasi;
 - p. pengkajian teknologi keamanan siber dan sandi;
 - q. pengelolaan penelitian teknologi keamanan siber dan sandi negara;
 - r. pengelolaan *security operation center* (SOC);
 - s. pengelolaan pusat kontak siber nasional;
 - t. analisis kelaikan sertifikat elektronik;
 - u. pemenuhan teknis sistem sertifikasi elektronik;
 - v. pengelolaan jaringan dan infrastruktur sertifikasi elektronik;
 - w. verifikasi algoritma kriptografi;
 - x. *functional testing*;
 - y. analisis kerawanan produk keamanan siber dan sandi negara; dan
 - z. pengelolaan pengujian produk keamanan siber dan sandi negara.
- (4) Kompetensi Manajerial sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b terdiri atas:
- a. integritas;
 - b. kerja sama;

- c. komunikasi;
 - d. orientasi pada hasil;
 - e. pelayanan publik;
 - f. pengembangan diri dan orang lain;
 - g. mengelola perubahan; dan
 - h. pengambilan keputusan.
- (5) Kompetensi Sosial Kultural sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c yaitu perekat bangsa.

Pasal 7

Standar Kompetensi sebagaimana dimaksud dalam Pasal 4 ayat (1) dilaksanakan berdasarkan:

- a. kamus kompetensi teknis;
- b. kamus kompetensi manajerial; dan
- c. kamus kompetensi sosial kultural.

Pasal 8

Standar Kompetensi Jabatan Fungsional Sandiman sebagaimana dimaksud dalam Pasal 4 dan Pasal 7 tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 9

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 12 Oktober 2021

MENTERI PENDAYAGUNAAN APARATUR
NEGARA DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA,

ttd.

TJAHJO KUMOLO

Diundangkan di Jakarta
pada tanggal 21 Oktober 2021

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd.

BENNY RIYANTO

LAMPIRAN
 PERATURAN MENTERI PENDAYAGUNAAN
 APARATUR NEGARA DAN REFORMASI
 BIROKRASI REPUBLIK INDONESIA
 NOMOR 44 TAHUN 2021
 TENTANG
 STANDAR KOMPETENSI JABATAN
 FUNGSIONAL SANDIMAN

STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN

A. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN KATEGORI
 KETERAMPILAN

1. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN
 TERAMPIL/ PELAKSANA

a. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Terampil |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN TERAMPIL | | | |
|--------------------------------------|--|-----------------|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi kendali operasi keamanan siber dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan SOC, pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 1 | Mampu bertindak | 1.1. Bertingkah laku sesuai dengan perkataan; |

| | | | |
|---------------|---|---|---|
| | | sesuai nilai, norma, dan etika organisasi, dalam kapasitas pribadi. | berkata sesuai dengan fakta; 1.2. Melaksanakan peraturan, kode etik organisasi dalam lingkungan kerja sehari-hari, pada tataran individu/pribadi; 1.3. Tidak menjanjikan/memberikan sesuatu yang bertentangan dengan aturan organisasi. |
| 2. Kerjasama | 1 | Berpartisipasi dalam kelompok kerja. | 1.1. Berpartisipasi sebagai anggota tim yang baik, melakukan tugas/bagiannya, dan mendukung keputusan tim; 1.2. Mendengarkan dan menghargai masukan dari orang lain dan memberikan usulan-usulan bagi kepentingan tim; 1.3. Mampu menjalin interaksi sosial untuk penyelesaian tugas. |
| 3. Komunikasi | 1 | Menyampaikan informasi dengan jelas, lengkap, pemahaman yang sama. | 1.1. Menyampaikan informasi (data), pikiran atau pendapat dengan jelas, singkat dan tepat dengan menggunakan cara/media yang sesuai dan mengikuti alur yang logis; |

| | | | |
|-------------------------|---|---|---|
| | | | <p>1.2. Memastikan pemahaman yang sama atas instruksi yang diterima/ diberikan;</p> <p>1.3. Mampu melaksanakan kegiatan surat menyurat sesuai tata naskah organisasi.</p> |
| 4. Orientasi pada hasil | 1 | Bertanggung jawab untuk memenuhi standar kerja. | <p>1.1. Menyelesaikan tugas dengan tuntas; dapat diandalkan;</p> <p>1.2. Bekerja dengan teliti dan hati-hati guna meminimalkan kesalahan dengan mengacu pada standar kualitas (SOP);</p> <p>1.3. Bersedia menerima masukan, mengikuti contoh cara bekerja yang lebih efektif, efisien di lingkungan kerjanya.</p> |
| 5. Pelayanan publik | 1 | Menjalankan tugas mengikuti standar pelayanan. | <p>1.1. Mampu mengerjakan tugas-tugas dengan mengikuti standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/ kelompok/ partai politik;</p> <p>1.2. Melayanai kebutuhan, permintaan dan keluhan pemangku</p> |

| | | | |
|-------------------------------------|---|------------------------------------|--|
| | | | <p>kepentingan;</p> <p>1.3. Menyelesaikan masalah dengan tepat tanpa bersikap membela diri dalam kapasitas sebagai pelaksana pelayanan publik.</p> |
| 6. Pengembangan diri dan orang lain | 1 | Pengembangan diri. | <p>1.1. Mengidentifikasi kebutuhan pengembangan diri dan menyeleksi sumber serta metodologi pembelajaran yang diperlukan;</p> <p>1.2. Menunjukkan usaha mandiri untuk mempelajari keterampilan atau kemampuan baru dari berbagai media pembelajaran;</p> <p>1.3. Berupaya meningkatkan diri dengan belajar dari orang-orang lain yang berwawasan luas di dalam organisasi.</p> |
| 7. Mengelola perubahan | 1 | Mengikuti perubahan dengan arahan. | <p>1.1. Sadar mengenai perubahan yang terjadi di organisasi dan berusaha menyesuaikan diri dengan perubahan tersebut;</p> <p>1.2. Mengikuti perubahan secara terbuka sesuai petunjuk/pedoman;</p> |

| | | | |
|---------------------------|---|---|--|
| | | | 1.3. Menyesuaikan cara kerja lama dengan menerapkan metode/proses baru dengan bimbingan orang lain. |
| 8. Pengambilan keputusan | 1 | Mengumpulkan informasi untuk bertindak sesuai kewenangan. | 1.1. Mengumpulkan dan mempertimbangkan informasi yang dibutuhkan dalam mencari solusi; 1.2. Mengenali situasi/pilihan yang tepat untuk bertindak sesuai kewenangan; 1.3. Mempertimbangkan kemungkinan solusi yang dapat diterapkan dalam pekerjaan rutin berdasarkan kebijakan dan prosedur yang telah ditentukan. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 1 | Peka memahami dan menerima kemajemukan. | 1.1. Mampu memahami, menerima, peka terhadap perbedaan individu/ kelompok masyarakat; 1.2. Terbuka, ingin belajar tentang perbedaan/kemajemukan masyarakat; 1.3. Mampu bekerja bersama dengan individu yang berbeda latar belakang dengannya. |

| C. Teknis | | | |
|---|---|--|---|
| 10. Manajemen Keamanan Siber dan Persandian | 1 | Memahami konsep dasar dan menguasai teori manajemen keamanan siber dan persandian. | <p>1.1 Mampu menjelaskan konsep dasar manajemen keamanan siber dan persandian;</p> <p>1.2 Mampu menguraikan tahapan implementasi teori manajemen keamanan siber dan persandian;</p> <p>1.3 Mampu mengasosiasikan teori Manajemen Keamanan Siber dan Persandian dengan norma, standar, prosedur, dan kriteria manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 1 | Memahami substansi kebijakan, teknik, dan metode advokasi. | <p>1.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>1.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan,</p> |

| | | | |
|---------------------|---|---|--|
| | | | <p>mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi;</p> <p>1.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| 12. Pengelolaan SOC | 1 | Menjelaskan konsep dasar, teknik, metode, sistem, peraturan, tata cara, prosedur pengelolaan SOC. | <p>1.1 Mampu menjelaskan konsep dasar, teknik, metode, sistem, peraturan, tata cara prosedur, tujuan dan manfaat pengelolaan SOC;</p> <p>1.2 Mampu menjelaskan konsep dasar, teknik metode, kriteria, tujuan, manfaat, dan identifikasi dukungan teknis operasional SOC;</p> <p>1.3 Mampu mengidentifikasi norma, standar, prosedur, kriteria pengelolaan</p> |

| | | | SOC yang berlaku. |
|--|---|--|---|
| 13.Manajemen Insiden Siber | 1 | Memahami konsep dasar, teknik, metode, peraturan, dan mekanisme, tata cara prosedur manajemen insiden siber. | 1.1 Mampu menjelaskan konsep dasar, teknik metode, peraturan dan mekanisme, tata cara prosedur manajemen insiden siber; 1.2 Mampu menjelaskan tahapan pelaksanaan manajemen insiden siber; 1.3 Mampu menjelaskan berbagai manfaat dari manajemen insiden siber. |
| 14.Pengelolaan Pusat Kontak Siber Nasional | 1 | Menjelaskan konsep dasar, teknik metode, peraturan, tata cara prosedur pengelolaan pusat kontak siber. | 1.1 Mampu menjelaskan konsep dasar, teknik metode, peraturan dan tata cara prosedur pengelolaan pusat kontak siber; 1.2 Mampu menjelaskan tujuan dan manfaat pengelolaan pusat kontak siber; 1.3 Mampu mengidentifikasi norma, standar, prosedur, dan kriteria pengelolaan pusat kontak siber yang berlaku. |
| 15.Monitoring Keamanan Jaringan | 1 | Memahami konsep dasar, teknik metode, tata cara dan prosedur dalam | 1.1 Mampu menjelaskan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan; |

| | | melakukan <i>monitoring</i> keamanan jaringan. | 1.2 Mampu menjelaskan fungsi dan manfaat perangkat <i>monitoring</i> keamanan jaringan; 1.3 Mampu menjelaskan tata cara dalam melakukan konfigurasi perangkat <i>monitoring</i> keamanan jaringan. | | |
|---------------------------------|----------------|---|---|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |

| | | | | | |
|--|--|------------------------------|---|---|--|
| | b. Pelatihan Dasar Persandian | | X | | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | | |
| | d. Pelatihan SOC | | X | | |
| | e. Pelatihan <i>Cyber Threat Analysis</i> | | | X | |
| | f. Pelatihan <i>Cyber Defence Operation</i> | | | X | |
| | g. Pelatihan Manajemen Insiden | | X | | |
| | h. Pelatihan Penanganan Insiden (<i>Incident Handling</i>) | | | X | |
| | i. Pelatihan Investigasi Siber | | X | | |
| | j. Pelatihan Perangkat Keamanan Jaringan | | X | | |
| | 3. Fungsional | Fungsional Sandiman Terampil | | X | |
| | C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | |

| | | | | |
|------------------------------|--|---|--|--|
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | |
| D. Pangkat | II/c (Pengatur) II/d (Pengatur Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil operasional layanan keamanan informasi, keamanan siber, dan persandian | | | |

b. Fungsi Pengkajian

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Terampil |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

JABATAN FUNGSIONAL SANDIMAN TERAMPIL**I. IKHTISAR JABATAN**

| | |
|------------------|---|
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan TI, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. |
|------------------|---|

II. STANDAR KOMPETENSI

| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
|------------|-------|-----------|----------------------|
|------------|-------|-----------|----------------------|

| A. Manajerial | | | |
|----------------------|---|---|---|
| 1. Integritas | 1 | Mampu bertindak sesuai nilai, norma, dan etika organisasi, dalam kapasitas pribadi. | <p>1.1. Bertingkah laku sesuai dengan perkataan; berkata sesuai dengan fakta;</p> <p>1.2. Melaksanakan peraturan, kode etik organisasi dalam lingkungan kerja sehari-hari, pada tataran individu/ pribadi;</p> <p>1.3. Tidak menjanjikan/memberikan sesuatu yang bertentangan dengan aturan organisasi.</p> |
| 2. Kerjasama | 1 | Berpartisipasi dalam kelompok kerja. | <p>1.1. Berpartisipasi sebagai anggota tim yang baik, melakukan tugas/bagiannya, dan mendukung keputusan tim;</p> <p>1.2. Mendengarkan dan menghargai masukan dari orang lain dan memberikan usulan-usulan bagi kepentingan tim;</p> <p>1.3. Mampu menjalin interaksi sosial untuk penyelesaian tugas.</p> |
| 3. Komunikasi | 1 | Menyampaikan informasi dengan jelas, lengkap, pemahaman yang sama. | <p>1.1. Menyampaikan informasi (data), pikiran atau pendapat dengan jelas, singkat dan tepat dengan menggunakan cara/media yang sesuai dan mengikuti alur yang logis;</p> <p>1.2. Memastikan pemahaman yang sama atas instruksi</p> |

| | | | |
|-------------------------|---|---|--|
| | | | yang diterima/diberikan; 1.3. Mampu melaksanakan kegiatan surat menyurat sesuai tata naskah organisasi. |
| 4. Orientasi pada hasil | 1 | Bertanggung jawab untuk memenuhi standar kerja. | 1.1. Menyelesaikan tugas dengan tuntas; dapat diandalkan; 1.2. Bekerja dengan teliti dan hati-hati guna meminimalkan kesalahan dengan mengacu pada standar kualitas (SOP); 1.3. Bersedia menerima masukan, mengikuti contoh cara bekerja yang lebih efektif, efisien di lingkungan kerjanya. |
| 5. Pelayanan publik | 1 | Menjalankan tugas mengikuti standar pelayanan. | 1.1. Mampu mengerjakan tugas-tugas dengan mengikuti standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/ kelompok/partai politik; 1.2. Melayanai kebutuhan, permintaan dan keluhan pemangku kepentingan; 1.3. Meneyelesaikan masalah dengan tepat tanpa bersikap membela diri dalam kapasitas sebagai pelaksana pelayanan |

| | | | |
|-------------------------------------|---|---|--|
| | | | publik. |
| 6. Pengembangan diri dan orang lain | 1 | Pengembangan diri. | <p>1.1. Mengidentifikasi kebutuhan pengembangan diri dan menyeleksi sumber serta metodologi pembelajaran yang diperlukan;</p> <p>1.2. Menunjukkan usaha mandiri untuk mempelajari keterampilan atau kemampuan baru dari berbagai media pembelajaran;</p> <p>1.3. Berupaya meningkatkan diri dengan belajar dari orang-orang lain yang berwawasan luas di dalam organisasi.</p> |
| 7. Mengelola perubahan | 1 | Mengikuti perubahan dengan arahan. | <p>1.1. Sadar mengenai perubahan yang terjadi di organisasi dan berusaha menyesuaikan diri dengan perubahan tersebut;</p> <p>1.2. Mengikuti perubahan secara terbuka sesuai petunjuk/pedoman;</p> <p>1.3. Menyesuaikan cara kerja lama dengan menerapkan metode/proses baru dengan bimbingan orang lain.</p> |
| 8. Pengambilan keputusan | 1 | Mengumpulkan informasi untuk bertindak sesuai kewenangan. | <p>1.1. Mengumpulkan dan mempertimbangkan informasi yang dibutuhkan dalam mencari solusi;</p> <p>1.2. Mengenali situasi/pilihan</p> |

| | | | |
|---|---|--|--|
| | | | <p>yang tepat untuk bertindak sesuai kewenangan;</p> <p>1.3. Mempertimbangkan kemungkinan solusi yang dapat diterapkan dalam pekerjaan rutin berdasarkan kebijakan dan prosedur yang telah ditentukan.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 1 | Peka memahami dan menerima kemajemukan. | <p>1.1. Mampu memahami, menerima, peka terhadap perbedaan individu/kelompok masyarakat;</p> <p>1.2. Terbuka, ingin belajar tentang perbedaan/kemajemukan masyarakat;</p> <p>1.3. Mampu bekerja bersama dengan individu yang berbeda latar belakang dengannya.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 1 | Memahami konsep dasar dan menguasai teori manajemen keamanan siber dan persandian. | <p>1.1 Mampu menjelaskan konsep dasar manajemen keamanan siber dan persandian;</p> <p>1.2 Mampu menguraikan tahapan implementasi teori manajemen keamanan siber dan persandian;</p> <p>1.3 Mampu mengasosiasikan teori Manajemen Keamanan Siber dan Persandian dengan norma,</p> |

| | | | |
|--------------------------------------|---|--|--|
| | | | standar, prosedur, dan kriteria manajemen keamanan siber dan persandian. |
| 11.Advokasi Kebijakan Keamanan Siber | 1 | Memahami substansi kebijakan, teknik, dan metode advokasi. | <p>1.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>1.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi;</p> <p>1.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil</p> |

| | | | |
|--|---|---|--|
| | | | <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. |
| 12.Rekayasa Kriptografi | 1 | Mengetahui konsep dasar dan prosedur rekayasa kriptografi. | 1.1 Mampu mendaftar perangkat yang dibutuhkan dalam rekayasa kriptografi; 1.2 Mampu memahami konsep dan teori dasar terkait pengkajian teknologi keamanan siber dan sandi; 1.3 Mampu memahami prosedur kerja atau petunjuk teknis melaksanakan rekayasa kriptografi. |
| 13.Rancang Bangun Perangkat Keamanan Teknologi Informasi | 1 | Mengetahui konsep dasar dan prosedur rancang bangun perangkat keamanan Teknologi Informasi. | 1.1 Mampu mendaftar perangkat yang dibutuhkan dalam rancang bangun keamanan TI; 1.2 Mampu memahami konsep dan teori dasar terkait rancang bangun perangkat keamanan TI; 1.3 Mampu memasang konfigurasi perangkat keamanan TI hasil rancang bangun. |
| 14.Pengkajian Teknologi Keamanan Siber dan Sandi | 1 | Mengetahui konsep dasar dan prosedur pengkajian teknologi keamanan siber dan sandi. | 1.1 Mampu mendaftar perangkat yang dibutuhkan dalam pengkajian teknologi keamanan siber dan sandi; 1.2 Mampu memahami pedoman kerja atau |

| | | | petunjuk teknis dalam pengkajian teknologi keamanan siber dan sandi; 1.3 Mampu memahami konsep dan teori dasar terkait pengkajian teknologi keamanan siber dan sandi. | | |
|--|----------------|---|--|---------|-------|
| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 1 | Mengetahui konsep dasar teknik, metode, peraturan, dan mekanisme, tata cara prosedur penelitian terkait teknologi keamanan siber dan sandi. | 1.1 Mampu mendaftar perangkat yang dibutuhkan dalam penelitian teknologi keamanan siber dan sandi; 1.2 Mampu memahami prosedur kerja atau petunjuk teknis melaksanakan tahapan penelitian; 1.3 Mampu mengkategorikan jenis penelitian, pemetaan personil, dan kerja sama yang dibutuhkan dalam penelitian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistim Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |

| | | | | |
|-----------|---|--|---|--|
| 2. Teknis | b. Pelatihan Pengembangan Diri | | X | |
| | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | d. Pelatihan Teknik Komunikasi | | X | |
| | a. Pelatihan Dasar Keamanan Siber | | X | |
| | b. Pelatihan Dasar Persandian | | X | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | d. Pelatihan Kriptografi Simetrik | | X | |
| | e. Pelatihan Kriptografi Asimetrik | | X | |
| | f. Pelatihan Fungsi Hash | | X | |
| | g. Pelatihan Pembangkit Bilangan Acak | | X | |
| | h. Pelatihan Infrastruktur Kunci Publik | | X | |
| | i. Pelatihan | | X | |

| | | | | | |
|---------------------|----|--|------------------------------|---|---|
| | | Protokol Kriptografi | | | |
| | | j. Pelatihan Bahasa Pemrograman | | X | |
| | | k. Pelatihan Steganografi | | X | |
| | | l. Pelatihan <i>Embedded System</i> | | X | |
| | | m. Pelatihan Perancangan Piranti Lunak | | X | |
| | | n. Pelatihan Perancangan Piranti Keras | | X | |
| | | o. Pelatihan <i>Software Testing</i> | | X | |
| | | p. Pelatihan <i>Hardware Testing</i> | | X | |
| | | q. Pelatihan Keamanan Jaringan | | X | |
| | | r. Pelatihan Pengelolaan Penelitian | | X | |
| | | 3. Fungsional | Fungsional Sandiman Terampil | | X |
| C. Pengalaman Kerja | a. | Lulus Diklat Dasar | X | | |
| | b. | Memiliki pengalaman di bidang | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | | | |
| D. Pangkat | II/c (Pengatur) II/d (Pengatur Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil operasional layanan keamanan informasi, keamanan siber, dan persandian | | | |

c. Fungsi Proteksi

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Terampil |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN TERAMPIL | |
|---|--|
| I. IKHTISAR JABATAN | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi dan <i>monitoring</i> keamanan jaringan. |
| II. STANDAR KOMPETENSI | |

| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
|----------------------|-------|---|---|
| A. Manajerial | | | |
| 1. Integritas | 1 | Mampu bertindak sesuai nilai, norma, dan etika organisasi, dalam kapasitas pribadi. | <p>1.1. Bertingkah laku sesuai dengan perkataan; berkata sesuai dengan fakta;</p> <p>1.2. Melaksanakan peraturan, kode etik organisasi dalam lingkungan kerja sehari-hari, pada tataran individu/ pribadi;</p> <p>1.3. Tidak menjanjikan/memberikan sesuatu yang bertentangan dengan aturan organisasi.</p> |
| 2. Kerjasama | 1 | Berpartisipasi dalam kelompok kerja. | <p>1.1. Berpartisipasi sebagai anggota tim yang baik, melakukan tugas/bagiannya, dan mendukung keputusan tim;</p> <p>1.2. Mendengarkan dan menghargai masukan dari orang lain dan memberikan usulan-usulan bagi kepentingan tim;</p> <p>1.3. Mampu menjalin interaksi sosial untuk penyelesaian tugas.</p> |
| 3. Komunikasi | 1 | Menyampaikan informasi dengan jelas, lengkap, pemahaman | 1.1. Menyampaikan informasi (data), pikiran atau pendapat dengan jelas, singkat dan tepat dengan menggunakan cara/media |

| | | | |
|-------------------------|---|---|--|
| | | yang sama. | yang sesuai dan mengikuti alur yang logis; 1.2. Memastikan pemahaman yang sama atas instruksi yang diterima/diberikan; 1.3. Mampu melaksanakan kegiatan surat menyurat sesuai tata naskah organisasi. |
| 4. Orientasi pada hasil | 1 | Bertanggung jawab untuk memenuhi standar kerja. | 1.1. Menyelesaikan tugas dengan tuntas; dapat diandalkan; 1.2. Bekerja dengan teliti dan hati-hati guna meminimalkan kesalahan dengan mengacu pada standar kualitas (SOP); 1.3. Bersedia menerima masukan, mengikuti contoh cara bekerja yang lebih efektif, efisien di lingkungan kerjanya. |
| 5. Pelayanan publik | 1 | Menjalankan tugas mengikuti standar pelayanan. | 1.1. Mampu mengerjakan tugas-tugas dengan mengikuti standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/ kelompok/partai politik; 1.2. Melayanai kebutuhan, permintaan dan keluhan pemangku kepentingan; 1.3. Menyelesaikan masalah |

| | | | |
|-------------------------------------|---|------------------------------------|--|
| | | | dengan tepat tanpa bersikap membela diri dalam kapasitas sebagai pelaksana pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 1 | Pengembangan diri. | <p>1.1. Mengidentifikasi kebutuhan pengembangan diri dan menyeleksi sumber serta metodologi pembelajaran yang diperlukan;</p> <p>1.2. Menunjukkan usaha mandiri untuk mempelajari keterampilan atau kemampuan baru dari berbagai media pembelajaran;</p> <p>1.3. Berupaya meningkatkan diri dengan belajar dari orang-orang lain yang berwawasan luas di dalam organisasi.</p> |
| 7. Mengelola perubahan | 1 | Mengikuti perubahan dengan arahan. | <p>1.1. Sadar mengenai perubahan yang terjadi di organisasi dan berusaha menyesuaikan diri dengan perubahan tersebut;</p> <p>1.2. Mengikuti perubahan secara terbuka sesuai petunjuk/pedoman;</p> <p>1.3. Menyesuaikan cara kerja lama dengan menerapkan metode/proses baru dengan bimbingan orang lain.</p> |

| | | | |
|---|---|--|---|
| 8. Pengambilan keputusan | 1 | Mengumpulkan informasi untuk bertindak sesuai kewenangan. | <p>1.1. Mengumpulkan dan mempertimbangkan informasi yang dibutuhkan dalam mencari solusi;</p> <p>1.2. Mengenali situasi/pilihan yang tepat untuk bertindak sesuai kewenangan;</p> <p>1.3. Mempertimbangkan kemungkinan solusi yang dapat diterapkan dalam pekerjaan rutin berdasarkan kebijakan dan prosedur yang telah ditentukan.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 1 | Peka memahami dan menerima kemajemukan. | <p>1.1. Mampu memahami, menerima, peka terhadap perbedaan individu/keompok masyarakat;</p> <p>1.2. Terbuka, ingin belajar tentang perbedaan/kemajemukan masyarakat;</p> <p>1.3. Mampu bekerja bersama dengan individu yang berbeda latar belakang dengannya.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 1 | Memahami konsep dasar dan menguasai teori manajemen keamanan siber | <p>1.1 Mampu menjelaskan konsep dasar manajemen keamanan siber dan persandian;</p> <p>1.2 Mampu menguraikan</p> |

| | | | |
|---------------------------------------|---|--|--|
| | | dan persandian. | <p>tahapan implementasi teori manajemen keamanan siber dan persandian;</p> <p>1.3 Mampu mengasosiasikan teori Manajemen Keamanan Siber dan Persandian dengan norma, standar, prosedur, dan kriteria manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 1 | Memahami substansi kebijakan, teknik, dan metode advokasi. | <p>1.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>1.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i></p> |

| | | | |
|------------------------------------|---|--|---|
| | | | <p>dalam implementasi keamanan informasi;</p> <p>1.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| 12.Manajemen Risiko Keamanan Siber | 1 | Memahami konsep dan teori manajemen risiko keamanan informasi. | <p>1.1 Mampu menjelaskan risiko keamanan informasi;</p> <p>1.2 Mampu menyebutkan risiko dalam keamanan informasi;</p> <p>1.3 Mampu menjelaskan konsep dan teori dalam manajemen risiko;</p> <p>1.4 Mampu mengidentifikasi aset yang terkait dengan keamanan informasi.</p> |
| 13.Audit Keamanan Informasi | 1 | Mampu menjelaskan konsep audit keamanan informasi, keamanan siber, dan persandian. | <p>1.1 Mampu menjelaskan tahapan audit keamanan informasi, keamanan siber, dan persandian;</p> <p>1.2 Mampu menjelaskan tujuan dan manfaat audit keamanan informasi, keamanan siber, dan persandian;</p> <p>1.3 Mampu mengidentifikasi norma,</p> |

| | | | | |
|---|--------|--|---|------|
| | | | standar, prosedur, dan kriteria audit keamanan informasi lain yang berlaku. | |
| 14. Penyediaan Layanan Keamanan Informasi | 1 | Memahami konsep dasar, metode, dan peraturan penyediaan layanan keamanan informasi. | <p>1.1 Mampu menjelaskan jenis dan konsep penyediaan layanan keamanan informasi;</p> <p>1.2 Mampu menjelaskan tahapan penyediaan layanan keamanan informasi;</p> <p>1.3 Mampu mengidentifikasi norma, standar, prosedur, dan kriteria penyediaan layanan keamanan informasi.</p> | |
| 15. <i>Monitoring</i> Keamanan Jaringan | 1 | Memahami konsep dasar, teknik, metode, tata cara dan prosedur dalam melakukan <i>monitoring</i> keamanan jaringan. | <p>1.1 Mampu menjelaskan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan;</p> <p>1.2 Mampu menjelaskan fungsi dan manfaat perangkat <i>monitoring</i> keamanan jaringan;</p> <p>1.3 Mampu menjelaskan tata cara dalam melakukan konfigurasi perangkat <i>monitoring</i> keamanan jaringan.</p> | |
| III. PERSYARATAN JABATAN | | | | |
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | Mutla | Pentin | Perl |

| | | | k | g | u |
|---------------|----------------|---|---|---|---|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |
| | | b. Pelatihan Dasar Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Dasar Keamanan Jaringan | | X | |
| | | e. Pelatihan Tata Kelola TIK | | X | |
| | | | | | |

| | | | | | |
|------------------------------|--|---|--|---|--|
| | | f. Pelatihan Audit Keamanan Informasi | | X | |
| | | g. Pelatihan Perangkat Keamanan Siber, Keamanan Informasi, dan Persandian | | X | |
| | | h. Pelatihan Manajemen Akses Kontrol | | X | |
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | 3. Fungsional | Fungsional Sandiman Terampil | | X | |
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | | |
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| D. Pangkat | II/c (Pengatur) II/d (Pengatur Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil operasional layanan keamanan informasi, keamanan siber, dan persandian | | | | |

2. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN MAHIR/
PELAKSANA LANJUTAN

a. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Mahir |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN MAHIR | | | |
|--|--|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi kendali operasi keamanan siber dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan <i>security operation center</i> (SOC), pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatnkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 2.2. Mengajak orang lain untuk bertindak sesuai etika dan kode etik; 2.3. Menerapkan norma-norma secara konsisten dalam |

| | | | |
|---------------|---|--|--|
| | | | <p>setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.4. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; | 2.1. Menggunakan gaya komunikasi informal untuk |

| | | | |
|-------------------------|---|--|--|
| | | Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dan lain-lain. | meningkatkan hubungan profesional; 2.2. Mendengarkan pihak lain secara aktif; 2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai; 2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dan lain-lain sesuai arahan pimpinan. |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, dan mencoba metode alternatif untuk peningkatan kinerja. | 2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi; 2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya; 2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih |

| | | | |
|---------------------|---|---|---|
| | | | efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain; |

| | | | |
|---------------------------|---|--|---|
| | | | <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam</p> |

| | | | |
|--|---|---|--|
| | | | <p>organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, gender, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam Perumusan Kebijakan Manajemen Keamanan Siber dan Persandian dan menerapkan kontrol keamanan siber dan persandian. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian;</p> <p>2.2 Mampu mengklasifikasikan aset-aset penting yang rentan terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasikan risiko keamanan siber dan</p> |

| | | | |
|---------------------------------------|---|--|---|
| | | | persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu melakukan advokasi kebijakan keamanan siber. | <p>2.1 Mampu menyusun rencana pelaksanaan kegiatan advokasi kebijakan;</p> <p>2.2 Mampu membuat alat bantu untuk kebutuhan advokasi, melakukan sosialisasi kebijakan dengan audiensi lingkup kecil;</p> <p>2.3 Mampu mengidentifikasi posisi dasar dan kebutuhan pemangku kepentingan terkait advokasi kebijakan.</p> |
| 12. Pengelolaan SOC | 2 | Menerapkan pengelolaan SOC. | <p>2.1 Mampu melaksanakan pengelolaan SOC sesuai prosedur;</p> <p>2.2 Mampu melatih <i>stakeholder</i> untuk dapat mengelola SOC;</p> <p>2.3 Mampu menentukan spesifikasi dukungan teknis operasional SOC;</p> <p>2.4 Mampu mengklasifikasikan dukungan teknis</p> |

| | | | |
|------------------------------------|---|---|--|
| | | | operasional SOC; 2.5 Mampu menggunakan instrumen penilaian maturitas SOC. |
| 13. Manajemen Insiden Siber | 2 | Mampu melaksanakan Manajemen Insiden Siber sesuai pedoman kerja/ petunjuk teknis. | 2.1 Mampu melaksanakan proses manajemen insiden sesuai prosedur yang ditetapkan; 2.2 Mampu menggunakan alat, metode, dan teknik untuk melakukan manajemen insiden siber; 2.3 Mampu mengidentifikasi permasalahan dasar terkait manajemen insiden siber; 2.4 Mampu menggambarkan prosedur manajemen insiden siber dalam bentuk SOP sederhana dan jadwal kerja; 2.5 Mampu mendemonstrasikan prosedur dan teknik pengelolaan. |
| 14. Pengelolaan Pusat Kontak Siber | 2 | Menerapkan konsep pengelolaan pusat kontak siber. | 2.1 Mampu menggunakan instrumen |

| | | | | |
|---|--------|---|---|------|
| Nasional | | | <p>pengelolaan pusat kontak siber;</p> <p>2.2 Mampu melengkapi bukti aduan dan identitas pelapor aduan siber;</p> <p>2.3 Mampu menentukan aduan siber terverifikasi dan tidak terverifikasi.</p> | |
| 15. <i>Monitoring</i> Keamanan Jaringan | 2 | Mampu menerapkan <i>monitoring</i> keamanan jaringan. | <p>2.1. Mampu menggunakan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan;</p> <p>2.2. Mampu mengoperasikan perangkat <i>monitoring</i> keamanan jaringan;</p> <p>2.3. Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan;</p> <p>2.4. Mampu mendemonstrasikan <i>monitoring</i> lalu lintas jaringan.</p> | |
| III. PERSYARATAN JABATAN | | | | |
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | Mutla | Pentin | Perl |

| | | | k | g | u |
|--|----------------|---|---|---|---|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan dasar keamanan siber | | X | |
| | | b. Pelatihan dasar persandian | | X | |
| | | c. Pelatihan kebijakan keamanan siber | | X | |
| | | d. Pelatihan <i>security operation center</i> | | X | |
| | | e. Pelatihan <i>cyber threat intelligence</i> | | | X |
| | | f. Pelatihan <i>cyber defense operation</i> | | | X |
| | | g. Pelatihan manajemen insiden | | X | |
| h. Pelatihan penanganan insiden (<i>Incident Handling</i>) | | | X | | |
| i. Pelatihan investigasi siber | | X | | | |
| j. Pelatihan | | X | | | |

| | | | | | |
|------------------------------|--|-----------------------------|--|---|--|
| | | perangkat keamanan jaringan | | | |
| | 3. Fungsional | Fungsional Sandiman Mahir | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Terampil | | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis layanan keamanan informasi, keamanan siber, dan persandian | | | | |

b. Fungsi Pengkajian

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Mahir |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

JABATAN FUNGSIONAL SANDIMAN MAHIR

| I. IKHTISAR JABATAN | |
|---------------------|---|
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang |

| | | bangun perangkat keamanan teknologi informasi, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. | |
|-------------------------------|-------|---|--|
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | <p>2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>2.2. Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.3. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.4. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | 2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran |

| | | | |
|-------------------------|---|---|---|
| | | | <p>tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif; menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.3. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang | 2.1. Menetapkan dan berupaya mencapai |

| | | | |
|---------------------|---|---|--|
| | | <p>lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja.</p> | <p>standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya.</p> |
| 5. Pelayanan publik | 2 | <p>Mampu mensupervisi/mengawasi/menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan.</p> | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan</p> |

| | | | |
|-------------------------------------|---|---|---|
| | | | <p>pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tata cara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik.</p> |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa</p> |

| | | | |
|--------------------------|---|---|---|
| | | | orang lain telah memahami penjelasan atau pengarahan. |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | <p>2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |

| B. Sosial Kultural | | | |
|---|---|--|---|
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan, dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | 2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian; |

| | | | |
|--------------------------------------|---|--|--|
| | | | <p>2.2 Mampu mengklasifikasi-kan asset-aset penting yang rentang terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasi-kan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi.</p> |
| 11.Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> , dan evaluasi kebijakan keamanan informasi. | <p>2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan</p> |

| | | | |
|-------------------------|---|--|--|
| | | | <p>keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12.Rekayasa Kriptografi | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan perancangan desain rekayasa kriptografi | <p>2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil rekayasa kriptografi;</p> <p>2.2 Mampu menerapkan prosedur kerja atau petunjuk teknis perancangan desain rekayasa kriptografi;</p> <p>2.3 Mampu menerapkan simulasi rekayasa</p> |

| | | | |
|--|---|--|--|
| | | | kriptografi. |
| 13.Rancang Bangun Perangkat Keamanan Teknologi Informasi | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan perancangan desain perangkat keamanan TI. | 2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil Pengkajian Teknologi keamanan siber dan sandi; 2.2 Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi; 2.3 Mampu menerapkan desain perangkat keamanan TI pada suatu <i>framework</i> tertentu. |
| 14.Pengkajian Teknologi Keamanan Siber dan Sandi | 2 | Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan Pengkajian Teknologi keamanan siber dan sandi. | 2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil Pengkajian Teknologi keamanan siber dan sandi; 2.2 Mampu menggali celah keamanan dalam suatu teknologi informasi; 2.3 Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi. |

| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan penelitian | 2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil rekayasa kriptografi; 2.2 Mampu menerapkan prosedur kerja atau petunjuk teknis tahapan proses penelitian. | | |
|--|----------------|---|---|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |
| | | b. Pelatihan Dasar Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |

| | | | | |
|--------------------------------|--|---|---|--|
| | d. Pelatihan Kriptografi Simetrik | | X | |
| | e. Pelatihan Kriptografi Asimetrik | | X | |
| | f. Pelatihan Fungsi <i>Hash</i> | | X | |
| | g. Pelatihan Pembangkit Bilangan Acak | | X | |
| | h. Pelatihan Infrastruktur Kunci Publik | | X | |
| | i. Pelatihan Protokol Kriptografi | | X | |
| | j. Pelatihan Bahasa Pemrograman | | X | |
| | k. Pelatihan Steganografi | | X | |
| | l. Pelatihan <i>Embedded System</i> | | X | |
| | m. Pelatihan Perancangan Piranti Lunak | | X | |
| | n. Pelatihan Perancangan Piranti Keras | | X | |
| | o. Pelatihan <i>Software Testing</i> | | X | |
| | p. Pelatihan <i>Hardware Testing</i> | | X | |
| | q. Pelatihan Keamanan Jaringan | | X | |
| r. Pelatihan Pengelolaan Kunci | | X | | |
| 3. Fungsional | Diklat Fungsional Sandiman Mahir | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Terampil | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis layanan keamanan informasi, keamanan siber, dan persandian | | | |

c. Fungsi Proteksi

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Mahir |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN MAHIR | | | |
|--|---|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; |

| | | | |
|--------------|---|--|--|
| | | | <p>Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.2. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.3. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim; mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.3. Membangun</p> |

| | | | |
|-------------------------|---|---|---|
| | | | komitmen yang tinggi untuk menyelesaikan tugas tim. |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh</p> |

| | | | |
|---------------------|---|---|---|
| | | | kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara,</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan |

| | | | |
|---------------------------|---|--|---|
| | | | <p>metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perikat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | 2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman |

| | | | |
|--|---|--|--|
| | | | <p>dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasi kan aset-aset penting yang rentang terhadap ancaman;</p> |

| | | | |
|---------------------------------------|---|--|---|
| | | | <p>2.3 Mampu mengkalkulasi-kan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasi-kan prosedur teknis penerapan kontrol keamanan informasi.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | <p>2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi</p> |

| | | | |
|------------------------------------|---|--|---|
| | | | <p>kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12.Manajemen Risiko Keamanan Siber | 2 | Mampu mengaplikasikan manajemen risiko keamanan informasi. | <p>2.1 Mampu mengklasifikasikan aset yang terkait keamanan informasi;</p> <p>2.2 Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan;</p> <p>2.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang</p> |

| | | | |
|---|---|--|---|
| | | | telah ditentukan. |
| 13.Audit Keamanan Informasi | 2 | Menerapkan konsep Audit Keamanan Informasi, Keamanan Siber dan Persandian. | 2.1 Mampu menentukan standar, prosedur dan kriteria Audit Keamanan Informasi, Keamanan Siber dan Persandian; 2.2 Mampu menggunakan instrumen audit keamanan informasi, keamanan siber dan persandian; 2.3 Mampu menentukan data yang diperlukan untuk kegiatan audit keamanan informasi, keamanan siber dan persandian. |
| 14.Penyediaan Layanan Keamanan Informasi | 2 | Menyelenggarakan penyediaan layanan keamanan informasi sesuai dengan prosedur/ petunjuk teknis | 2.1 Mampu menentukan kebutuhan pengguna dan kecukupan sumber daya yang dialokasikan oleh organisasi untuk melaksanakan penyediaan layanan keamanan informasi; |

| | | | |
|---|---|---|---|
| | | | <p>2.2 Mampu melaksanakan layanan keamanan informasi berdasarkan norma, standar, prosedur, dan kriteria yang berlaku;</p> <p>2.3 Mampu menangani permasalahan teknis saat penyelenggaraan layanan keamanan informasi.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 2 | Mampu menerapkan <i>monitoring</i> keamanan jaringan. | <p>2.1 Mampu menggunakan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan;</p> <p>2.2 Mampu mengoperasikan perangkat <i>monitoring</i> keamanan jaringan;</p> <p>2.3 Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan;</p> <p>2.4 Mampu mendemonstrasikan <i>monitoring</i> lalu lintas jaringan.</p> |
| III. PERSYARATAN JABATAN | | | |

| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
|-------------------|----------------|---|-------------------------------------|---------|-------|
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |
| | | b. Pelatihan Dasar Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Dasar Keamanan Jaringan | | X | |
| | | e. Pelatihan Tata Kelola TIK | | X | |
| | | f. Pelatihan Audit Keamanan Informasi | | X | |
| | | g. Pelatihan Perangkat Keamanan Siber, Keamanan Informasi, dan Persandian | | X | |
| | | h. Pelatihan Manajemen Akses Kontrol | | X | |

| | | | | | |
|------------------------------|---------------|--|---|---|--|
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | 3. Fungsional | Fungsional Sandiman Mahir | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | |
| | | b. Telah menduduki Jabatan Sandiman Terampil | | | |
| D. Pangkat | | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | | Hasil analisis layanan keamanan informasi, keamanan siber, dan persandian | | | |

3. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN PENYELIA

a. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Penyelia |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN PENYELIA | | | |
|--------------------------------------|--|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi kendali operasi keamanan siber dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan SOC, pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | <p>3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin.</p> |

| | | | |
|---------------|---|---|--|
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda; membuat</p> |

| | | | |
|-------------------------|---|--|--|
| | | | proposal yang rinci dan lengkap. |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | <p>masalah yang dihadapi pemangku kepentingan/ masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya.</p> |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan; memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.5. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit</p> |

| | | | |
|---------------------------|---|---|---|
| | | | kerjanya secara tepat; 3.4. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan. |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | 3.1. Membandingkan berbagai alternatif tindakan dan implikasinya; 3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku; 3.3. Mengidentifikasi potensi salah-pahaman yang diakibatkan adanya keragaman budaya yang ada; 3.4. Menjadi mediator untuk |

| | | | |
|---|---|---|--|
| | | | menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam Manajemen Keamanan Siber dan Persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu menyelenggarakan advokasi kebijakan keamanan siber. | <p>3.1 Mampu bahan menyusun instrumen dan pelaksanaan advokasi kebijakan pendekatan, melalui bimbingan sosialisasi, teknis, pendampingan, dan <i>monitoring</i> evaluasi advokasi kebijakan;</p> <p>3.2 Mampu mengembangkan serta menjalankan strategi atau intervensi melalui sosialisasi, pendekatan, bimbingan teknis, dan pendampingan dalam mengatasi hambatan sistemis dan resistensi pemangku kepentingan dalam menerapkan kebijakan;</p> |

| | | | |
|--|---|---|---|
| | | | 3.3 Mampu mengimplementasikan strategi komunikasi dengan target dan waktu yang terukur dan terencana dengan mendapatkan hasil sesuai yang diharapkan antara lain pemangku kepentingan dapat memahami serta menerapkan kebijakan, <i>monitoring</i> , dan evaluasi kebijakan. |
| 12. Pengelolaan <i>Security Operation Center</i> (SOC) | 3 | Menganalisis keberlangsungan pengelolaan SOC. | 3.1 Mampu menelaah NSPK terkait pengelolaan SOC; 3.2 Mampu memeriksa keberlangsungan layanan pengelolaan SOC; 3.3 Mampu memecahkan masalah teknis operasional yang timbul; 3.4 Mampu membuat instrumen penilaian maturitas SOC; 3.5 Mampu menelaah spesifikasi dukungan teknis operasional SOC. |
| 13. Manajemen Insiden Siber | 3 | Mampu menyelenggarakan Manajemen Insiden Siber. | 3.1 Mampu melakukan analisis terkait manajemen insiden siber; 3.2 Mampu melaksanakan rekomendasi teknis terkait manajemen insiden siber; 3.3 Membimbing perbaikan kesalahan prosedur dalam manajemen insiden siber; 3.4 Mampu menunjukkan perbandingan antara kedua metode pengelolaan data tersebut, setidaknya dari segi kelebihan dan kekurangan; |

| | | | | | |
|---|----------------|--|---|---------|-------|
| | | | 3.5 Mengomunikasikan hasil analisis melalui lisan dan tulisan. | | |
| 14. Pengelolaan Pusat Kontak Siber Nasional | 3 | Menganalisis pelaksanaan pengelolaan pusat kontak siber. | 3.1 Mampu memeriksa proses pelaksanaan pengelolaan pusat kontak siber; 3.2 Mampu menganalisis masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber; 3.3 Mampu memecahkan masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber; 3.4 Mampu membuat garis besar instrumen pengelolaan pusat kontak siber. | | |
| 15. <i>Monitoring</i> Keamanan Jaringan | 3 | Mampu melakukan analisis keamanan jaringan. | 3.1 Mampu mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan; 3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan; 3.3 Mampu mendeteksi adanya anomali pada <i>log</i> perangkat <i>monitoring</i> keamanan jaringan; 3.4 Mampu menganalisis hasil temuan anomali. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi | | | |

| | | Komputer, Teknik Elektronika, Persandian | | | |
|--------------|-------------------|---|--|---|---|
| B. Pelatihan | 1. Manajeria 1 | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan dasar persandian | | X | |
| | | b. Pelatihan dasar keamanan siber | | X | |
| | | c. Pelatihan kebijakan keamanan siber | | X | |
| | | d. Pelatihan <i>Automation and Continuous Security Monitoring</i> | | X | |
| | | e. Pelatihan <i>cyber threat intelligence analysis</i> | | X | |
| | | f. Pelatihan manajemen insiden | | | X |
| | | g. Pelatihan penanganan insiden (<i>Incident Handling</i>) | | X | |
| | | h. Pelatihan Investigasi siber | | | X |

| | | | | | |
|------------------------------|--|--|--|---|---|
| | | i. Pelatihan <i>Cyber Defence Analysis</i> | | X | |
| | | j. Pelatihan <i>System Test and Evaluation</i> | | | X |
| | | k. Pelatihan arsitektur keamanan jaringan | | X | |
| | 3. Fungsional | Fungsional Sandiman Penyelia | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Mahir | | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi layanan keamanan informasi, keamanan siber, dan persandian | | | | |

b. Fungsi Pengkajian

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Penyelia |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN PENYELIA | | | |
|---|--|--|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan teknologi informasi, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk | 3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat; |

| | | | |
|-------------------------|---|--|---|
| | | peningkatan kinerja organisasi. | <p>3.2. Mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.3. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.4. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/tertulis untuk menyampaikan informasi yang sensitif/rumit/kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/periodik/ naskah/ dokumen/ proposal yang kompleks; Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda; membuat proposal yang rinci dan lengkap.</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan</p> |

| | | | |
|---------------------|---|--|---|
| | | memberi apresiasi, dan teguran untuk mendorong kinerja. | teguran untuk mendorong pencapaian hasil unit kerjanya; 3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya. |
| 5. Pelayanan public | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | 3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak; 3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya; 3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya. |
| 6. Pengemba | 3 | Memberikan | 3.1. Memberikan tugas-tugas yang |

| | | | |
|--------------------------|---|---|---|
| ngan diri dan orang lain | | umpan balik, membimbing. | <p>menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang</p> |

| | | | |
|---|---|---|--|
| | | n risiko keberhasilan dalam implementasi. | terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku; 3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada; 3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | 3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku; 3.2 Mampu menganalisis prosedur teknis penerapan kontro |

| | | | |
|---------------------------------------|---|---|--|
| | | | keamanan informasi ke dalam format NSPK yang berlaku; 3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan; 3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi; 3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. |
| 12. Rekayasa Kriptografi | 3 | Menganalisis rancangan rekayasa | 3.1 Mampu menguji hasil rekayasa kriptografi. 3.2 Mampu menganalisis kekuatan |

| | | | |
|---|---|--|---|
| | | kriptografi. | algoritma, manajemen kunci, dan protokol kriptografi. 3.3 Mampu menganalisis kebutuhan rekayasa kriptografi. |
| 13. Rancang Bangun Perangkat Keamanan Teknologi Informasi | 3 | Menganalisis perancangan perangkat keamanan teknologi informasi | 3.1 Mampu menemukan pola konfigurasi yang tepat pada perangkat keamanan teknologi informasi hasil rancang bangun. 3.2 Mampu menganalisis hasil pengujian perangkat keamanan teknologi informasi hasil rancang bangun. 3.3 Mampu menganalisis kebutuhan rancang bangun perangkat keamanan teknologi informasi. 3.4 Mampu memerinci spesifikasi teknis perangkat keamanan teknologi informasi hasil rancang bangun. 3.5 Mampu menjamin pemberian dukungan pada pengkajian teknologi keamanan siber dan sandi. |
| 14. Pengakajian Teknologi Keamanan Siber dan Sandi | 3 | Menganalisis pelaksanaan kegiatan pengkajian teknologi keamanan siber dan sandi. | 3.1 Mampu menguji celah keamanan teknologi informasi. 3.2 Mampu membuat blueprint simulasi perangkat keamanan teknologi informasi. 3.3 Mampu mengklasifikasikan prosedur dalam identifikasi kebutuhan pengkajian teknologi keamanan siber dan sandi. 3.4 Mampu menganalisis kebutuhan pengkajian teknologi keamanan siber dan sandi. |

| | | | | | |
|---|----------------|---|--|---------|-------|
| 15. Pengelola n Penelitian Teknologi Keamanan Siber dan Sandi Negara | 3 | Mengelola dan merencanakan penelitian. | 3.1 Mampu menata instrumen untuk kegiatan identifikasi, pengumpulan, pengolahan, dan pelaporan suatu kegiatan penelitian dalam bidang teknologi keamanan siber dan sandi. 3.2 Mampu mengoptimalkan pengetahuan terkait tujuan, metode, teknik analisis, dan kesimpulan suatu penelitian secara teknis maupun operasional melalui bimbingan teknis. 3.3 Mampu memecahkan masalah teknis operasional penelitian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |

| | | | | |
|-----------|---|--|---|--|
| 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |
| | b. Pelatihan Dasar Persandian | | X | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | d. Pelatihan Kriptografi Simetrik | | X | |
| | e. Pelatihan Kriptografi Asimetrik | | X | |
| | f. Pelatihan Fungsi <i>Hash</i> | | X | |
| | g. Pelatihan Pembangkit Bilangan Acak | | X | |
| | h. Pelatihan Infrastruktur Kunci Publik | | X | |
| | i. Pelatihan Protokol Kriptografi | | X | |
| | j. Pelatihan Bahasa Pemrograman | | X | |
| | k. Pelatihan Steganografi | | X | |
| | l. Pelatihan <i>Embedded System</i> | | X | |
| | m. Pelatihan Perancangan Piranti Lunak | | X | |
| | n. Pelatihan | | X | |

| | | | | | |
|------------------------------|---|---|---|---|--|
| | | Perancangan Piranti Keras | | | |
| | | o. Pelatihan <i>Software Testing</i> | | X | |
| | | p. Pelatihan <i>Hardware Testing</i> | | X | |
| | | q. Pelatihan Keamanan Jaringan | | X | |
| | | r. Pelatihan Pengelolaan Kunci | | X | |
| | 3. Fungsional | Diklat Fungsional Sandiman Penyelia | | X | |
| C. Pengalaman Kerja | a. | Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | |
| | b. | Telah menduduki Jabatan Sandiman Mahir | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi layanan keamanan informasi, keamanan siber, dan persandian | | | | |

c. Fungsi Proteksi

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Penyelia |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN PENYELIA | | | |
|--|--|--|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran |

| | | | |
|--------------|---|---|--|
| | | organisasi, dalam lingkup formal. | bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | 3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal; 3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/keompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja; 3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target |

| | | | |
|-------------------------|---|--|--|
| | | | kerja kelompok. |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/tertulis untuk menyampaikan informasi yang sensitif/rumit/kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap.</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih</p> |

| | | | |
|---------------------|---|--|--|
| | | | efektif dan efisien untuk mencapai target kerja unitnya. |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah</p> |

| | | | |
|-------------------------------------|---|-------------------------------------|--|
| | | | yang dihadapi pemangku kepentingan/ masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya. |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu</p> |

| | | | |
|--------------------------|---|---|---|
| | | | bawahan menemukan peluang untuk berkembang. |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat;</p> <p>3.4. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, dan mengikuti prinsip kehati-hatian;</p> <p>3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam</p> |

| | | | |
|---|---|---|---|
| | | | implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | <p>3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan;</p> <p>3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada;</p> <p>3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis</p> |

| | | | |
|---------------------------------------|---|--|--|
| | | | <p>penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | <p>Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> | <p>3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i></p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | <p>dalam implementasi keamanan informasi;</p> <p>3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| 12. Manajemen Risiko Keamanan Siber | 3 | Mampu melaksanakan penilaian risiko dan menganalisis penerapan manajemen risiko. | <p>3.1 Mampu mengidentifikasi risiko berdasarkan aset maupun proses bisnis organisasi;</p> <p>3.2 Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan;</p> <p>3.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan.</p> |
| 13. Audit Keamanan Informasi | 3 | Mengaudit keamanan informasi, keamanan siber dan persandian sesuai dengan prosedur/ petunjuk teknis | <p>3.1 Mampu menelaah kesesuaian data pada kegiatan audit keamanan informasi, keamanan siber dan persandian;</p> <p>3.2 Mampu mengaudit lapangan (<i>onsite</i>) sesuai</p> |

| | | | |
|---|---|--|--|
| | | | <p>prosedur, standar, dan norma tentang audit keamanan informasi, keamanan siber, dan persandian;</p> <p>3.3 Mampu mendokumentasikan hasil audit keamanan informasi, keamanan siber dan persandian;</p> <p>3.4 Mampu memeriksa proses audit keamanan informasi, keamanan siber, dan persandian.</p> |
| 14. Penyediaan Layanan Keamanan Informasi | 3 | Mengelola penyelenggaraan penyediaan layanan keamanan informasi. | <p>3.1 Mampu menganalisis kebutuhan penyelenggaraan layanan keamanan informasi sesuai dengan kebutuhan pengguna dan kecukupan sumber daya yang dialokasikan oleh organisasi atau pengguna;</p> <p>3.2 Mampu menganalisis norma, standar, prosedur, dan kriteria untuk penyelenggaraan layanan keamanan informasi;</p> <p>3.3 Mampu memberikan bimbingan teknis mengenai layanan keamanan informasi yang akan diterapkan.</p> |
| 15. <i>Monitoring</i> | 3 | Mampu | 3.1 Mampu |

| | | | | | |
|---------------------------------|----------------|---|---|---------|-------|
| Keamanan Jaringan | | melakukan analisis keamanan jaringan. | mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan; 3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan; 3.3 Mampu mendeteksi adanya anomali pada <i>log</i> perangkat <i>monitoring</i> keamanan jaringan; 3.4 Mampu menganalisis hasil temuan anomali. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah D-3 | | | |
| | 2. Bidang Ilmu | Ilmu Komputer/Informatika, Teknologi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Komputer, Teknik Elektronika, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik | | X | |

| | | | | | |
|--|-----------|---|------------|---|---|
| | | Komunikasi | | | |
| | 2. Teknis | a. Pelatihan Dasar Keamanan Siber | | X | |
| | | b. Pelatihan Dasar Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Dasar Keamanan Jaringan | | X | |
| | | e. Pelatihan Tata Kelola TIK | | X | |
| | | f. Pelatihan Audit Keamanan Informasi | | X | |
| | | g. Pelatihan Perangkat Keamanan Siber, Keamanan Informasi, dan Persandian | | X | |
| | | h. Pelatihan Manajemen Akses Kontrol | | X | |
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | | 3. Fungsional | Fungsional | | X |

| | | | | | |
|------------------------------|--|----------------------|--|--|--|
| | | Sandiman Penyelia | | | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Mahir | | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi layanan keamanan informasi, keamanan siber, dan persandian | | | | |

B. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN KATEGORI KEAHLIAN

1. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA

a. Fungsi Sertifikasi Elektronik

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|--|--|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi sertifikasi elektronik dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, analisis kelaikan sertifikat elektronik, pemenuhan teknis sistem sertifikasi elektronik, pengelolaan jaringan dan infrastruktur sertifikasi elektronik. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; Mengajak orang lain untuk bertindak sesuai etika dan kode etik; 2.2. Menerapkan norma- |

| | | | |
|---------------|---|--|--|
| | | | <p>norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.3. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; | 2.1. Menggunakan gaya komunikasi informal untuk meningkatkan |

| | | | |
|-------------------------|---|---|--|
| | | Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | <p>hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan, dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya.</p> |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia | 2.1. Menunjukkan sikap yakin dalam |

| | | | |
|-----------------|---|--|--|
| | | dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | mengerjakan tugas-tugas pemerintahan/pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil; 2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap; 2.3. Mampu mengenali dan memanfaatkan kebiasaan, tata cara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan | 2 | Meningkatkan | 2.1. Meningkatkan |

| | | | |
|--------------------------|---|--|---|
| diri dan orang lain | | kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan; 2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru; 2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan. |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain; 2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan; 2.3. Cepat dan tanggap dalam menerima perubahan. |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | 2.1. Melakukan analisis secara mendalam |

| | | | |
|---------------------------|---|--|---|
| | | | <p>terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perikat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh</p> |

| | | | |
|--|---|--|--|
| | | | perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik di lingkungan unit kerjanya. |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasi-kan aset-aset penting yang rentang terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasikan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi.</p> |
| 11.Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang |

| | | | |
|------------------------------------|---|--|--|
| | | | <p>dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12.Manajemen Risiko Keamanan Siber | 2 | Mampu mengaplikasikan manajemen risiko keamanan informasi. | 2.1 Mampu mengklasifikasi-kan aset yang terkait keamanan informasi; |

| | | | |
|--|---|--|--|
| | | | <p>2.2 Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan;</p> <p>2.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan.</p> |
| 13. Analisis Kelaikan Sertifikasi Elektronik | 2 | Mampu menerapkan konsep dasar, teknik, metode, tata cara, dan prosedur sertifikasi elektronik. | <p>2.1 Mampu menangani pelayanan administratif dalam rangka verifikasi terhadap dokumen dan berkas permohonan penerbitan, pembaruan, dan pencabutan sertifikat elektronik;</p> <p>2.2 Mampu menangani penerbitan, pembaruan, dan pencabutan sertifikat elektronik;</p> <p>2.3 Mampu mengklasifikasikan permasalahan dalam proses penerbitan, pembaruan, dan pencabutan sertifikat elektronik;</p> <p>2.4 Mampu</p> |

| | | | |
|---|---|---|--|
| | | | menerapkan sistem manajemen keamanan siber dan persandian dan manajemen kunci kriptografi. |
| 14. Pemenuhan Teknis Sistem Sertifikasi Elektronik | 2 | Mampu menerapkan pemenuhan teknis sistem sertifikasi elektronik. | <p>2.1 Mampu membangun sistem sertifikasi elektronik berdasarkan analisis kebutuhan;</p> <p>2.2 Mampu menerapkan modul-modul sertifikasi elektronik ke sistem milik pengguna;</p> <p>2.3 Mampu menerapkan sistem manajemen keamanan siber dan persandian dan manajemen kunci kriptografi;</p> <p>2.4 Mampu memberikan bimbingan teknis pengimplementasian sistem sertifikasi elektronik kepada pengguna.</p> |
| 15. Pengelolaan Jaringan dan Infrastruktur Sertifikasi Elektronik | 2 | Mampu menentukan keamanan jaringan, sistem dan aplikasi sertifikasi elektronik. | 2.1 Mampu melakukan instalasi dan konfigurasi jaringan, sistem, aplikasi dan perangkat keamanan dalam rangka |

| | | | penyelenggaraan sertifikasi elektronik; 2.2 Mampu merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (<i>business continuity dan disaster recovery plans</i>) penyelenggaraan sertifikasi elektronik; 2.3 Mampu melakukan <i>monitoring</i> keamanan dan pemeriksaan status sistem agar dapat beroperasi dengan baik; 2.4 Mampu melakukan <i>backup</i> data dan sistem. | | |
|---------------------------------|----------------|---|---|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |

| | | | | | |
|--|-----------|--|---|---|---|
| | 2. Teknis | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | | a. Pelatihan Infrastruktur Kunci Publik | X | | |
| | | b. Pelatihan <i>Public Key Infrastructure Core System</i> | | | X |
| | | c. Pelatihan Keamanan Sistem Informasi | X | | |
| | | d. Pelatihan Penyusunan Dokumen Pedoman/ Norma | | | X |
| | | e. Pelatihan <i>Software Development Life Cycle (SDLC)</i> | | X | |
| | | f. Pelatihan Pemrograman | | | X |
| | | g. Pelatihan Infrastruktur <i>Cloud</i> | | | X |
| | | h. Pelatihan Infrastruktur <i>Container</i> | | | X |

| | | | | | |
|------------------------------|---|----------------------------------|---|--|---|
| | | i. Pelatihan Administrasi Linux | | | X |
| | | j. Pelatihan Jaringan | | | X |
| | | k. Pelatihan Aplikasi Web Server | | | X |
| | | l. Pelatihan Database | | | X |
| | 3. Fungsional | Fungsional Sandiman Pertama | X | | |
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | | |
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | | |

b. Fungsi Sertifikasi dan Evaluasi Produk

| | | |
|--------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
|--------------|---|-----------------------|

| | | |
|-------------------|---|--------------------|
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|--|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan sertifikasi dan evaluasi produk dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan pengujian produk keamanan siber dan sandi negara, verifikasi algoritma kriptografi, <i>functional testing</i> , dan analisis kerawanan produk keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatnkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; Mengajak orang lain untuk bertindak sesuai etika dan kode etik; 2.2. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya; 2.3. Memberikan |

| | | | |
|---------------|---|---|--|
| | | | informasi yang dapat dipercaya sesuai dengan etika organisasi. |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan</p> |

| | | | |
|-------------------------|---|---|---|
| | | menyusun materi presentasi, pidato, naskah, laporan, dll. | menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai; 2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan, dll sesuai arahan pimpinan. |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | 2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi; 2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya; 2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara | 2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/pelayanan publik, mampu |

| | | | |
|-------------------------------------|---|--|--|
| | | transparan. | <p>menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tata cara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik.</p> |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan | 2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, |

| | | | |
|--------------------------|---|---|---|
| | | cara melaksanakan suatu pekerjaan. | instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan; 2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru; 2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan. |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain; 2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan; 2.3. Cepat dan tanggap dalam menerima perubahan. |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | 2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam |

| | | | |
|---------------------------|---|--|---|
| | | | <p>upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar</p> |

| | | | |
|---|---|--|---|
| | | | belakang, agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik di lingkungan unit kerjanya. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam Perumusan Kebijakan Manajemen Keamanan Siber dan Persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian;</p> <p>2.2 Mampu mengklasifikasi kan aset-aset penting yang rentang terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasi-kan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang |

| | | | |
|--|--|--|--|
| | | | <p>dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
|--|--|--|--|

| | | | |
|--|---|--|--|
| 12. Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara | 2 | Melaksanakan layanan pengujian produk. | 2.1 Mampu mengurutkan dan menurunkan tahapan pengujian produk ke dalam kegiatan yang lebih rinci sesuai pedoman kerja/ petunjuk teknis yang berlaku; 2.2 Mampu mendemonstrasikan tahapan-tahapan pengujian produk sesuai pedoman kerja/ petunjuk teknis yang berlaku; 2.3 Mampu menyusun laporan pelaksanaan pengujian produk. |
| 13. Verifikasi Algoritma Kriptografi | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan verifikasi algoritma kriptografi. | 2.1 Mampu mengurutkan tahapan kegiatan verifikasi algoritma kriptografi berdasarkan pedoman/ petunjuk teknis yang berlaku; 2.2 Mampu mendemonstrasikan kegiatan verifikasi algoritma kriptografi berdasarkan pedoman kerja/ petunjuk teknis |

| | | | |
|---|---|--|---|
| | | | yang berlaku; 2.3 Mampu menyusun laporan pelaksanaan verifikasi algoritma kriptografi. |
| 14. <i>Functional Testing</i> | 2 | Melaksanakan <i>functional testing</i> . | 2.1 Mampu menentukan tahapan yang dilakukan dalam pelaksanaan <i>functional testing</i> ; 2.2 Mampu menyusun rencana uji <i>functional testing</i> ; 2.3 Mampu menjalankan <i>functional testing</i> sesuai <i>test plan</i> dan metode yang berlaku. |
| 15. Analisis Kerawanan Produk Keamanan Siber dan Sandi Negara | 2 | Melaksanakan analisis kerawanan produk. | 2.1 Mampu menentukan tahapan yang dilakukan dalam pelaksanaan analisis kerawanan produk; 2.2 Mampu menyusun rencana uji analisis kerawanan produk; 2.3 Mampu menjalankan analisis kerawanan produk sesuai <i>test plan</i> dan metode yang berlaku. |

| III. PERSYARATAN JABATAN | | | | | |
|--------------------------|----------------|---|---------|-------|--|
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | | |
| | | Mutlak | Penting | Perlu | |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Standar Keamanan Modul Sandi | | X | |

| | | | | | |
|--|---------------------|---|---|---|---|
| | | e. Pelatihan Standar Keamanan Perangkat TI | | X | |
| | | f. Pelatihan Metode Evaluasi Keamanan Modul Sandi | | X | |
| | | g. Pelatihan Metode Evaluasi Keamanan Perangkat TI | | X | |
| | | h. Pelatihan Verifikasi Algoritma | | X | |
| | | i. Pelatihan Bahasa Pemrograman | | X | |
| | | j. Pelatihan <i>Software Testing</i> | | X | |
| | | k. Pelatihan <i>Hardware Testing</i> | | X | |
| | | l. Pelatihan Kesehatan dan Keselamatan Kerja Laboratorium | | | X |
| | 3. Fungsional | Fungsional Sandiman Pertama | | X | |
| | C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | |

| | | | | |
|------------------------------|---|---|--|--|
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

c. Fungsi Investigasi Forensik Digital

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|--|---------------------|-----------------------|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi investigasi forensik digital dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, forensik digital, <i>data science</i> keamanan siber dan sandi negara, analisis kripto, dan investigasi siber. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Leve 1 | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, | 2.1. Mengingatn rekan |

| | | | |
|--------------|---|---|--|
| | | mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | <p>kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.2. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.3. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota</p> |

| | | | |
|-------------------------|---|--|--|
| | | | <p>dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | <p>Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll.</p> | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan, dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | <p>Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja.</p> | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba</p> |

| | | | |
|---------------------|---|--|--|
| | | | <p>metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya.</p> |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyalia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyalia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | <p>tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik.</p> |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |

| | | | |
|---------------------------|---|---|---|
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | <p>2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat | 2 | Aktif mengembangkan | 2.1. Menampilkan sikap |

| | | | |
|--|---|--|--|
| Bangsa | | sikap saling menghargai, menekankan persamaan dan persatuan. | <p>dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasikan</p> |

| | | | |
|---------------------------------------|---|--|--|
| | | | <p>aset-aset penting yang rentan terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasikan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | <p>2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi;</p> |

| | | | |
|---------------------|---|-----------------------------------|---|
| | | | <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12.Forensik Digital | 2 | Menyelidiki sumber bukti digital. | <p>2.1 Mampu menentukan sumber data (sumber bukti digital, <i>log file</i>, dan informasi lainnya) yang potensial terkait keamanan siber;</p> <p>2.2 Mampu melakukan preservasi sumber bukti digital;</p> <p>2.3 Mampu menggunakan <i>tools</i></p> |

| | | | |
|---|---|--|--|
| | | | forensik digital; 2.4 Mampu menentukan metode-metode forensik digital. |
| 13. <i>Data Science</i> Keamanan Siber dan Sandi Negara | 2 | Menerapkan pengumpulan dan pemetaan serta metode <i>data science</i> . | 2.1 Mampu melakukan pengumpulan <i>data science</i> ; 2.2 Mampu melakukan pemetaan <i>data science</i> ; 2.3 Mampu menerapkan metode <i>data science</i> ; |
| 14. Analisis Kripto | 2 | Menerapkan Analisis Kripto. | 2.1 Mampu menggunakan <i>tools</i> Analisis Kripto; 2.2 Mampu menerapkan prosedur/petunjuk pelaksanaan analisis kripto; 2.3 Mampu memperoleh profil target Analisis Kripto; 2.4 Mampu memecahkan kode (<i>code breaking</i>). |
| 15. Investigasi Siber | 2 | Melakukan investigasi siber. | 2.1 Mampu mengklasifikasi kan temuan investigasi siber; 2.2 Mampu menentukan sumber daya pelaksanaan investigasi siber; 2.3 Mampu menerapkan |

| | | | metodologi investigasi siber. | | |
|--------------------------|----------------|---|-------------------------------------|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Kemanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Computer Forensic Analysis</i> | | X | |
| | | e. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| | | | | | |

| | | | | |
|---------------------|---|-----------------------------|---|---|
| | f. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| | g. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| | h. Pelatihan <i>Anti-Forensic Analysis</i> | | X | |
| | i. Pelatihan <i>Media Digital Forensic Analysis</i> | | X | |
| | j. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| | k. Pelatihan <i>Cryptocurrency Forensic Analysis</i> | | X | |
| | l. Pelatihan <i>IoT Forensic Analysis</i> | | X | |
| | m. Pelatihan <i>Reverse-Engineering Malware</i> | | X | |
| | n. Pelatihan <i>Cloud Forensic Analysis</i> | | X | |
| | o. Pelatihan <i>Investigasi Siber</i> | | X | |
| | p. Pelatihan <i>Cyber Law Data Security and Investigation</i> | | X | |
| | q. Pelatihan <i>Incident Handling</i> | | X | |
| | r. Pelatihan <i>Threat Intelligence</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Pertama | | X |
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | |
| | b. Memiliki pengalaman di | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

d. Fungsi Penanggulangan dan Pemulihan

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|---|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi penanggulangan dan pemulihan dengan melakukan Manajemen Keamanan Siber dan Persandian, Advokasi Kebijakan Keamanan Siber, pengelolaan CSIRT, manajemen insiden siber, manajemen krisis siber, dan forensik digital. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Leve 1 | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam |

| | | | |
|--------------|---|--|---|
| | | | <p>segala situasi dan kondisi; Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.2. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.3. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi</p> |

| | | | |
|-------------------------|---|---|--|
| | | | untuk menyelesaikan tugas tim. |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan, dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh</p> |

| | | | |
|---------------------|---|---|--|
| | | | kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tata cara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | <p>2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi</p> |

| | | | |
|---------------------------|---|--|--|
| | | | perubahan; 2.3. Cepat dan tanggap dalam menerima perubahan. |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | 2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi; 2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan; 2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | 2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan; 2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan; 2.3. Bersikap tenang, |

| | | | |
|--|---|--|--|
| | | | mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, gender, sosial ekonomi, preferensi politik di lingkungan unit kerjanya. |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasi-kan aset-aset penting yang rentan terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasi-kan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi.</p> |

| | | | |
|--|---|--|---|
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan siber. | <p>2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan siber, penyelenggaraan keamanan siber, penatakelolaan aplikasi keamanan siber, dan/atau pengelolaan keamanan siber;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan siber;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi</p> |
|--|---|--|---|

| | | | |
|-----------------------------|---|---|---|
| | | | penerapan kebijakan keamanan siber. |
| 12. Pengelolaan CSIRT | 2 | Mampu melaksanakan pengelolaan CSIRT sesuai prosedur. | <p>2.1 Mampu menerapkan prosedur untuk melakukan asistensi CSIRT;</p> <p>2.2 Mampu menerapkan prosedur pada kegiatan yang terkait pembangunan kapabilitas CSIRT untuk melakukan penanganan insiden keamanan siber, sesuai prosedur;</p> <p>2.3 Mampu menentukan sumber data yang diperlukan dalam penilaian kesiapan CSIRT dalam melakukan penanganan insiden keamanan siber;</p> <p>2.4 Mampu menentukan sumber data yang diperlukan dalam penilaian kematangan CSIRT.</p> |
| 13. Manajemen Insiden Siber | 2 | Mampu melaksanakan Manajemen Insiden Siber sesuai pedoman kerja/ petunjuk teknis. | <p>2.1 Mampu melaksanakan proses manajemen insiden sesuai prosedur yang ditetapkan;</p> <p>2.2 Mampu menggunakan alat, metode, dan teknik</p> |

| | | | |
|----------------------------|---|--|--|
| | | | <p>untuk melakukan manajemen insiden siber;</p> <p>2.3 Mampu mengidentifikasi permasalahan dasar terkait manajemen insiden siber;</p> <p>2.4 Mampu mengumpulkan laporan <i>information security events</i> dari konstituen/<i>vendor/team IRT</i> lain dan sensor;</p> <p>2.5 Mampu mendemonstrasikan prosedur dan teknik pengelolaan.</p> |
| 14. Manajemen Krisis Siber | 2 | Mampu melaksanakan Manajemen Krisis Siber sesuai pedoman kerja/ petunjuk teknis. | <p>2.1 Mampu melaksanakan pemberian peringatan/ deteksi dari insiden yang tidak biasa;</p> <p>2.2 Mampu mengklasifikasi-kan informasi yang relevan terkait kondisi krisis siber;</p> <p>2.3 Mampu melaksanakan peningkatan pertahanan aset vital.</p> |
| 15. Forensik Digital | 2 | Menyelidiki sumber bukti digital. | 2.1 Mampu menentukan sumber |

| | | | data (sumber bukti digital, <i>log file</i> , dan informasi lainnya) yang potensial terkait keamanan siber; 2.2 Mampu melakukan preservasi sumber bukti digital; 2.3 Mampu menggunakan tools forensik digital; 2.4 Mampu menentukan metode-metode forensik digital. | | |
|---------------------------------|----------------|---|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | | X |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | | X |

| | | | | |
|--|--|-----------------------------|---|---|
| | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | | X |
| | c. Pelatihan Kebijakan Keamanan Siber | | | X |
| | d. Pelatihan Audit Keamanan Siber | | | X |
| | e. Pelatihan CEH | | | X |
| | f. Pelatihan <i>Management CSIRT</i> | | | X |
| | g. Pelatihan Manajemen Insiden Siber | | X | |
| | h. Pelatihan <i>Incident Handling</i> | | X | |
| | i. Pelatihan <i>Log Analysis</i> | | X | |
| | j. Pelatihan <i>Network Security</i> | | | X |
| | k. Pelatihan <i>Artifak Handling</i> | | X | |
| | l. Pelatihan <i>Malware Forensic Analysis</i> | | | X |
| | m. Pelatihan <i>Computer Forensic Analysis</i> | | | X |
| | n. Pelatihan <i>Digital Storage Forensic Analysis</i> | | | X |
| | o. Pelatihan <i>Network Forensic Analysis</i> | | | X |
| | p. Pelatihan DFIR (<i>Digital Forensic for Incident Responder</i>) | | | X |
| | 3. Fungsional | Fungsional Sandiman Pertama | | X |

| | | | | |
|------------------------------|---|---|--|--|
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | |
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

e. Fungsi Identifikasi dan Deteksi

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|--|-----------|----------------------|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi identifikasi dan deteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, intelijen siber, penilaian keamanan TI dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu | 2.1. Mengingat rekan |

| | | | |
|--------------|---|---|---|
| | | mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | <p>kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.2. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.3. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok</p> |

| | | | |
|-------------------------|---|---|---|
| | | | <p>kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | <p>Aktif menjalankan komunikasi secara formal dan informal;</p> <p>Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll.</p> | <p>2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif, menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.3. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dll sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | <p>Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja.</p> | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil</p> |

| | | | |
|---------------------|---|--|---|
| | | | kerjanya; 2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | 2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil; 2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap; 2.3. Mampu mengenali dan memanfaatkan kebiasaan, tata cara, |

| | | | |
|-------------------------------------|---|---|--|
| | | | situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan |

| | | | |
|---------------------------|---|--|---|
| | | | <p>yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar</p> |

| | | | |
|---|---|--|--|
| | | | <p>individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasikan aset-aset penting yang rentang terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasikan risiko keamanan informasi;</p> |

| | | | |
|---------------------------------------|---|--|--|
| | | | 2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi. |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi; 2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi |

| | | | |
|------------------------------------|---|--|--|
| | | | kebijakan keamanan informasi; 2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi. |
| 12.Manajemen Risiko Keamanan Siber | 2 | Mampu mengaplikasikan manajemen risiko keamanan informasi. | 2.1 Mampu mengklasifikasikan aset yang terkait keamanan informasi; 2.2 Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan; 2.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan. |
| 13.Penilaian Keamanan TI | 2 | Mampu menerapkan teknik, metode, tata cara, dan prosedur dalam melakukan pengujian keamanan teknologi informasi. | 2.1 Mampu menentukan teknik, dan metode dalam melakukan pengujian keamanan teknologi informasi; 2.2 Mampu mengoperasikan perangkat pengujian keamanan teknologi informasi; 2.3 Mampu |

| | | | |
|--------------------------------|---|---|---|
| | | | <p>mengilustrasikan hasil pengumpulan aktivitas <i>malware</i> pada perangkat teknologi keamanan informasi;</p> <p>2.4 Mampu mendemonstrasikan pengujian keamanan teknologi informasi;</p> <p>2.5 Mampu menemukan celah keamanan pada teknologi informasi.</p> |
| 14. Intelijen Siber | 2 | Mampu menerapkan konsep dasar, teknik, metode, tata cara, dan prosedur dalam melakukan intelijen siber. | <p>2.1 Mampu menentukan teknik, dan metode pengumpulan informasi intelijen yang dibutuhkan;</p> <p>2.2 Mampu menentukan teknik, dan metode pengolahan informasi intelijen yang dibutuhkan;</p> <p>2.3 Mampu mengoperasikan perangkat pengumpulan dan pengolahan informasi intelijen;</p> <p>2.4 Mampu mengilustrasikan hasil pengumpulan informasi intelijen.</p> |
| 15. <i>Monitoring</i> Keamanan | 2 | Mampu menerapkan <i>monitoring</i> keamanan | 2.1 Mampu menggunakan teknik dan |

| | | | | | |
|---------------------------------|----------------|---|---|---------|-------|
| Jaringan | | jaringan. | metode dalam mengumpulkan aktivitas data dalam jaringan; 2.2 Mampu mengoperasikan perangkat <i>monitoring</i> keamanan jaringan; 2.3 Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan; 2.4 Mampu mendemonstrasikan <i>monitoring</i> lalu lintas jaringan. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |

| | | | | |
|-----------|--|--|---|--|
| 2. Teknis | d. Pelatihan Teknik Komunikasi | | X | |
| | a. Pelatihan Manajemen Risiko Siber | | X | |
| | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | d. Pelatihan <i>Penetration Testing</i> | | X | |
| | e. Pelatihan <i>Vulnerability Assessment</i> | | X | |
| | f. Pelatihan <i>Secure Software Development</i> | | X | |
| | g. Pelatihan Audit Keamanan Informasi | | X | |
| | h. Pelatihan Arsitektur Keamanan Sistem | | X | |
| | i. Pelatihan <i>Global Industrial Security/SCADA</i> | | X | |
| | j. Pelatihan Keamanan | | X | |

| | | | | |
|------------------------------|---|-----------------------------|---|---|
| | Jaringan | | | |
| | k. Pelatihan Investigasi Intelijen Siber | | X | |
| | l. Pelatihan <i>Cyber Threat Intelligence</i> | | X | |
| | m. Pelatihan <i>Analysis Malware</i> | | X | |
| | n. Pelatihan Kontra Penginderaan | | X | |
| | o. Pelatihan <i>System Security</i> | | X | |
| | p. Pelatihan <i>Cyberwarfare</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Pertama | | X |
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | |
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

f. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI PERTAMA | | | |
|--|--|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi kendali operasi keamanan siber dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan <i>security operation center</i> (SOC), pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Leve 1 | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 2.2. Mengajak orang lain untuk bertindak sesuai etika dan kode etik; 2.3. Menerapkan norma-norma secara |

| | | | |
|---------------|---|--|--|
| | | | <p>konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.4. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim.</p> |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal | 2.1. Menggunakan gaya komunikasi informal |

| | | | |
|-------------------------|---|---|---|
| | | <p>dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dan lain-lain.</p> | <p>untuk meningkatkan hubungan profesional;</p> <p>2.2. Mendengarkan pihak lain secara aktif;</p> <p>2.3. Menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai;</p> <p>2.4. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dan lain-lain sesuai arahan pimpinan.</p> |
| 4. Orientasi pada hasil | 2 | <p>Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja.</p> | <p>2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi;</p> <p>2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya;</p> <p>2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode</p> |

| | | | |
|---------------------|---|--|--|
| | | | kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa |

| | | | |
|---------------------------|---|---|---|
| | | | <p>arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima perubahan.</p> |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | <p>2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan, dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik</p> |

| | | | |
|---|---|---|--|
| | | | <p>antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik di lingkungan unit kerjanya.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam perumusan kebijakan manajemen keamanan siber dan persandian dan menerapkan kontrol keamanan siber dan persandian. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>2.2 Mampu mengklasifikasi kan aset-aset penting yang rentan terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasi kan risiko keamanan</p> |

| | | | |
|--|---|--|---|
| | | | siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu melakukan advokasi kebijakan keamanan siber. | <p>2.1 Mampu menyusun rencana pelaksanaan kegiatan advokasi kebijakan;</p> <p>2.2 Mampu membuat alat bantu untuk kebutuhan advokasi, melakukan sosialisasi kebijakan dengan audiensi lingkup kecil;</p> <p>2.3 Mampu mengidentifikasi posisi dasar dan kebutuhan pemangku kepentingan terkait advokasi kebijakan.</p> |
| 12. Pengelolaan <i>Security Operation Center (SOC)</i> | 2 | Menerapkan pengelolaan SOC. | <p>2.1 Mampu melaksanakan pengelolaan SOC sesuai prosedur;</p> <p>2.2 Mampu melatih <i>stakeholder</i> untuk dapat mengelola SOC;</p> <p>2.3 Mampu menentukan spesifikasi dukungan teknis operasional SOC;</p> <p>2.4 Mampu</p> |

| | | | |
|----------------------------|---|--|---|
| | | | <p>mengklasifikasikan dukungan teknis operasional SOC;</p> <p>2.5 Mampu menggunakan instrumen penilaian maturitas SOC.</p> |
| 13.Manajemen Insiden Siber | 2 | Mampu melaksanakan manajemen insiden siber sesuai pedoman kerja/ petunjuk teknis | <p>2.1 Mampu melaksanakan proses manajemen insiden sesuai prosedur yang ditetapkan;</p> <p>2.2 Mampu menggunakan alat, metode, dan teknik untuk melakukan manajemen insiden siber;</p> <p>2.3 Mampu mengidentifikasi permasalahan dasar terkait manajemen insiden siber;</p> <p>2.4 Mampu menggambarkan prosedur manajemen insiden siber dalam bentuk SOP sederhana dan jadwal kerja;</p> <p>2.5 Mampu mendemonstrasikan prosedur dan teknik pengelolaan.</p> |
| 14.Pengelolaan | 2 | Menerapkan konsep | 2.1 Mampu |

| | | | |
|--|---------------|--|---|
| <p>Pusat Kontak Siber Nasional</p> | | <p>pengelolaan pusat kontak siber.</p> | <p>menggunakan instrumen pengelolaan pusat kontak siber; 2.2 Mampu melengkapi bukti aduan dan identitas pelapor aduan siber; 2.3 Mampu menentukan aduan siber terverifikasi dan tidak terverifikasi.</p> |
| <p>15. <i>Monitoring</i> Keamanan Jaringan</p> | <p>2</p> | <p>Mampu menerapkan <i>monitoring</i> keamanan jaringan.</p> | <p>2.1. Mampu menggunakan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan; 2.2. Mampu mengoperasikan perangkat <i>monitoring</i> keamanan jaringan; 2.3. Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan; 2.4. Mampu mendemonstrasikan <i>monitoring</i> lalu lintas jaringan.</p> |
| <p>III. PERSYARATAN JABATAN</p> | | | |
| <p>Jenis Persyaratan</p> | <p>Uraian</p> | <p>Tingkat pentingnya</p> | |

| | | terhadap jabatan | | | |
|--|----------------|---|---------|-------|---|
| | | Mutlak | Penting | Perlu | |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan manajemen risiko siber | | X | |
| | | b. Pelatihan manajemen keamanan siber dan persandian | | X | |
| | | c. Pelatihan kebijakan keamanan siber | | X | |
| | | d. Pelatihan <i>security operation center</i> | | X | |
| | | e. Pelatihan <i>cyber threat intelligence</i> | | | X |
| | | f. Pelatihan <i>cyber defense operation</i> | | | X |
| | | g. Pelatihan manajemen insiden | | X | |
| | | h. Pelatihan penanganan insiden (<i>Incident Handling</i>) | | | X |
| | | i. Pelatihan investigasi siber | | X | |
| j. Pelatihan perangkat keamanan jaringan | | X | | | |

| | | | | | |
|------------------------------|---------------|---|---|---|--|
| | 3. Fungsional | Fungsional Sandiman Pertama | | X | |
| C. Pengalaman Kerja | | a. Lulus Diklat Dasar | X | | |
| | | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | |
| D. Pangkat | | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

g. Fungsi Pengkajian

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|---|-----------|----------------------|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan teknologi informasi, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |

| | | | |
|---------------|---|---|--|
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | <p>2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>2.2. Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.3. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.4. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Membantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim; mempertimbangkan masukan dan keahlian anggota dalam tim/kelompok kerja</p> |

| | | | |
|-------------------------|---|---|--|
| | | | serta bersedia untuk belajar dari orang lain; 2.3. Membangun komitmen yang tinggi untuk menyelesaikan tugas tim. |
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | 2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional; 2.2. Mendengarkan pihak lain secara aktif; menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai; 2.3. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan dll sesuai arahan pimpinan. |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | 2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi; 2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya; 2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk |

| | | | |
|---------------------|---|--|--|
| | | | mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan publik | 2 | Mampu mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan. | <p>2.1. Menunjukkan sikap yakin dalam mengerjakan tugas-tugas pemerintahan/pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik. |
| 6. Pengembangan diri dan orang lain | 2 | Meningkatkan kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | <p>2.1. Meningkatkan kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan;</p> <p>2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru;</p> <p>2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan.</p> |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | <p>2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain;</p> <p>2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan;</p> <p>2.3. Cepat dan tanggap dalam menerima</p> |

| | | | |
|---------------------------|---|--|--|
| | | | perubahan. |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | 2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam upaya mencari solusi; 2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan; 2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | 2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan; 2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan; 2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam |

| | | | |
|---|---|--|---|
| | | | menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik di lingkungan unit kerjanya. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam Perumusan Kebijakan Manajemen Keamanan Siber dan Persandian dan menerapkan kontrol keamanan informasi. | 2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian; 2.2 Mampu mengklasifikasikan aset-aset penting yang rentang terhadap ancaman; 2.3 Mampu mengkalkulasikan risiko keamanan informasi; 2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan | 2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, |

| | | | |
|--------------------------|---|---|---|
| | | evaluasi kebijakan keamanan informasi. | <p>informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/ atau pengelolaan keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12. Rekayasa Kriptografi | 2 | Menerapkan pedoman kerja/ petunjuk teknis | 2.1 Mampu mengoperasikan |

| | | | |
|---|---|---|---|
| | | dalam melaksanakan perancangan desain rekayasa kriptografi. | <p>prosedur penyalinan/ pencadangan data hasil rekayasa kriptografi;</p> <p>2.2 Mampu menerapkan prosedur kerja atau petunjuk teknis perancangan desain rekayasa kriptografi;</p> <p>2.3 Mampu menerapkan simulasi rekayasa kriptografi.</p> |
| 13. Rancang Bangun Perangkat Keamanan Teknologi Informasi | 2 | Menerapkan pedoman kerja/petunjuk teknis dalam melaksanakan perancangan desain perangkat keamanan TI. | <p>2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil Pengkajian Teknologi keamanan siber dan sandi;</p> <p>2.2 Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi;</p> <p>2.3 Mampu menerapkan desain perangkat keamanan TI pada suatu <i>framework</i> tertentu.</p> |
| 14. Pengkajian Teknologi Keamanan Siber dan Sandi | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan Pengkajian Teknologi keamanan siber dan sandi. | <p>2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil Pengkajian Teknologi keamanan siber dan sandi;</p> |

| | | | 2.2 Mampu menggali celah keamanan dalam suatu teknologi informasi; | | |
|--|----------------|---|---|---------|-------|
| | | | 2.3 Mampu menerapkan konsep dan teori terkait pengkajian teknologi keamanan siber dan sandi. | | |
| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 2 | Menerapkan pedoman kerja/ petunjuk teknis dalam melaksanakan penelitian | 2.1 Mampu mengoperasikan prosedur penyalinan/ pencadangan data hasil rekayasa kriptografi; 2.2 Mampu menerapkan prosedur kerja atau petunjuk teknis tahapan proses penelitian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan | | X | |

| | | | | |
|-----------|--|--|---|--|
| 2. Teknis | Budaya Integritas dan Anti Korupsi | | | |
| | d. Pelatihan Teknik Komunikasi | | X | |
| | a. Pelatihan Manajemen Risiko Siber | | X | |
| | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | d. Pelatihan Kriptografi Simetrik | | X | |
| | e. Pelatihan Kriptografi Asimetrik | | X | |
| | f. Pelatihan Fungsi Hash | | X | |
| | g. Pelatihan Pembangkit Bilangan Acak | | X | |
| | h. Pelatihan Infrastruktur Kunci Publik | | X | |
| | i. Pelatihan Protokol Kriptografi | | X | |
| | j. Pelatihan Bahasa | | X | |

| | | | | | | |
|--|---------------------|--|------------------------------------|---|---|--|
| | | Pemrograman | | | | |
| | | k. Pelatihan Steganografi | | X | | |
| | | l. Pelatihan <i>Embedded System</i> | | X | | |
| | | m. Pelatihan Perancangan Piranti Lunak | | X | | |
| | | n. Pelatihan Perancangan Piranti Keras | | X | | |
| | | o. Pelatihan <i>Software Testing</i> | | X | | |
| | | p. Pelatihan <i>Hardware Testing</i> | | X | | |
| | | q. Pelatihan Keamanan Jaringan | | X | | |
| | | r. Pelatihan Pengelolaan Kunci | | X | | |
| | | 3. Fungsional | Diklat Fungsional Sandiman Pertama | | X | |
| | C. Pengalaman Kerja | | a. Lulus Diklat Dasar | X | | |
| | | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan | X | | | |

| | | | | |
|------------------------------|---|--|--|--|
| | persandian paling sedikit 2 (dua) tahun. | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | |

h. Fungsi Proteksi

| | | |
|-------------------|---|-----------------------|
| Nama Jabatan | : | Sandiman Ahli Pertama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI PERTAMA | | | |
|---|---|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran operasional dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 2 | Mampu mengingatkan, mengajak rekan kerja untuk bertindak sesuai nilai, norma, dan etika organisasi. | 2.1. Mengingatkan rekan kerja untuk bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; |

| | | | |
|--------------|---|--|--|
| | | | <p>2.2. Mengajak orang lain untuk bertindak sesuai etika dan kode etik;</p> <p>2.3. Menerapkan norma-norma secara konsisten dalam setiap situasi, pada unit kerja terkecil/ kelompok kerjanya;</p> <p>2.4. Memberikan informasi yang dapat dipercaya sesuai dengan etika organisasi.</p> |
| 2. Kerjasama | 2 | Menumbuhkan tim kerja yang partisipatif dan efektif. | <p>2.1. Memmbantu orang lain dalam menyelesaikan tugas-tugas dalam menyelesaikan mereka untuk mendukung sasaran tim;</p> <p>2.2. Berbagi informasi yang relevan atau bermanfaat pada anggota tim;</p> <p>2.3. Mempertimbangkan masukan dan keahlian anggota dalam tim/ kelompok kerja serta bersedia untuk belajar dari orang lain;</p> <p>2.4. Membangun komitmen yang tinggi untuk menyelesaikan</p> |

| | | | tugas tim. |
|-------------------------|---|---|---|
| 3. Komunikasi | 2 | Aktif menjalankan komunikasi secara formal dan informal; Bersedia mendengarkan orang lain, menginterpretasikan pesan dengan respon yang sesuai, mampu menyusun materi presentasi, pidato, naskah, laporan, dll. | 2.1. Menggunakan gaya komunikasi informal untuk meningkatkan hubungan profesional; 2.2. Mendengarkan pihak lain secara aktif; menangkap dan menginterpretasikan pesan-pesan dari orang lain, serta memberikan respon yang sesuai; 2.3. Membuat materi presentasi, pidato, <i>draft</i> naskah, laporan, dll sesuai arahan pimpinan. |
| 4. Orientasi pada hasil | 2 | Berupaya meningkatkan hasil kerja pribadi yang lebih tinggi dari standar yang ditetapkan, mencari, mencoba metode alternatif untuk peningkatan kinerja. | 2.1. Menetapkan dan berupaya mencapai standar kerja pribadi yang lebih tinggi dari standar kerja yang ditetapkan organisasi; 2.2. Mencari, mencoba metode kerja alternatif untuk meningkatkan hasil kerjanya; 2.3. Memberi contoh kepada orang-orang di unit kerjanya untuk mencoba menerapkan metode kerja yang lebih efektif yang sudah dilakukannya. |
| 5. Pelayanan | 2 | Mampu | 2.1. Menunjukkan sikap |

| | | | |
|---------------|---|---|--|
| publik | | <p>mensupervisi/ mengawasi/ menyelia dan menjelaskan proses pelaksanaan tugas-tugas pemerintahan/ pelayanan publik secara transparan.</p> | <p>yakin dalam mengerjakan tugas- tugas pemerintahan/ pelayanan publik, mampu menyelia dan menjelaskan secara objektif bila ada yang mempertanyakan kebijakan yang diambil;</p> <p>2.2. Secara aktif mencari informasi untuk mengenali kebutuhan pemangku kepentingan agar dapat menjalankan pelaksanaan tugas pemerintahan, pembangunan dan pelayanan publik secara cepat dan tanggap;</p> <p>2.3. Mampu mengenali dan memanfaatkan kebiasaan, tatacara, situasi tertentu sehingga apa yang disampaikan menjadi perhatian pemangku kepentingan dalam hal penyelesaian tugas-tugas pemerintahan, pembangunan dan pelayanan publik.</p> |
| 6. Pengembang | 2 | Meningkatkan | 2.1. Meningkatkan |

| | | | |
|--------------------------|---|--|---|
| n diri dan orang lain | | kemampuan bawahan dengan memberikan contoh dan penjelasan cara melaksanakan suatu pekerjaan. | kemampuan bawahan dengan memberikan contoh, instruksi, penjelasan dan petunjuk praktis yang jelas kepada bawahan dalam menyelesaikan suatu pekerjaan; 2.2. Membantu bawahan untuk mempelajari proses, program atau sistem baru; 2.3. Menggunakan metode lain untuk meyakinkan bahwa orang lain telah memahami penjelasan atau pengarahan. |
| 7. Mengelola perubahan | 2 | Proaktif beradaptasi mengikuti perubahan. | 2.1. Menyesuaikan cara kerja lama dengan menerapkan metode/ proses baru selaras dengan ketentuan yang berlaku tanpa arahan orang lain; 2.2. Mengembangkan kemampuan diri untuk menghadapi perubahan; 2.3. Cepat dan tanggap dalam menerima perubahan. |
| 8. Pengambilan keputusan | 2 | Menganalisis masalah secara mendalam. | 2.1. Melakukan analisis secara mendalam terhadap informasi yang tersedia dalam |

| | | | |
|---------------------------|---|--|--|
| | | | <p>upaya mencari solusi;</p> <p>2.2. Mempertimbangkan berbagai alternatif yang ada sebelum membuat keputusan;</p> <p>2.3. Membuat keputusan operasional berdasarkan kesimpulan dari berbagai sumber informasi yang sesuai dengan pedoman yang ada.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 2 | Aktif mengembangkan sikap saling menghargai, menekankan persamaan dan persatuan. | <p>2.1. Menampilkan sikap dan perilaku yang peduli akan nilai-nilai keberagaman dan menghargai perbedaan;</p> <p>2.2. Membangun hubungan baik antar individu dalam organisasi, mitra kerja, pemangku kepentingan;</p> <p>2.3. Bersikap tenang, mampu mengendalikan emosi, kemarahan dan frustrasi dalam menghadapi pertentangan yang ditimbulkan oleh perbedaan latar belakang, agama/</p> |

| | | | |
|---|---|--|--|
| | | | kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik di lingkungan unit kerjanya. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 2 | Menyediakan data dukung dalam Perumusan Kebijakan Manajemen Keamanan Siber dan Persandian dan menerapkan kontrol keamanan informasi. | <p>2.1 Mampu memperoleh data dukung dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian;</p> <p>2.2 Mampu mengklasifikasikan aset-aset penting yang rentang terhadap ancaman;</p> <p>2.3 Mampu mengkalkulasikan risiko keamanan informasi;</p> <p>2.4 Mampu mengoperasikan prosedur teknis penerapan kontrol keamanan informasi</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 2 | Mampu menyiapkan bahan perumusan kebijakan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 2.1 Mampu mengidentifikasi, mengumpulkan, mengolah dan menyiapkan data, informasi dan bahan-bahan, yang dibutuhkan untuk perumusan kebijakan dalam pengelolaan |

| | | | |
|------------------------------------|---|--|---|
| | | | <p>sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi;</p> <p>2.2 Mampu menyusun <i>draft</i> awal program implementasi kebijakan dengan memahami konten dan konteks kebijakan dan menjabarkan dalam program implementasi kebijakan keamanan informasi;</p> <p>2.3 Mampu menyiapkan bahan dan instrumen untuk melakukan <i>monitoring</i> dan evaluasi penerapan kebijakan keamanan informasi.</p> |
| 12.Manajemen Risiko Keamanan Siber | 2 | Mampu mengaplikasikan manajemen risiko keamanan informasi. | <p>2.1 Mampu mengklasifikasikan aset yang terkait keamanan informasi;</p> <p>2.2 Mampu menerapkan manajemen risiko sesuai standar atau</p> |

| | | | |
|---|---|---|---|
| | | | kebijakan yang ditentukan; 2.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan. |
| 13.Audit Keamanan Informasi | 2 | Menerapkan konsep audit keamanan informasi, keamanan siber dan persandian. | 2.1 Mampu menentukan standar, prosedur dan kriteria audit keamanan informasi, keamanan siber dan persandian; 2.2 Mampu menggunakan instrumen audit keamanan informasi, keamanan siber dan persandian; 2.3 Mampu menentukan data yang diperlukan untuk kegiatan audit keamanan informasi, keamanan siber dan persandian. |
| 14.Penyediaan Layanan Keamanan Informasi | 2 | Menyelenggarakan penyediaan layanan keamanan informasi sesuai dengan prosedur/ petunjuk teknis. | 2.1 Mampu menentukan kebutuhan pengguna dan kecukupan sumber daya yang dialokasikan oleh organisasi untuk melaksanakan penyediaan layanan keamanan informasi; 2.2 Mampu |

| | | | | | |
|---|------------|---|---|---------|-------|
| | | | <p>melaksanakan layanan keamanan informasi berdasarkan norma, standar, prosedur, dan kriteria yang berlaku;</p> <p>2.3 Mampu menangani permasalahan teknis saat penyelenggaraan layanan keamanan informasi.</p> | | |
| 15. <i>Monitoring</i> Keamanan Jaringan | 2 | Mampu menerapkan <i>monitoring</i> keamanan jaringan. | <p>2.1 Mampu menggunakan teknik dan metode dalam mengumpulkan aktivitas data dalam jaringan;</p> <p>2.2 Mampu mengoperasikan perangkat <i>monitoring</i> keamanan jaringan;</p> <p>2.3 Mampu mengilustrasikan hasil pengumpulan aktivitas data dalam jaringan;</p> <p>2.4 Mampu mendemonstrasikan <i>monitoring</i> lalu lintas jaringan.</p> | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |

| | | | | | |
|--------------|----------------|---|--|---|--|
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Secure Software Development</i> | | X | |
| | | e. Pelatihan Audit Keamanan Informasi | | X | |
| | | f. Pelatihan Arsitektur Keamanan Sistem | | X | |
| | | g. Pelatihan <i>Global Industrial</i> | | X | |

| | | | | | |
|------------------------------|---|--|--|---|--|
| | | <i>Security/SCADA</i> | | | |
| | | h. Pelatihan Keamanan Jaringan | | X | |
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | | j. Pelatihan Keamanan Sistim Informasi | | X | |
| | | k. Pelatihan Peralatan Keamanan Siber dan Persandian | | X | |
| | | l. Pelatihan Diplomasi Siber | | X | |
| | 3. Fungsional | Fungsional Sandiman Pertama | | X | |
| C. Pengalaman Kerja | a. Lulus Diklat Dasar | X | | | |
| | b. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | | |
| D. Pangkat | III/a (Penata Muda) III/b (Penata Muda Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil implementasi keamanan informasi, keamanan siber, dan persandian | | | | |

2. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN AHLI MUDA/ MUDA

a. Fungsi Sertifikasi Elektronik

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MUDA | | | |
|---------------------------------------|--|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi sertifikasi elektronik dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, analisis kelaikan sertifikasi elektronik, pemenuhan teknis sistem sertifikasi elektronik, pengelolaan jaringan dan infrastruktur sertifikasi elektronik. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit |

| | | | |
|---------------|---|---|---|
| | | | kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/ kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/ kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/rumit/kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/ rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap.</p> |

| | | | |
|-------------------------|---|--|---|
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | pelayanan publik di unit kerjanya. |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan; memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.5. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan | 3 | Membandingkan berbagai | 3.1. Membandingkan berbagai alternatif tindakan dan |

| | | | |
|---|---|---|--|
| keputusan | | alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | implikasinya; 3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perikat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku; 3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada; 3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber | 3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku; |

| | | | |
|---------------------------------------|---|---|---|
| | | dan persandian. | <p>3.2 Mampu menganalisis prosedur teknis penerapan kontro keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | <p>3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi;</p> <p>3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| 12. Manaje | 3 | Mampu | 3.1 mampu mengidentifikasi risiko |

| | | | |
|---|---|--|---|
| men Risiko Keamanan Siber | | melaksanakan penilaian risiko dan menganalisis penerapan manajemen risiko. | berdasarkan aset maupun proses bisnis organisasi; 3.2 mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan; 3.3 mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan. |
| 13. Analisis Kelaikan Sertifikasi Elektronik | 3 | Membimbing penerapan dan manajemen sertifikat elektronik. | 3.1 mampu mengidentifikasi teknik dan metode analisis keamanan teknologi informasi yang dibutuhkan; 3.2 mampu mengkorelasikan teknik dan metode analisis keamanan teknologi informasi; 3.3 mampu menganalisis dampak yang ditimbulkan oleh <i>malware</i> pada perangkat teknologi keamanan informasi; 3.4 mampu mendiagnosis karakteristik <i>malware</i> terhadap suatu perangkat teknologi keamanan informasi; 3.5 mampu memvalidasi hasil temuan celah keamanan teknologi informasi. |
| 14. Pemenu han Teknis Sistem Sertifikasi Elektronik | 3 | Mampu menganalisis kebutuhan pemenuhan teknis sistem sertifikasi elektronik. | 3.1 mampu menganalisis kebutuhan penerapan teknologi sertifikat elektronik; 3.2 mampu mengidentifikasi proses bisnis sistem <i>stakeholder</i> dalam rangka implementasi sertifikat elektronik; 3.3 mampu menganalisis kebutuhan desain dan perencanaan teknis |

| | | | <p>penerapan sertifikat elektronik pada <i>stakeholder</i>.</p> <p>3.4 mampu menguji hasil penerapan modul-modul sertifikasi elektronik pada aplikasi pengguna;</p> | | |
|---|----------------|---|---|---------|-------|
| 15. Pengelolaan Jaringan dan Infrastruktur Sertifikasi Elektronik | 3 | Mengelola sistem penyelenggaraan sertifikasi elektronik. | <p>3.1 mampu mengelola hak akses pengelola/<i>administrator</i> sistem sertifikasi elektronik dalam pembuatan, pemeliharaan dan pencabutan hak akses;</p> <p>3.2 mampu mengelola perangkat dan infrastruktur pengelolaan sistem sertifikasi elektronik (termasuk pemutakhiran);</p> <p>3.3 mampu mendeteksi gangguan dan permasalahan dalam operasional pengelolaan sistem sertifikasi elektronik;</p> <p>3.4 mampu mengelola risiko keamanan informasi penyelenggaraan sertifikasi elektronik;</p> <p>3.5 mampu mengoptimalkan perangkat keamanan sistem sertifikasi elektronik seperti <i>hardware security module</i> (hsm) serta <i>backup data</i> dan sistem.</p> | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |

| | | | | | |
|--------------|-------------------|--|---|---|---|
| B. Pelatihan | 1. Manajeria 1 | a. Pelatihan Pelayanan Prima | | x | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Infrastruktur Kunci Publik | X | | |
| | | b. Pelatihan <i>Public Key Infrastructure Core System</i> | | X | |
| | | c. Pelatihan Keamanan Sistem Informasi | X | | |
| | | d. Pelatihan Penyusunan Dokumen Pedoman/ Norma | | X | |
| | | e. Pelatihan <i>Software Development Life Cycle (SDLC)</i> | | X | |
| | | f. Pelatihan Pemrograman | | | X |
| | | g. Pelatihan Infrastruktur <i>Cloud</i> | | X | |
| | | h. Pelatihan Infrastruktur <i>Container</i> | | | X |
| | | i. Pelatihan Administrasi | | | X |

| | | | | | |
|------------------------------|---|-------------------------------------|---|---|---|
| | | Linux | | | |
| | | j. Pelatihan Jaringan | | | X |
| | | k. Pelatihan Aplikasi Web Server | | | X |
| | | l. Pelatihan Database | | | X |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | | X | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Pertama | | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | | |

b. Fungsi Sertifikasi dan Evaluasi Produk

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MUDA | | | |
|--|--|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi sertifikasi dan evaluasi produk dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan pengujian produk keamanan siber dan sandi negara, verifikasi algoritma kriptografi, <i>functional testing</i> , dan analisis kerawanan produk keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | <p>3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin.</p> |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-</p> |

| | | | |
|-------------------------|---|--|---|
| | | | <p>usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/ rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. membuat proposal yang rinci dan lengkap.</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja</p> |

| | | | |
|-------------------------------------|---|--|--|
| | | | unitnya. |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya.</p> |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam</p> |

| | | | |
|--------------------------|---|---|--|
| | | | <p>mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama,</p> |

| | | | |
|---|---|--|---|
| | | | <p>mengikuti prinsip kehati-hatian;</p> <p>3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | <p>Mempromosikan, mengembangkan sikap toleransi dan persatuan.</p> | <p>3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan;</p> <p>3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada;</p> <p>3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | <p>Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian.</p> | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontro keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan</p> |

| | | | |
|--|---|---|---|
| | | | manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | <p>3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi;</p> <p>3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| 12. Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara | 3 | Mengelola Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara. | <p>3.1 Mampu merancang instrumen pengujian dokumen, penyiapan sarana prasarana, dokumen serta melakukan koordinasi dalam rangka penyelenggaraan layanan sertifikasi produk;</p> <p>3.2 Mampu mensosialisasikan kebijakan, peraturan, tahapan pelaksanaan layanan pengujian</p> |

| | | | |
|--|---|---|--|
| | | | keamanan produk; 3.3 Mampu memecahkan permasalahan teknis operasional dalam penyelenggaraan layanan pengujian produk. |
| 13.Verifikasi Algoritma Kriptografi | 3 | Mengelola Verifikasi Algoritma Kriptografi. | 3.1 Mampu menganalisis hasil Verifikasi Algoritma Kriptografi; 3.2 Mampu menguji hasil Verifikasi Algoritma Kriptografi; 3.3 Mampu mendeteksi ketidaksesuaian proses Verifikasi Algoritma Kriptografi. |
| 14.Functional Testing | 3 | Mengelola <i>functional testing</i> . | 3.1 Mampu memverifikasi hasil instalasi dan/atau konfigurasi <i>software</i> atau <i>hardware</i> yang dibutuhkan untuk melakukan <i>functional testing</i> ; 3.2 Mampu menganalisis hasil <i>functional testing</i> ; 3.3 Mampu memecahkan permasalahan yang dihadapi dalam melakukan <i>functional testing</i> . |
| 15.Analisis Kerawanan Produk Keamanan Siber dan Sandi Negara | 3 | Mengelola analisis kerawanan produk. | 3.1 Mampu memverifikasi hasil instalasi dan/atau konfigurasi <i>software</i> atau <i>hardware</i> yang dibutuhkan untuk melakukan analisis kerawanan produk; 3.2 Mampu menganalisis hasil analisis kerawanan produk; 3.3 Mampu memecahkan permasalahan yang dihadapi dalam melakukan analisis kerawanan produk. |
| III. PERSYARATAN JABATAN | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya |

| | | | terhadap jabatan | | |
|---------------|----------------|---|------------------|---------|-------|
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Standar Keamanan Modul Sandi | | X | |
| | | e. Pelatihan Standar Keamanan Perangkat TI | | X | |
| | | f. Pelatihan Metode Evaluasi Keamanan Modul Sandi | | X | |

| | | | | | |
|----------------------|--|--|---|---|---|
| | | g. Pelatihan Metode Evaluasi Keamanan Perangkat TI | | X | |
| | | h. Pelatihan Verifikasi Algoritma | | X | |
| | | i. Pelatihan Bahasa Pemrograman | | X | |
| | | j. Pelatihan Kompetensi Laboratorium Pengujian ISO | | X | |
| | | k. Pelatihan Lembaga Sertifikasi Produk | | X | |
| | | l. Pelatihan Kesehatan dan Keselamatan Kerja Laboratorium | | | X |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Pertama | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja | Hasil analisis keamanan informasi, keamanan siber, | | | | |

| | |
|---------|----------------|
| Jabatan | dan persandian |
|---------|----------------|

c. Fungsi Investigasi Forensik Digital

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI MUDA | | | |
|---|---|--|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi investigasi forensik digital dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, forensik digital, <i>data science</i> keamanan siber dan sandi negara, analisis kripto, dan investigasi siber. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; |

| | | | |
|---------------|---|--|--|
| | | | 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis | 3.1. Menyampaikan suatu informasi yang sensitif/ rumit dengan cara penyampaian dan kondisi yang tepat, sehingga |

| | | | |
|-------------------------|---|--|--|
| | | untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | dapat dipahami dan diterima oleh pihak lain; 3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain; 3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks; 3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda; 3.5. Membuat proposal yang rinci dan lengkap. |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | 3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi; 3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya; 3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya. |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan | 3.1. Memahami, mendeskripsikan pengaruh dan hubungan/ kekuatan kelompok yang sedang |

| | | | |
|-------------------------------------|---|-------------------------------------|--|
| | | publik di lingkup unit kerja. | berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak; 3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya; 3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya. |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | 3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media |

| | | | |
|------------------------|---|---|--|
| | | | <p>belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan; memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.5. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif</p> |

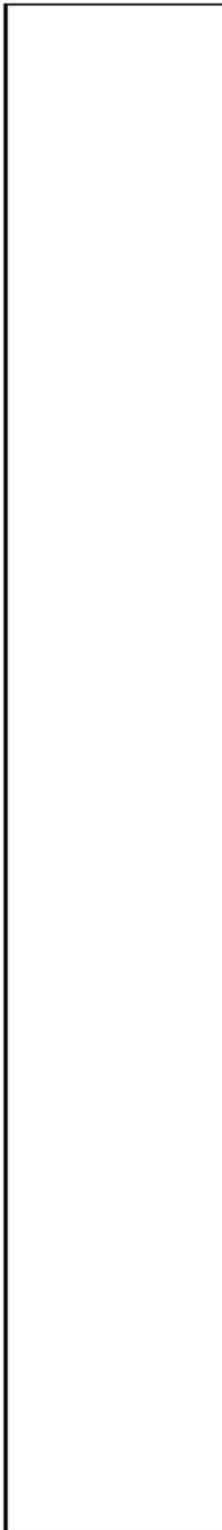
| | | | |
|---------------------------|---|---|--|
| | | | terhadap masalah yang ditimbulkan oleh adanya perubahan. |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian;</p> <p>3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya.</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | <p>3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan;</p> <p>3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalah-pahaman yang diakibatkan adanya keragaman budaya yang</p> |

| | | | |
|---|---|---|--|
| | | | ada; 3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | 3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku; 3.2 Mampu menganalisis prosedur teknis penerapan kontro keamanan informasi ke dalam format NSPK yang berlaku; 3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi | 3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah |

| | | | |
|---------------------|---|------------------------------------|--|
| | | kebijakan keamanan informasi. | kebijakan; 3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi; 3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. |
| 12.Forensik Digital | 3 | Menganalisis sumber bukti digital. | 3.1 Mampu menganalisis sumber bukti digital dan informasi lainnya dalam rangka forensik digital; 3.2 Mampu mengkorelasikan hasil analisis dengan bukti-bukti digital lainnya; 3.3 Mampu menganalisis |

| | | | |
|---|---|--|---|
| | | | norma, standar, prosedur, dan kriteria (NSPK) di bidang forensik digital. |
| 13. <i>Data Science</i> Keamanan Siber dan Sandi Negara | 3 | Menganalisis/interpretasi <i>information gathering</i> . | 3.1 Mampu menganalisis hasil pengumpulan <i>data science</i> ; 3.2 Mampu menganalisis norma, standar, prosedur, dan kriteria <i>data science</i> di bidang keamanan siber; 3.3 Mampu menganalisis metode pengumpulan <i>data science</i> di bidang keamanan siber |
| 14. Analisis Kripto | 3 | Mengevaluasi analisis kripto. | 3.1 Mampu menganalisis algoritma kriptografi target; 3.2 Mampu menganalisis profil target; 3.3 Mampu mengevaluasi metode-metode analisis kripto; |
| 15. Investigasi Siber | 3 | Menganalisis investigasi siber. | 3.1 Mampu menganalisis hasil investigasi siber; 3.2 Mampu menganalisis hasil temuan penyimpangan penyelenggaraan persandian; 3.3 Mampu menganalisis norma, standar, prosedur dan kriteria (NSPK) investigasi di bidang keamanan siber, dan/atau persandian. |

| III. PERSYARATAN JABATAN | | | | | |
|--------------------------|----------------|---|-------------------------------------|---------|-------|
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Computer Forensic</i> | | X | |



| | | | |
|---|--|---|--|
| <i>Analysis</i> | | | |
| c. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| f. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| g. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| h. Pelatihan <i>Anti-Forensic Analysis</i> | | X | |
| i. Pelatihan <i>Media Digital Forensic Analysis</i> | | X | |
| j. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| k. Pelatihan <i>Cryptocurrenc y Forensic Analysis</i> | | X | |
| l. Pelatihan <i>IoT</i> <i>Forensic Analysis</i> | | X | |
| m. Pelatihan <i>Reverse- Engineering</i> | | X | |

| | | | | | |
|---------------------|--|--|---|---|--|
| | | <i>Malware</i> | | | |
| | | n. Pelatihan <i>Cloud Forensic Analysis</i> | | X | |
| | | o. Pelatihan Investigasi Siber | | X | |
| | | p. Pelatihan <i>Cyber Law Data Security and Investigation</i> | | X | |
| | | q. Pelatihan <i>Incident Handling</i> | | X | |
| | | r. Pelatihan <i>Threat Intelligence</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | | X | | |
| | b. Telah menduduki Jabatan Sandiman | | | | |

| | | | | |
|------------------------------|---|--|--|--|
| | Ahli Pertama | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | |

d. Fungsi Penanggulangan dan Pemulihan

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI MUDA | | | |
|---|--|--|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi penanggulangan dan pemulihan dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan CSIRT, manajemen insiden siber, manajemen krisis siber, dan forensik digital. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan |

| | | | |
|---------------|---|---|--|
| | | formal. | evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/ rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks; Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda; membuat proposal yang</p> |

| | | | |
|-------------------------|---|---|--|
| | | | rinci dan lengkap; |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi, dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya. |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya</p> |

| | | | |
|---------------------------|---|---|--|
| | | | perubahan. |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | 3.1. Membandingkan berbagai alternatif tindakan dan implikasinya; 3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perikat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku; 3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada; 3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan | 3 | Menganalisis kebutuhan dalam penyelenggaraan | 3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam Manajemen |

| | | | |
|---------------------------------------|---|---|--|
| Siber dan Persandian | | manajemen keamanan siber dan persandian. | Keamanan Siber dan Persandian sesuai dengan standar yang berlaku; 3.2 Mampu menganalisis prosedur teknis penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku; 3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | 3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan; 3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi; 3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan |

| | | | |
|-----------------------------|---|--|--|
| | | | keamanan informasi. |
| 12. Pengelolaan CSIRT | 3 | Mampu menyusun bahan materi pada kegiatan pembangunan kapasitas CSIRT. | <p>3.1 Mampu membuat bahan materi pada kegiatan asistensi CSIRT;</p> <p>3.2 Mampu membuat bahan materi pada pelaksanaan kegiatan pembangunan kapabilitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber;</p> <p>3.3 Mampu menguji kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber;</p> <p>3.4 Mampu menguji kematangan CSIRT.</p> |
| 13. Manajemen Insiden Siber | 3 | Mampu menyelenggarakan Manajemen Insiden Siber. | <p>3.1 Mampu melakukan analisis terkait manajemen insiden siber;</p> <p>3.2 Mampu melaksanakan rekomendasi teknis terkait manajemen insiden siber;</p> <p>3.3 membimbing perbaikan kesalahan prosedur dalam manajemen insiden siber;</p> <p>3.4 Mampu menunjukkan perbandingan antara kedua metode pengelolaan data tersebut, setidaknya dari segi kelebihan dan kekurangan;</p> <p>3.5 mengomunikasikan hasil analisis melalui lisan dan tulisan.</p> |
| 14. Manajemen Krisis Siber | 3 | Mampu menyelenggarakan Manajemen Krisis Siber. | <p>3.1 mampu melakukan penilaian situasional untuk deklarasi kondisi krisis;</p> <p>3.2 mampu menjalankan <i>crisis management plan</i>;</p> <p>3.3 mampu melakukan simulasi</p> |

| | | | | | |
|---------------------------------|----------------|---|--|---------|-------|
| | | | krisis siber. | | |
| 15.Forensik Digital | 3 | Menganalisis sumber bukti digital. | 3.1 mampu menganalisis sumber bukti digital dan informasi lainnya dalam rangka forensik digital; 3.2 mampu mengkorelasikan hasil analisis dengan bukti-bukti digital lainnya; 3.3 mampu menganalisis norma, standar, prosedur, dan kriteria (NSPK) di bidang forensik digital. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya Terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan | | | X |

| | | | | |
|--|---|--|---|---|
| | Manajemen Keamanan Siber dan Persandian | | | |
| | c. Pelatihan Kebijakan Keamanan Siber | | | X |
| | d. Pelatihan Audit Keamanan Siber | | X | |
| | e. Pelatihan CEH | | X | |
| | f. Pelatihan <i>Management</i> CSIRT | | X | |
| | g. Pelatihan Manajemen Insiden Siber | | X | |
| | h. Pelatihan <i>Incident</i> <i>Handling</i> | | X | |
| | i. Pelatihan <i>Log</i> <i>Analysis</i> | | X | |
| | j. Pelatihan <i>Network</i> <i>Security</i> | | X | |
| | k. Pelatihan <i>Artifak Handling</i> | | X | |
| | l. Pelatihan <i>Disaster</i> <i>Recovery</i> | | | X |
| | m. Pelatihan <i>Malware</i> <i>Forensic</i> <i>Analysis</i> | | X | |
| | n. Pelatihan <i>Computer</i> <i>Forensic</i> <i>Analysis</i> | | X | |

| | | | | |
|---------------------|--|--------------------------|---|---|
| | o. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| | p. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| | q. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| | r. Pelatihan Investigasi Siber | | X | |
| | s. Pelatihan <i>Cyber Crisis Management Planning</i> | | X | |
| | t. Pelatihan DFIR (<i>Digital Forensic for Incident Responder</i>) | | X | |
| | 3. Fungsional | Fungsional Sandiman Muda | | X |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | |
| | b. Telah menduduki Jabatan | | | |

| | | | | |
|------------------------------|---|--|--|--|
| | Sandiman Ahli Pertama | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | |

e. Identifikasi dan Deteksi

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MUDA | | | |
|--|--|--|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi identifikasi dan deteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, intelijen siber, penilaian keamanan teknologi informasi dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang |

| | | | |
|---------------|---|---|---|
| | | etika organisasi, dalam lingkup formal. | dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | 3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal; 3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja; 3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok. |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, | 3.1. Menyampaikan suatu informasi yang sensitif/ |

| | | | |
|-------------------------|---|---|--|
| | | <p>terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks.</p> | <p>rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap.</p> |
| 4. Orientasi pada hasil | 3 | <p>Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja.</p> | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan | 3 | Mampu | 3.1. Memahami, |

| | | | |
|--------|--|--|--|
| publik | | memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | mendeskripsikan pengaruh dan hubungan/ kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak; 3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya; 3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas |
|--------|--|--|--|

| | | | |
|-------------------------------------|---|---|--|
| | | | <p>pelayanan publik di unit kerjanya.</p> |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> |

| | | | |
|---------------------------|---|---|--|
| | | | <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat;</p> <p>3.4. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian;</p> <p>3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya.</p> |
| B. Sosial Kultural | | | |
| 9. rekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | <p>3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan;</p> <p>3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya</p> |

| | | | |
|---|---|---|---|
| | | | <p>yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalah-pahaman yang diakibatkan adanya keragaman budaya yang ada;</p> <p>3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam Manajemen Keamanan Siber dan Persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontro keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian.</p> |
| 11. Advokasi Kebijakan | 3 | Mampu melakukan | 3.1 Mampu melakukan penilaian dan evaluasi |

| | | | |
|----------------|---|--|---|
| Keamanan Siber | | penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan. keamanan informasi. | terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan; 3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi; 3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. |
| 12. Manajemen | 3 | Mampu | 3.1 Mampu mengidentifikasi |

| | | | |
|---|---|--|---|
| Risiko Keamanan Siber | | melaksanakan penilaian risiko dan menganalisis penerapan manajemen risiko. | risiko berdasarkan aset maupun proses bisnis organisasi; 3.2 Mampu menerapkan manajemen risiko sesuai standar atau kebijakan yang ditentukan; 3.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan. |
| 13. Penilaian Keamanan Teknologi Informasi | 3 | Mampu menganalisis hasil pengujian keamanan teknologi informasi. | 3.1 Mampu mengidentifikasi teknik dan metode analisis keamanan teknologi informasi yang dibutuhkan; 3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan teknologi informasi; 3.3 Mampu menganalisis dampak yang ditimbulkan oleh <i>malware</i> pada perangkat teknologi keamanan informasi; 3.4 Mampu mendiagnosis karakteristik <i>malware</i> terhadap suatu perangkat teknologi keamanan informasi; 3.5 Mampu memvalidasi hasil temuan celah keamanan teknologi |

| | | | |
|---|---|---|--|
| | | | informasi. |
| 14. Intelijen Siber | 3 | Mampu melakukan analisis informasi intelijen siber. | <p>3.1 Mampu mengidentifikasi teknik dan metode analisis informasi intelijen siber yang dibutuhkan;</p> <p>3.2 Mampu mengkorelasikan teknik dan metode analisis informasi intelijen siber;</p> <p>3.3 Mampu memberikan bimbingan teknis, dan asistensi dalam melakukan analisis informasi intelijen siber;</p> <p>3.4 Mampu mengidentifikasi karakteristik dari target <i>monitoring</i>;</p> <p>3.5 Mampu menyimpulkan pola, metode, teknik ancaman keamanan informasi, keamanan siber, dan persandian.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 3 | Mampu melakukan analisis keamanan jaringan. | <p>3.1 Mampu mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan;</p> <p>3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan;</p> <p>3.3 Mampu mendeteksi adanya anomali pada <i>log</i> perangkat <i>monitoring</i> keamanan jaringan;</p> |

| | | | 3.4 Mampu menganalisis hasil temuan anomali. | | |
|--------------------------|----------------|---|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |



| | | | |
|--|--|---|--|
| d. Pelatihan <i>Penetration Testing</i> | | X | |
| e. Pelatihan <i>Vulnerability Assessment</i> | | X | |
| f. Pelatihan <i>Secure Software Development</i> | | X | |
| g. Pelatihan Audit Keamanan Informasi | | X | |
| h. Pelatihan Arsitektur Keamanan Sistem | | X | |
| i. Pelatihan <i>Global Industrial Security/SCA DA</i> | | X | |
| j. Pelatihan Keamanan Jaringan | | X | |
| k. Pelatihan Investigasi Intelijen Siber | | X | |
| l. Pelatihan <i>Cyber Threat Intelligence</i> | | X | |
| m. Pelatihan <i>Analysis Malware</i> | | X | |
| n. Pelatihan | | X | |

| | | | | | |
|------------------------------|---|---|---|---|--|
| | | Kontra Penginderaan | | | |
| | | o. Pelatihan <i>System Security</i> | | X | |
| | | p. Pelatihan <i>Cyberwarfare</i> | | X | |
| | | q. Pelatihan <i>Social Engineering</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun. | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Pertama | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | | |

f. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI MUDA | | | |
|---|--|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi kendali operasi keamanan siber dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan security operation center (SOC), pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | <p>3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap</p> |

| | | | |
|---------------|---|---|--|
| | | | integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.2. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | 3.1. Menyampaikan suatu informasi yang sensitif/rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain; |

| | | | |
|-------------------------|---|--|---|
| | | | <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap;</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit | 3.1. Memahami, mendeskripsikan pengaruh dan hubungan/ kekuatan kelompok yang sedang berjalan di organisasi |

| | | | |
|--|--|--------|---|
| | | kerja. | <p>(aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/ masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya.</p> |
|--|--|--------|---|

| | | | |
|-------------------------------------|---|---|--|
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> |

| | | | |
|---------------------------|---|---|--|
| | | | <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat;</p> <p>3.4. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | <p>3.1. Membandingkan berbagai alternatif tindakan dan implikasinya;</p> <p>3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian;</p> <p>3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya.</p> |
| B. Sosial Kultural | | | |
| 9. Perikat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | <p>3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan;</p> <p>3.2. Melakukan pemetaan</p> |

| | | | |
|--|---|---|---|
| | | | <p>sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalah-pahaman yang diakibatkan adanya keragaman budaya yang ada;</p> <p>3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik.</p> |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan, manajemen keamanan siber dan persandian | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan</p> |

| | | | |
|---------------------------------------|---|---|---|
| | | | manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu menyelenggarakan advokasi kebijakan keamanan siber. | <p>3.1 Mampu bahan menyusun instrumen dan pelaksanaan advokasi kebijakan pendekatan, melalui bimbingan sosialisasi, teknis, pendampingan, dan <i>monitoring</i> evaluasi advokasi kebijakan.</p> <p>3.2 Mampu mengembangkan serta menjalankan strategi atau intervensi melalui sosialisasi, pendekatan, bimbingan teknis, dan pendampingan dalam mengatasi hambatan sistemis dan resistensi pemangku kepentingan dalam menerapkan kebijakan</p> <p>3.3 Mampu mengimplementasikan strategi komunikasi dengan target dan waktu yang terukur dan terencana dengan mendapatkan hasil sesuai yang diharapkan antara lain pemangku kepentingan dapat memahami serta menerapkan kebijakan, <i>monitoring</i>, dan evaluasi</p> |

| | | | |
|---|---|---|--|
| | | | kebijakan |
| 12. Pengelolaan <i>Security Operation Center (SOC)</i> | 3 | Menganalisis keberlangsungan pengelolaan SOC. | <p>3.1 Mampu menelaah NSPK terkait pengelolaan SOC;</p> <p>3.2 Mampu memeriksa keberlangsungan layanan pengelolaan SOC;</p> <p>3.3 Mampu memecahkan masalah teknis operasional yang timbul;</p> <p>3.4 Mampu membuat instrumen penilaian maturitas SOC.</p> <p>3.5 Mampu menelaah spesifikasi dukungan teknis operasional SOC.</p> |
| 13. Manajemen Insiden Siber | 3 | Mampu menyelenggarakan Manajemen Insiden Siber. | <p>3.1 Mampu melakukan analisis terkait manajemen insiden siber;</p> <p>3.2 Mampu melaksanakan rekomendasi teknis terkait manajemen insiden siber;</p> <p>3.3 Membimbing perbaikan kesalahan prosedur dalam manajemen insiden siber;</p> <p>3.4 Mampu menunjukkan perbandingan antara kedua metode</p> |

| | | | |
|---|---|--|--|
| | | | <p>pengelolaan data tersebut, setidaknya dari segi kelebihan dan kekurangan;</p> <p>3.5 Mengomunikasikan hasil analisis melalui lisan dan tulisan.</p> |
| 14. Pengelolaan Pusat Kontak Siber Nasional | 3 | Menganalisis pelaksanaan pengelolaan pusat kontak siber. | <p>3.1 Mampu memeriksa proses pelaksanaan pengelolaan pusat kontak siber;</p> <p>3.2 Mampu menganalisis masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber;</p> <p>3.3 Mampu memecahkan masalah teknis dalam pelaksanaan pengelolaan pusat kontak siber;</p> <p>3.4 Mampu membuat garis besar instrumen pengelolaan pusat kontak siber.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 3 | Mampu melakukan analisis keamanan jaringan. | <p>3.1 Mampu mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan;</p> <p>3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan;</p> <p>3.3 Mampu mendeteksi adanya anomali pada</p> |

| | | | <i>log</i> perangkat <i>monitoring</i> keamanan jaringan; 3.4 Mampu menganalisis hasil temuan anomali. | | |
|---------------------------------|----------------|---|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan manajemen risiko siber | | X | |
| | | b. Pelatihan manajemen keamanan siber dan persandian | | X | |
| | | c. Pelatihan kebijakan keamanan siber | | X | |

| | | | | | |
|--|---|--------------------------|---|---|--|
| | d. Pelatihan <i>Automation and Continuous Security Monitoring</i> | | X | | |
| | e. Pelatihan <i>cyber threat intelligence analysis</i> | | X | | |
| | f. Pelatihan manajemen insiden | | | X | |
| | g. Pelatihan penanganan insiden (<i>Incident Handling</i>) | | X | | |
| | h. Pelatihan Investigasi siber | | | X | |
| | i. Pelatihan <i>Cyber Defence Analysis</i> | | X | | |
| | j. Pelatihan <i>System Test and Evaluation</i> | | | X | |
| | k. Pelatihan arsitektur keamanan jaringan | | X | | |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| | C. Pengalaman Kerja | a. Memiliki | X | | |

| | | | | |
|------------------------------|--|--|--|--|
| | pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun b. Telah menduduki Jabatan Sandiman Ahli Pertama | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | |

g. Fungsi Pengkajian

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MUDA | |
|--|---|
| I. IKHTISAR JABATAN | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan TI, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. |
| II. STANDAR KOMPETENSI | |

| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
|----------------------|-------|--|--|
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | <p>3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin.</p> |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | <p>3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat,</p> <p>3.2. mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal;</p> <p>3.3. Mengupayakan dan mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.4. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunika | 3 | Berkomunikasi | 3.1. Menyampaikan suatu informasi |

| | | | |
|-------------------------|---|---|--|
| si | | secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | <p>yang sensitif/rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap.</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | 3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, |

| | | | |
|-------------------------------------|---|-------------------------------------|--|
| | | | <p>tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya.</p> |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur; melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.3. Mendorong kepercayaan diri bawahan; memberikan kepercayaan penuh pada</p> |

| | | | |
|---------------------------|---|---|---|
| | | | bawahan untuk mengerjakan tugas dengan caranya sendiri; memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang. |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | 3.1. Membantu orang lain dalam melakukan perubahan; 3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan; 3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan. |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | 3.1. Membandingkan berbagai alternatif tindakan dan implikasinya; 3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di |

| | | | |
|---|---|--|--|
| | | | <p>masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku;</p> <p>3.3. Mengidentifikasi potensi kesalahpahaman yang diakibatkan adanya keragaman budaya yang ada;</p> <p>3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan pelaksanaan | <p>3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan terhadap naskah kebijakan;</p> <p>3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan</p> |

| | | | |
|---|---|--|--|
| | | dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. | konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi; 3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi. |
| 12. Rekayasa Kriptografi | 3 | Menganalisis rancangan rekayasa kriptografi. | 3.1 Mampu menguji hasil rekayasa kriptografi. 3.2 Mampu menganalisis kekuatan algoritma, manajemen kunci, dan protokol kriptografi. 3.3 Mampu menganalisis kebutuhan rekayasa kriptografi. |
| 13. Rancang Bangun Perangkat Keamanan Teknologi Informasi | 3 | Menganalisis perancangan perangkat keamanan teknologi informasi. | 3.1 Mampu menemukan pola konfigurasi yang tepat pada perangkat keamanan teknologi informasi hasil rancang bangun. 3.2 Mampu menganalisis hasil pengujian perangkat keamanan teknologi informasi hasil rancang bangun. 3.3 Mampu menganalisis kebutuhan rancang bangun perangkat keamanan teknologi informasi. |

| | | | |
|--|---|--|---|
| | | | <p>3.4 Mampu memerinci spesifikasi teknis perangkat keamanan teknologi informasi hasil rancang bangun.</p> <p>3.5 Mampu menjamin pemberian dukungan pada pengkajian teknologi keamanan siber dan sandi.</p> |
| 14. Pengkajian Teknologi Keamanan Siber dan Sandi | 3 | Menganalisis pelaksanaan kegiatan pengkajian teknologi keamanan siber dan sandi. | <p>3.1 Mampu menguji celah keamanan teknologi informasi.</p> <p>3.2 Mampu membuat <i>blueprint</i> simulasi perangkat keamanan teknologi informasi.</p> <p>3.3 Mampu mengklasifikasikan prosedur dalam identifikasi kebutuhan pengkajian teknologi keamanan siber dan sandi.</p> <p>3.4 Mampu menganalisis kebutuhan pengkajian teknologi keamanan siber dan sandi.</p> |
| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 3 | Mengelola dan merencanakan penelitian. | <p>3.1 Mampu menata instrumen untuk kegiatan identifikasi, pengumpulan, pengolahan, dan pelaporan suatu kegiatan penelitian dalam bidang teknologi keamanan siber dan sandi.</p> <p>3.2 Mampu mengoptimalkan pengetahuan terkait tujuan, metode, teknik analisis, dan kesimpulan suatu penelitian secara teknis maupun operasional melalui bimbingan teknis.</p> <p>3.3 Mampu memecahkan masalah teknis operasional penelitian.</p> |
| III. PERSYARATAN JABATAN | | | |

| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
|-------------------|----------------|---|-------------------------------------|---------|-------|
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Kriptografi Simetrik | | X | |
| | | e. Pelatihan Kriptografi | | X | |

| | | | |
|--|---|---|--|
| | Asimetrik | | |
| | f. Pelatihan Fungsi Hash | X | |
| | g. Pelatihan Pembangkit Bilangan Acak | X | |
| | h. Pelatihan Infrastruktur Kunci Publik | X | |
| | i. Pelatihan Protokol Kriptografi | X | |
| | j. Pelatihan Bahasa Pemrograman | X | |
| | k. Pelatihan Steganografi | X | |
| | l. Pelatihan <i>Embedded System</i> | X | |
| | m. Pelatihan Perancangan Piranti Lunak | X | |
| | n. Pelatihan Perancangan Piranti Keras | X | |
| | o. Pelatihan <i>Software Testing</i> | X | |
| | p. Pelatihan <i>Hardware Testing</i> | X | |
| | q. Pelatihan Keamanan Jaringan | X | |
| | r. Pelatihan | X | |

| | | | | | |
|------------------------------|--|--|---|---|--|
| | | Pengelolaan Kunci | | | |
| | 3. Fungsional 1 | Diklat Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | b. Telah menduduki Jabatan Sandiman Ahli Pertama | X | | |
| | | | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian | | | | |

h. Fungsi Proteksi

| | | |
|-------------------|---|--------------------|
| Nama Jabatan | : | Sandiman Ahli Muda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

JABATAN FUNSIONAL SANDIMAN AHLI MUDA

| | |
|----------------------------|--|
| I. IKHTISAR JABATAN | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran taktis dengan menjalankan fungsi proteksi dengan melakukan |

| | | manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi, dan <i>monitoring</i> keamanan jaringan | |
|------------------------|-------|---|--|
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 3 | Mampu memastikan, menanamkan keyakinan bersama agar anggota yang dipimpin bertindak sesuai nilai, norma, dan etika organisasi, dalam lingkup formal. | 3.1. Memastikan anggota yang dipimpin bertindak sesuai dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.2. Mampu untuk memberi apresiasi dan teguran bagi anggota yang dipimpin agar bertindak selaras dengan nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 3.3. Melakukan <i>monitoring</i> dan evaluasi terhadap penerapan sikap integritas di dalam unit kerja yang dipimpin. |
| 2. Kerjasama | 3 | Efektif membangun tim kerja untuk peningkatan kinerja organisasi. | 3.1. Melihat kekuatan/kelemahan anggota tim, membentuk tim yang tepat, mengantisipasi kemungkinan hambatan, dan mencari solusi yang optimal; 3.2. Mengupayakan dan |

| | | | |
|---------------|---|---|--|
| | | | <p>mengutamakan pengambilan keputusan berdasarkan usulan-usulan anggota tim/kelompok, bernegosiasi secara efektif untuk upaya penyelesaian pekerjaan yang menjadi target kinerja kelompok dan/atau unit kerja;</p> <p>3.3. Membangun aliansi dengan para pemangku kepentingan dalam rangka mendukung penyelesaian target kerja kelompok.</p> |
| 3. Komunikasi | 3 | Berkomunikasi secara asertif, terampil berkomunikasi lisan/ tertulis untuk menyampaikan informasi yang sensitif/ rumit/ kompleks. | <p>3.1. Menyampaikan suatu informasi yang sensitif/ rumit dengan cara penyampaian dan kondisi yang tepat, sehingga dapat dipahami dan diterima oleh pihak lain;</p> <p>3.2. Menyederhanakan topik yang rumit dan sensitif sehingga lebih mudah dipahami dan diterima orang lain;</p> <p>3.3. Membuat laporan tahunan/ periodik/ naskah/ dokumen/ proposal yang kompleks;</p> <p>3.4. Membuat surat resmi</p> |

| | | | |
|-------------------------|---|--|---|
| | | | <p>yang sistematis dan tidak menimbulkan pemahaman yang berbeda;</p> <p>3.5. Membuat proposal yang rinci dan lengkap;</p> |
| 4. Orientasi pada hasil | 3 | Menetapkan target kerja yang menantang bagi unit kerja, memberi apresiasi dan teguran untuk mendorong kinerja. | <p>3.1. Menetapkan target kinerja unit yang lebih tinggi dari target yang ditetapkan organisasi;</p> <p>3.2. Memberikan apresiasi dan teguran untuk mendorong pencapaian hasil unit kerjanya;</p> <p>3.3. Mengembangkan metode kerja yang lebih efektif dan efisien untuk mencapai target kerja unitnya.</p> |
| 5. Pelayanan publik | 3 | Mampu memanfaatkan kekuatan kelompok serta memperbaiki standar pelayanan publik di lingkup unit kerja. | <p>3.1. Memahami, mendeskripsikan pengaruh dan hubungan/kekuatan kelompok yang sedang berjalan di organisasi (aliansi atau persaingan) dan dampaknya terhadap unit kerja untuk menjalankan tugas pemerintahan secara profesional dan netral, tidak memihak;</p> <p>3.2. Menggunakan keterampilan dan pemahaman lintas</p> |

| | | | |
|-------------------------------------|---|-------------------------------------|---|
| | | | <p>organisasi untuk secara efektif memfasilitasi kebutuhan kelompok yang lebih besar dengan cara-cara yang mengikuti standar objektif, transparan, profesional, sehingga tidak merugikan para pihak di lingkup pelayanan publik unit kerjanya;</p> <p>3.3. Mengimplementasikan cara-cara yang efektif untuk memantau dan mengevaluasi masalah yang dihadapi pemangku kepentingan/masyarakat serta mengantisipasi kebutuhan mereka saat menjalankan tugas pelayanan publik di unit kerjanya.</p> |
| 6. Pengembangan diri dan orang lain | 3 | Memberikan umpan balik, membimbing. | <p>3.1. Memberikan tugas-tugas yang menantang pada bawahan sebagai media belajar untuk mengembangkan kemampuannya;</p> <p>3.2. Mengamati bawahan dalam mengerjakan tugasnya dan memberikan umpan balik yang objektif dan jujur;</p> |

| | | | |
|--------------------------|---|---|--|
| | | | <p>3.3. Melakukan diskusi dengan bawahan untuk memberikan bimbingan dan umpan balik yang berguna bagi bawahan;</p> <p>3.4. Mendorong kepercayaan diri bawahan;</p> <p>3.5. Memberikan kepercayaan penuh pada bawahan untuk mengerjakan tugas dengan caranya sendiri;</p> <p>3.6. Memberi kesempatan dan membantu bawahan menemukan peluang untuk berkembang.</p> |
| 7. Mengelola perubahan | 3 | Membantu orang lain mengikuti perubahan, mengantisipasi perubahan secara tepat. | <p>3.1. Membantu orang lain dalam melakukan perubahan;</p> <p>3.2. Menyesuaikan prioritas kerja secara berulang-ulang jika diperlukan;</p> <p>3.3. Mengantisipasi perubahan yang dibutuhkan oleh unit kerjanya secara tepat;</p> <p>3.4. Memberikan solusi efektif terhadap masalah yang ditimbulkan oleh adanya perubahan.</p> |
| 8. Pengambilan keputusan | 3 | Membandingkan berbagai | 3.1. Membandingkan berbagai alternatif |

| | | | |
|---------------------------|---|--|--|
| | | alternatif, menyeimbangkan risiko keberhasilan dalam implementasi. | tindakan dan implikasinya; 3.2. Memilih alternatif solusi yang terbaik, membuat keputusan operasional mengacu pada alternatif solusi terbaik yang didasarkan pada analisis data yang sistematis, seksama, mengikuti prinsip kehati-hatian; 3.3. Menyeimbangkan antara kemungkinan risiko dan keberhasilan dalam implementasinya. |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 3 | Mempromosikan, mengembangkan sikap toleransi dan persatuan. | 3.1. Mempromosikan sikap menghargai perbedaan di antara orang-orang yang mendorong toleransi dan keterbukaan; 3.2. Melakukan pemetaan sosial di masyarakat sehingga dapat memberikan respon yang sesuai dengan budaya yang berlaku; 3.3. Mengidentifikasi potensi kesalah-pahaman yang diakibatkan adanya keragaman budaya yang ada; |

| | | | |
|---|---|--|--|
| | | | 3.4. Menjadi mediator untuk menyelesaikan konflik atau mengurangi dampak negatif dari konflik atau potensi konflik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 3 | Menganalisis kebutuhan dalam penyelenggaraan manajemen keamanan siber dan persandian. | <p>3.1 Mampu mengukur kesenjangan antara kondisi terkini dan kondisi ideal dalam manajemen keamanan siber dan persandian sesuai dengan standar yang berlaku;</p> <p>3.2 Mampu menganalisis prosedur teknis penerapan kontrol keamanan informasi ke dalam format NSPK yang berlaku;</p> <p>3.3 Mampu mengoptimalkan instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 3 | Mampu melakukan penilaian dan evaluasi terhadap konsep kebijakan, program implementasi dan | 3.1 Mampu melakukan penilaian dan evaluasi terhadap naskah kebijakan keamanan informasi, mengidentifikasi kekurangan dan merumuskan perbaikan |

| | | | |
|--|---|---|---|
| | | <p>pelaksanaan dan hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> | <p>terhadap naskah kebijakan;</p> <p>3.2 Mampu melakukan penilaian dan evaluasi implementasi kebijakan, menguasai konten dan konteks kebijakan, mengetahui dampak positif dan negatif dari suatu kebijakan, mengetahui hambatan dan daya dukung terhadap implementasi kebijakan, serta dapat melakukan koordinasi dengan <i>stakeholders</i> dalam implementasi keamanan informasi;</p> <p>3.3 Mampu menyusun perencanaan dan melaksanakan program <i>monitoring</i> dan evaluasi terhadap penerapan kebijakan serta melakukan analisis terhadap hasil <i>monitoring</i> dan evaluasi kebijakan keamanan informasi.</p> |
| <p>12. Manajemen Risiko Keamanan Siber</p> | 3 | <p>Mampu melaksanakan penilaian risiko dan menganalisis penerapan manajemen risiko.</p> | <p>3.1 Mampu mengidentifikasi risiko berdasarkan aset maupun proses bisnis organisasi;</p> <p>3.2 Mampu menerapkan</p> |

| | | | |
|---|---|---|--|
| | | | <p>manajemen risiko sesuai standar atau kebijakan yang ditentukan;</p> <p>3.3 Mampu menerapkan kontrol terhadap risiko berdasarkan standar atau kebijakan yang telah ditentukan.</p> |
| 13. Audit Keamanan Informasi | 3 | Mengaudit keamanan informasi, keamanan siber dan persandian sesuai dengan prosedur / petunjuk teknis. | <p>3.1 Mampu menelaah kesesuaian data pada kegiatan audit keamanan informasi, keamanan siber dan persandian;</p> <p>3.2 Mampu mengaudit lapangan (<i>onsite</i>) sesuai prosedur, standar, dan norma tentang audit keamanan informasi, keamanan siber, dan persandian;</p> <p>3.3 Mampu mendokumentasikan hasil audit keamanan informasi, keamanan siber dan persandian;</p> <p>3.4 Mampu memeriksa proses audit keamanan informasi, keamanan siber, dan persandian.</p> |
| 14. Penyediaan Layanan Keamanan Informasi | 3 | Mengelola penyelenggaraan penyediaan layanan keamanan | <p>3.1 Mampu menganalisis kebutuhan penyelenggaraan layanan keamanan informasi sesuai</p> |

| | | | |
|---|---|---|--|
| | | informasi. | dengan kebutuhan pengguna dan kecukupan sumber daya yang dialokasikan oleh organisasi atau pengguna; 3.2 Mampu menganalisis norma, standar, prosedur, dan kriteria untuk penyelenggaraan layanan keamanan informasi; 3.3 Mampu memberikan bimbingan teknis mengenai layanan keamanan informasi yang akan diterapkan. |
| 15. <i>Monitoring</i> Keamanan Jaringan | 3 | Mampu melakukan analisis keamanan jaringan. | 3.1 Mampu mengidentifikasi teknik dan metode analisis keamanan jaringan yang dibutuhkan; 3.2 Mampu mengkorelasikan teknik dan metode analisis keamanan jaringan; 3.3 Mampu mendeteksi adanya anomali pada <i>log</i> perangkat <i>monitoring</i> keamanan jaringan; 3.4 Mampu menganalisis hasil temuan anomali. |
| III. PERSYARATAN JABATAN | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan |

| | | | Mutlak | Penting | Perlu |
|---------------|----------------|---|--------|---------|-------|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Secure Software Development</i> | | X | |
| | | e. Pelatihan Audit Keamanan Informasi | | X | |
| | | f. Pelatihan Arsitektur Keamanan | | X | |

| | | | | | |
|---------------------|--|---|--|---|--|
| | | Sistem | | | |
| | | g. Pelatihan <i>Global Industrial Security/ SCADA</i> | | X | |
| | | h. Pelatihan Keamanan Jaringan | | X | |
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | | j. Pelatihan Keamanan Sistim Informasi | | X | |
| | | k. Pelatihan Peralatan Keamanan Siber dan Persandian | | X | |
| | | l. Pelatihan Diplomasi Siber | | X | |
| | 3. Fungsional | Fungsional Sandiman Muda | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Pertama | | | | |
| D. Pangkat | III/c (Penata) III/d (Penata Tingkat I) | | | | |

| | |
|------------------------------|---|
| E. Indikator Kinerja Jabatan | Hasil analisis keamanan informasi, keamanan siber, dan persandian |
|------------------------------|---|

3. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN AHLI MADYA/ MADYA

a. Fungsi Sertifikasi dan Evaluasi Produk

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Mayda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MADYA | | | |
|---|--|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi sertifikasi dan evaluasi produk dengan melakukan Manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan pengujian produk keamanan siber dan sandi negara, verifikasi algoritma kriptografi, <i>functional testing</i> , dan analisis kerawanan produk keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | 4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya; 4.3. Berani melakukan |

| | | | |
|---------------|---|---|---|
| | | | koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko. |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk | 4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama; |

| | | | |
|-------------------------|---|--|--|
| | | mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepatutnya pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |

| | | | |
|---------------------|---|---|---|
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | <p>4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/ kelompok/ partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar</p> |
|---------------------|---|---|---|

| | | | |
|-------------------------------------|---|--|--|
| | | | objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | 4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan |

| | | | |
|---------------------------|---|--|--|
| | | | <p>termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk | 4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan |

| | | | |
|---|---|--|---|
| | | meningkatkan efektifitas organisasi | <p>masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, gender, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, jender, sosial ekonomi, preferensi politik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan manajemen keamanan siber dan persandian | <p>4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi;</p> <p>4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian;</p> |

| | | | |
|---------------------------------------|---|---|---|
| | | | 4.3 Mampu mensosialisasikan kebijakan Manajemen Keamanan Siber dan Persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 4 | Mampu melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, <i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika | 4.1 Mampu melakukan penyesuaian (harmonisasi) dengan peraturan perundang-undangan yang lain; mampu merumuskan intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/naskah</i> final kebijakan keamanan informasi; 4.2 Menguasai kunci-kunci sukses dalam implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam |

| | | | |
|--|---|--|--|
| | | | <p>implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas implementasi suatu kebijakan keamanan informasi;</p> <p>4.3 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi kebijakan di instansi <i>benchmark</i>; menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i> dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi.</p> |
| 12. Pengelolaan Pengujian Produk Keamanan Siber dan Sandi Negara | 4 | Mengevaluasi kegiatan pengelolaan pengujian produk keamanan siber dan sandi negara | <p>4.1 Mampu menilai efektivitas dan efisiensi prosedur, metode, dan standar yang digunakan dalam layanan pengujian produk;</p> <p>4.2 Mampu menyusun prosedur, metode, dan standar layanan pengujian produk yang lebih efektif dan efisien;</p> <p>4.3 Mampu menyamakan persepsi dan membuat kesepakatan dengan <i>stakeholder</i> dalam</p> |

| | | | |
|--|---|--|---|
| | | | pelaksanaan layanan pengujian produk. |
| 13. Verifikasi Algoritma Kriptografi | 4 | Mengevaluasi kegiatan verifikasi algoritma kriptografi | <p>4.1 Mampu menilai efektivitas dan efisiensi prosedur dan metode verifikasi algoritma kriptografi;</p> <p>4.2 Mampu mengarahkan prosedur dan metode verifikasi algoritma kriptografi yang dinilai lebih efektif dan efisien;</p> <p>4.3 Mampu menyamakan persepsi dan membuat kesepakatan dengan <i>stakeholder</i> dalam pelaksanaan verifikasi algoritma kriptografi.</p> |
| 14. <i>Functional Testing</i> | 4 | Mengevaluasi test plan dan pelaksanaan <i>functional testing</i> | <p>4.1 Mampu menilai keabsahan test plan yang disusun;</p> <p>4.2 Mampu menilai efektivitas dan efisiensi prosedur, dan metode yang digunakan dalam <i>functional testing</i>;</p> <p>4.3 Mampu menyusun prosedur, metode, dan standar analisis kerawanan produk yang lebih efektif dan efisien.</p> |
| 15. Analisis Kerawanan Produk Keamanan Siber dan | 4 | Mengevaluasi test plan dan pelaksanaan analisis kerawanan produk | <p>4.1 Mampu menilai keabsahan test plan yang disusun;</p> <p>4.2 Mampu menilai efektivitas dan efisiensi</p> |

| | | | | | |
|---------------------------------|----------------|---|--|---------|-------|
| Sandi Negara | | | prosedur, dan metode yang digunakan dalam analisis kerawanan produk; 4.3 Mampu mengevaluasi tren investigasi di bidang keamanan siber, dan/atau persandian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber | | X | |



| | | | |
|--|--|---|--|
| dan Persandian | | | |
| c. Pelatihan Kebijakan Keamanan Siber | | X | |
| d. Pelatihan Standar Keamanan Modul Sandi | | X | |
| e. Pelatihan Standar Keamanan Perangkat TI | | X | |
| f. Pelatihan Metode Evaluasi Keamanan Modul Sandi | | X | |
| g. Pelatihan Metode Evaluasi Keamanan Perangkat TI | | X | |
| h. Pelatihan Persyaratan Umum Kompetensi Laboratorium Pengujian | | X | |
| i. Pelatihan Persyaratan Umum Lembaga Sertifikasi | | X | |
| j. Pelatihan Skema dan Layanan Sertifikasi Produk | | X | |

| | | | | | |
|------------------------------|---|---|---|---|--|
| | | k. Pelatihan Audit Internal Sistem Manajemen Mutu | | X | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber dan persandian paling sedikit 2 (dua) tahun | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | | |

b. Fungsi Investigasi Forensik Digital

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Madya |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| |
|--|
| JABATAN FUNSIONAL SANDIMAN AHLI MADYA |
| I. IKHTISAR JABATAN |

| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi investigasi forensik digital dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, forensik digital, <i>data science</i> keamanan siber dan sandi negara, analisis kripto, dan investigasi siber | | |
|------------------------|--|---|---|
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | <p>4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya;</p> <p>4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko.</p> |
| 2. Kerjasama | 4 | Membangun | 4.1. Membangun sinergi |

| | | | |
|---------------|---|--|--|
| | | komitmen tim, sinergi. | <p>antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan</p> |

| | | | |
|-------------------------|---|--|---|
| | | | <p>pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangkai meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, | 4.1. Memahami dan memberi perhatian |

| | | | |
|--|--|---|---|
| | | <p>memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional.</p> | <p>kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/ kelompok/ partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam</p> |
|--|--|---|---|

| | | | |
|-------------------------------------|---|---|--|
| | | | menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara</p> |

| | | | |
|--------------------------|---|---|---|
| | | | konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya. |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> |

| | | | |
|---------------------------|---|--|--|
| | | | 4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk meningkatkan efektifitas organisasi. | <p>4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang</p> |

| | | | |
|---|---|--|--|
| | | | agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan Manajemen Keamanan Siber dan Persandian. | 4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi; 4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan Manajemen Keamanan Siber dan Persandian; 4.3 Mampu mensosialisasikan kebijakan Manajemen Keamanan Siber dan Persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 4 | Mampu melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, <i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika. | 4.1 Mampu melakukan penyesuaian (harmonisasi) dengan peraturan perundang-undangan yang lain; mampu merumuskan intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/naskah</i> final |

| | | | |
|--|--|--|---|
| | | | <p>kebijakan keamanan informasi;</p> <p>4.2 Menguasai kunci-kunci sukses dalam implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas implementasi suatu kebijakan keamanan informasi;</p> <p>4.3 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi kebijakan di instansi <i>benchmark</i>; menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i></p> |
|--|--|--|---|

| | | | |
|---|---|---|---|
| | | | dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi. |
| 12. Forensik Digital | 4 | Merekomendasikan hasil forensik digital. | <p>4.1 Mampu merekomendasikan terkait dengan profil hasil forensik digital;</p> <p>4.2 Mampu mengevaluasi norma, standar, prosedur, kriteria (NSPK) di bidang forensik digital;</p> <p>4.3 Mampu mengevaluasi tren forensik digital.</p> |
| 13. Data Science Keamanan Siber dan Sandi | 4 | Merekomendasikan hasil <i>information gathering</i> . | <p>4.1 Mampu merekomendasikan hasil pengumpulan <i>data science</i>;</p> <p>4.2 Mampu mengevaluasi norma, standar, prosedur, kriteria (NSPK) di bidang <i>data science</i> di bidang keamanan siber;</p> <p>4.3 Mampu menganalisis <i>data science</i>.</p> |
| 14. Analisis Kripto | 4 | Merekomendasikan hasil analisis kripto. | <p>4.1 Mampu menyampaikan hasil <i>analisis kripto</i>;</p> <p>4.2 Mampu memberikan alternatif prosedur/ metode <i>analisis kripto</i>;</p> |

| | | | 4.3 Mampu merekomendasikan tren <i>analisis kripto</i> . | | |
|---------------------------------|----------------|---|--|---------|-------|
| 15. Investigasi Siber | 4 | Mengevaluasi investigasi siber. | 4.1 Mampu mengevaluasi hasil investigasi di bidang keamanan siber, dan/atau persandian; 4.2 Mampu mengevaluasi norma, standar, prosedur, kriteria (NSPK) investigasi di bidang keamanan siber, dan/atau persandian; 4.3 Mampu mengevaluasi tren investigasi di bidang keamanan siber, dan/atau persandian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya | | X | |

| | | | | | |
|--|-----------|--|--|---|--|
| | | Integritas dan Anti Korupsi | | | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Computer Forensic Analysis</i> | | X | |
| | | e. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| | | f. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| | | g. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |



| | | | |
|---|--|---|--|
| h. Pelatihan <i>Anti-Forensic Analysis</i> | | X | |
| i. Pelatihan <i>Media Digital Forensic Analysis</i> | | X | |
| j. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| k. Pelatihan <i>Cryptocurren cy Forensic Analysis</i> | | X | |
| l. Pelatihan <i>IoT Forensic Analysis</i> | | X | |
| m. Pelatihan <i>Reverse- Engineering Malware</i> | | X | |
| n. Pelatihan <i>Cloud Forensic Analysis</i> | | X | |
| o. Pelatihan Investigasi Siber | | X | |
| p. Pelatihan <i>Cyber Law Data Secuiry and Investigation</i> | | X | |
| q. Pelatihan <i>Incident</i> | | X | |

| | | | | | |
|------------------------------|---|---|---|---|--|
| | | <i>Handling</i> | | | |
| | | r. Pelatihan <i>Threat Intelligence</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber dan persandian paling sedikit 2 (dua) tahun | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Muda | | x | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | | |

c. Fungsi Penanggulangan dan Pemulihan

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Mayda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MADYA | | | |
|---|--|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi penanggulangan dan pemulihan dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan CSIRT, manajemen insiden siber, manajemen krisis siber, dan forensik digital. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | 4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi; 4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya; |

| | | | |
|---------------|---|--|---|
| | | | 4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko. |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | 4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin; 4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi; 4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/ semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi. |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara | 4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain |

| | | | |
|-------------------------|---|---|--|
| | | lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/ konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar</p> |

| | | | |
|------------------------|---|--|---|
| | | | unit kerja dalam rangkat meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi; 4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/ kelompok/ partai politik; 4.3. Menerapkan strategi |

| | | | |
|-------------------------------------|---|---|--|
| | | | <p>jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/ kelompok.</p> |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang</p> |

| | | | |
|--------------------------|---|--|---|
| | | | disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya. |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/ seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan</p> |

| | | | |
|---------------------------|---|--|--|
| | | | dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk meningkatkan efektifitas organisasi. | <p>4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi,</p> |

| | | | |
|--|---|--|--|
| | | | preferensi politik. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan manajemen keamanan siber dan persandian. | 4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi; 4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian; 4.3 Mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 4 | Mampu melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, <i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika. | 4.1 Mampu melakukan penyesuaian (harmonisasi) dengan peraturan perundang-undangan yang lain; 4.2 Mampu merumuskan intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/</i> naskah final kebijakan keamanan informasi; 4.3 Menguasai kunci-kunci sukses dalam |

| | | | |
|--|--|--|--|
| | | | <p>implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas implementasi suatu kebijakan keamanan informasi;</p> <p>4.4 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi kebijakan di instansi <i>benchmark</i>;</p> <p>4.5 Menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i> dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi.</p> |
|--|--|--|--|

| | | | |
|-----------------------|---|--|--|
| 12. Pengelolaan CSIRT | 4 | Mampu mengevaluasi kegiatan yang terkait dengan pembangunan kapasitas CSIRT. | 4.1 Mampu memberikan pertimbangan dalam rangka evaluasi kegiatan asistensi CSIRT; 4.2 Mampu memberikan pertimbangan dalam rangka evaluasi kegiatan pembangunan kapasitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber; 4.3 Mampu merinci aspek-aspek penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber; 4.4 Mampu merinci aspek-aspek penilaian kematangan CSIRT; 4.5 Mampu mengevaluasi penilaian kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber; 4.6 Mampu mengevaluasi instrumen audit keamanan informasi, keamanan siber, dan |
|-----------------------|---|--|--|

| | | | |
|----------------------------|---|--|--|
| | | | persandian |
| 13.Manajemen Insiden Siber | 4 | Mampu mengevaluasi dan menyusun perangkat norma standar prosedur instrumen pada Manajemen Insiden Siber. | <p>4.1 Mampu melakukan evaluasi implementasi pengamanan informasi;</p> <p>4.2 Mampu merancang metode dalam meningkatkan efisiensi dan/atau efektivitas manajemen insiden siber pada lingkup instansinya;</p> <p>4.3 Mampu melakukan penilaian kesiapan manajemen insiden siber pada lingkup instansinya;</p> <p>4.4 Mampu merancang skenario simulasi kesiapan manajemen insiden siber;</p> <p>4.5 Mampu melakukan Penilaian keamanan informasi dan penentuan insiden keamanan informasi</p> |
| 14.Manajemen Krisis Siber | 4 | Mampu mengevaluasi dan menyusun perangkat norma standar prosedur instrumen pada Manajemen Krisis Siber. | <p>4.1 Mampu menyusun pedoman, petunjuk teknis, cara kerja yang dijadikan norma standar, prosedur, instrumen pelaksanaan manajemen krisis siber;</p> <p>4.2 Mampu melakukan evaluasi terhadap teknis/ metode/ sistem cara kerja penanganan</p> |

| | | | | |
|---------------------------------|--------|---|--|-------|
| | | | <p>krisis siber dan melakukan pengembangan atau perbaikan cara kerja penanganan insiden;</p> <p>4.3 Mampu melaksanakan hubungan dan koneksi dengan organisasi internal dan eksternal dalam proses manajemen krisis siber;</p> <p>4.4 Mampu menyusun dokumen <i>crisis management plan</i>;</p> <p>4.5 Mampu memberikan bimbingan/asistensi pembuatan kebijakan manajemen krisis level organisasi</p> | |
| 15.Forensik Digital | 4 | Merekomendasikan hasil forensik digital | <p>4.1 mampu merekomendasikan terkait dengan profil hasil forensik digital;</p> <p>4.2 mampu mengevaluasi norma, standar, prosedur, kriteria (NSPK) di bidang forensik digital;</p> <p>4.3 mampu mengevaluasi tren forensik digital;</p> | |
| III. PERSYARATAN JABATAN | | | | |
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | Mutlak | Pentin | Perlu |

| | | | | g | |
|---------------|----------------|---|--|---|--|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Audit Keamanan Siber | | X | |
| | | e. Pelatihan CEH | | X | |
| | | f. Pelatihan <i>Management CSIRT</i> | | X | |
| | | g. Pelatihan Manajemen Insiden Siber | | X | |
| | | h. Pelatihan <i>Incident Handling</i> | | X | |
| | | i. Pelatihan <i>Log Analysis</i> | | X | |

| | | | | |
|---------------------|--|---|---|--|
| | j. Pelatihan <i>Network Security</i> | | X | |
| | k. Pelatihan <i>Artifak Handling</i> | | X | |
| | l. Pelatihan <i>Disaster Recovery</i> | | X | |
| | m. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| | n. Pelatihan <i>Computer Forensic Analysis</i> | | X | |
| | o. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| | p. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| | q. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| | r. Pelatihan <i>Investigasi Siber</i> | | X | |
| | s. Pelatihan <i>Cyber Crisis Management Planning</i> | | X | |
| | t. Pelatihan <i>DFIR (Digital Forensic for Incident Responder)</i> | | X | |
| 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | (dua) tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | |

d. Fungsi Identifikasi dan Deteksi

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Mayda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI MADYA | | | |
|--|---|---|--|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi identifikasi dan deteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, intelijen siber, penilaian keamanan teknologi informasi, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada | 4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi |

| | | | |
|---------------|---|-------------------------------------|---|
| | | nilai, norma, dan etika organisasi. | <p>dalam segala situasi dan kondisi;</p> <p>4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya;</p> <p>4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu | 4.1. Mengintegrasikan |

| | | | |
|-------------------------|---|--|--|
| | | mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama; 4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan; 4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal; 4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan. |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | 4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan; 4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi; 4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangkai meningkatkan |

| | | | |
|---------------------|---|---|--|
| | | | efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan public | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | <p>4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/ kelompok/ partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun</p> |

| | | | |
|-------------------------------------|---|---|--|
| | | | kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | 4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin |

| | | | |
|---------------------------|---|---|--|
| | | | <p>terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk meningkatkan efektifitas organisasi. | 4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan |

| | | | |
|--|---|---|--|
| | | | <p>menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik.</p> |
| C. Teknis | | | |
| 10.Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan manajemen keamanan siber dan persandian. | <p>4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi;</p> <p>4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>4.3 mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian.</p> |

| | | | |
|--|----------|---|---|
| <p>11. Advokasi Kebijakan Keamanan Siber</p> | <p>4</p> | <p>Mampu melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, <i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika.</p> | <p>4.1 Mampu melakukan penyesuaian (harmonisasi) dengan peraturan perundang-undangan yang lain; mampu merumuskan intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/naskah</i> final kebijakan keamanan informasi;</p> <p>4.2 Menguasai kunci-kunci sukses dalam implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas</p> |
|--|----------|---|---|

| | | | |
|--|---|---|---|
| | | | <p>implementasi suatu kebijakan keamanan informasi;</p> <p>4.3 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi kebijakan di instansi <i>benchmark</i>; menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i> dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi.</p> |
| 12. Manajemen Risiko Keamanan Siber | 4 | Mengevaluasi manajemen risiko. | <p>4.1 Mampu menilai tingkat kematangan manajemen risiko keamanan informasi suatu organisasi;</p> <p>4.2 Mampu mengevaluasi efektifitas dan efisiensi pelaksanaan manajemen risiko;</p> <p>4.3 Mampu mengevaluasi <i>Risk Treatment Plan</i> yang sudah ada.</p> |
| 13. Penilaian Keamanan Teknologi Informasi | 4 | Mampu memberikan pertimbangan pelaksanaan penilaian keamanan teknologi informasi. | <p>4.1 Mampu memberi pertimbangan terhadap tata cara pelaksanaan penilaian keamanan teknologi informasi;</p> <p>4.2 Mampu menilai efektivitas dan efisiensi terhadap tata cara</p> |

| | | | |
|---|---|--|---|
| | | | <p>pelaksanaan penilaian keamanan teknologi informasi;</p> <p>4.3 Mampu menyusun materi diseminasi penilaian keamanan teknologi informasi;</p> <p>4.4 Mampu meyakinkan pemangku kepentingan terkait manfaat penilaian keamanan teknologi informasi.</p> |
| 14. Intelijen Siber | 4 | Mampu memberikan pertimbangan pelaksanaan intelijen siber. | <p>4.1 Mampu memutuskan ruang lingkup target <i>monitoring</i> intelijen siber;</p> <p>4.2 Mampu memvalidasi target <i>monitoring</i>;</p> <p>4.3 Mampu memprediksi ancaman dan kerawanan siber;</p> <p>4.4 Mampu memberi pertimbangan terhadap tata cara pelaksanaan intelijen siber;</p> <p>4.5 Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan intelijen siber.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 4 | Mampu memberikan pertimbangan pelaksanaan <i>monitoring</i> keamanan jaringan. | <p>4.1 Mampu memutuskan ruang lingkup target <i>monitoring</i> jaringan;</p> <p>4.2 Mampu menyimpulkan pola, metode, teknik serangan pada jaringan;</p> <p>4.3 Mampu memprediksi</p> |

| | | | ancaman dan kerawanan jaringan; 4.4 Mampu memberi pertimbangan terhadap tata cara pelaksanaan <i>monitoring</i> keamanan jaringan; 4.5 Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan <i>monitoring</i> keamanan jaringan; 4.6 Mampu menyusun materi diseminasi keamanan jaringan; 4.7 Mampu meyakinkan pemangku kepentingan terkait manfaat <i>monitoring</i> keamanan jaringan. | | |
|---------------------------------|----------------|---|---|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihanx | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya | | X | |

| | | | | |
|-----------|--|--|---|--|
| 2. Teknis | Integritas dan Anti Korupsi | | | |
| | d. Pelatihan Teknik Komunikasi | | X | |
| | a. Pelatihan Manajemen Risiko Siber | | X | |
| | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | d. Pelatihan <i>Penetration Testing</i> | | X | |
| | e. Pelatihan <i>Vulnerability Assessment</i> | | X | |
| | f. Pelatihan <i>Secure Software Development</i> | | X | |
| | g. Pelatihan Audit Keamanan Informasi | | X | |
| | h. Pelatihan Arsitektur Keamanan Sistem | | X | |
| | i. Pelatihan | | X | |

| | | | | | |
|---------------------|--|---|---------------------------|---|---|
| | | <i>Global Industrial Security/ SCADA</i> | | | |
| | | j. Pelatihan Keamanan Jaringan | | X | |
| | | k. Pelatihan Investigasi Intelijen Siber | | X | |
| | | l. Pelatihan <i>Cyber Threat Intelligence</i> | | X | |
| | | m. Pelatihan <i>Analysis Malware</i> | | X | |
| | | n. Pelatihan Kontra Penginderaan | | X | |
| | | o. Pelatihan <i>System Security</i> | | X | |
| | | p. Pelatihan <i>Cyberwarfare</i> | | X | |
| | | q. Pelatihan <i>Social Engineering</i> | | X | |
| | | 3. Fungsional | Fungsional Sandiman Madya | | X |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | siber, dan persandian paling sedikit 2 (dua) tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | |

e. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Mayda |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI MADYA | | | |
|---|---|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi kendali operasi keamanan siber dengan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan <i>security operation center</i> (SOC), pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | <p>4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya;</p> <p>4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode</p> |

| | | | |
|---------------|---|---|---|
| | | | etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko. |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk</p> |

| | | | |
|-------------------------|---|--|--|
| | | meningkatkan kinerja secara keseluruhan. | <p>tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, | 4.1. Memahami dan memberi perhatian |

| | | | |
|--|--|---|---|
| | | <p>memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional.</p> | <p>kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak</p> |
|--|--|---|---|

| | | | |
|-------------------------------------|---|---|--|
| | | | memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/pendidikan/pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja | 4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi |

| | | | |
|---------------------------|---|---|--|
| | | | <p>risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk | 4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan |

| | | | |
|---|---|--|---|
| | | meningkatkan efektifitas organisasi. | <p>masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Mengevaluasi penyelenggaraan Manajemen Keamanan Siber dan Persandian | <p>4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan siber dan persandian;</p> <p>4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan</p> |

| | | | |
|---------------------------------------|---|---|--|
| | | | <p>manajemen keamanan siber dan persandian;</p> <p>4.3 mampu memproyeksikan kebutuhan pengembangan kebijakan manajemen keamanan siber dan persandian berdasarkan peraturan maupun standar yang berlaku</p> <p>4.4 Mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 4 | Mampu mengevaluasi dan menyusun perangkat norma, prosedur, dan instrumen dalam advokasi kebijakan keamanan siber. | <p>4.1 Mampu mengevaluasi teknik, metode, dan strategi advokasi yang ada saat ini, menganalisis kelemahan dan kekurangan serta mengembangkan berbagai teknik, metode, dan strategi advokasi yang lebih efektif dan efisien dari berbagai kondisi pemangku kepentingan</p> <p>4.2 Mampu mengembangkan norma standar, kriteria, pedoman, petunjuk teknis strategi komunikasi, dan pelaksanaan advokasi</p> |

| | | | |
|--|---|--|---|
| | | | <p>yang efektif serta <i>monitoring</i> evaluasi advokasi kebijakan.</p> <p>4.3 Mampu meyakinkan dan memperoleh dukungan dari pemangku kepentingan, memberikan bimbingan, dan fasilitasi kepada pemangku kepentingan.</p> |
| 12. Pengelolaan <i>Security Operation Center</i> (SOC) | 4 | Mengevaluasi pengelolaan SOC. | <p>4.1 Mampu menilai kepatuhan pengelolaan SOC;</p> <p>4.2 Mampu memberi pertimbangan terhadap tata cara pelaksanaan pengelolaan SOC;</p> <p>4.3 Mampu mengevaluasi instrumen penilaian maturitas SOC.</p> |
| 13. Manajemen Insiden Siber | 4 | Mampu mengevaluasi dan menyusun perangkat norma standar prosedur instrumen pada Manajemen Insiden Siber. | <p>4.1 Mampu melakukan evaluasi implementasi pengamanan informasi;</p> <p>4.2 Mampu merancang metode dalam meningkatkan efisiensi dan/atau efektivitas manajemen insiden siber pada lingkup instansinya;</p> <p>4.3 Mampu melakukan penilaian kesiapan manajemen insiden siber pada lingkup instansinya;</p> <p>4.4 Mampu merancang</p> |

| | | | |
|---|---|--|--|
| | | | <p>skenario simulasi kesiapan manajemen insiden siber;</p> <p>4.5 Mampu melakukan penilaian keamanan informasi dan penentuan insiden keamanan informasi.</p> |
| 14. Pengelolaan Pusat Kontak Siber Nasional | 4 | Mengevaluasi pengelolaan pusat kontak siber | <p>4.1 Mampu mengevaluasi teknis/ metode/ sistem cara kerja pengelolaan pusat kontak siber;</p> <p>4.2 Mampu memberi pertimbangan terhadap tata cara pelaksanaan pengelolaan pusat kontak siber;</p> <p>4.3 Mampu mengevaluasi instrumen pengelolaan pusat kontak siber.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 4 | Mampu memberikan pertimbangan pelaksanaan <i>monitoring</i> keamanan jaringan. | <p>4.1 Mampu memutuskan ruang lingkup target <i>monitoring</i> jaringan;</p> <p>4.2 Mampu menyimpulkan pola, metode, teknik serangan pada jaringan;</p> <p>4.3 Mampu memprediksi ancaman dan kerawanan jaringan;</p> <p>4.4 Mampu memberi pertimbangan terhadap tata cara pelaksanaan <i>monitoring</i> keamanan</p> |

| | | | <p>jaringan;</p> <p>4.5 Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan <i>monitoring</i> keamanan jaringan;</p> <p>4.6 Mampu menyusun materi diseminasi keamanan jaringan;</p> <p>4.7 Mampu meyakinkan pemangku kepentingan terkait manfaat <i>monitoring</i> keamanan jaringan.</p> | | |
|---------------------------------|----------------|---|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan manajemen risiko siber | | | X |
| | | b. Pelatihan | | X | |

| | | | | |
|--|---|--|---|---|
| | manajemen keamanan siber dan persandian | | | |
| | c. Pelatihan kebijakan keamanan siber | | X | |
| | d. Pelatihan <i>Automation and Continuous Security Monitoring</i> | | X | |
| | e. Pelatihan <i>cyber threat intelligence analysis</i> | | X | |
| | f. Pelatihan manajemen insiden | | | X |
| | g. Pelatihan penanganan insiden (<i>Incident Handling</i>) | | X | |
| | h. Pelatihan <i>Cyber Defence Evaluation</i> | | X | |
| | i. Pelatihan <i>System Test and Evaluation</i> | | | X |
| | j. Pelatihan arsitektur keamanan | | X | |

| | | | | | |
|------------------------------|---|---------------------------|--|---|--|
| | | jaringan | | | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 3 (tiga) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | | |

f. Fungsi Pengkajian

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Madya |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

JABATAN FUNSIONAL SANDIMAN AHLI MADYA**I. IKHTISAR JABATAN**

| | | | |
|-------------------------------|--|---|--|
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan teknologi informasi, pengkajian teknologi keamanan siber dan sandi, pengelolaan penelitian teknologi keamanan siber dan sandi negara. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | <p>4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya;</p> <p>4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-niai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko.</p> |
| 2. Kerjasama | 4 | Membangun | 4.1. Membangun sinergi |

| | | | |
|---------------|---|--|--|
| | | komitmen tim, sinergi. | <p>antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> |

| | | | |
|-------------------------|---|--|---|
| | | | 4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan. |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | 4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan; 4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi; 4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan |

| | | | |
|--------------------------------|---|--|--|
| | | kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | <p>mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/parta i politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok.</p> |
| 6. Pengembangan diri dan orang | 4 | Menyusun program | 4.1. Menyusun program pengembangan jangka |

| | | | |
|------------------------|---|--|--|
| lain | | pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan</p> |

| | | | |
|---------------------------|---|---|--|
| | | | memastikan penerapan program-program perubahan selaras antar unit kerja. |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk meningkatkan efektifitas organisasi. | 4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat; |

| | | | |
|---|---|---|---|
| | | | <p>4.2. Mampu mendayagunakan perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan Manajemen Keamanan Siber dan Persandian. | <p>4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi;</p> <p>4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>4.3 Mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi | 4 | Mampu | 4.1 Mampu melakukan |

| | | | |
|--------------------------------|--|--|--|
| Kebijakan Keamanan Siber | | melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, <i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika. | penyelarasan (harmonisasi) dengan peraturan perundang-undangan yang lain; 4.2 Mampu merumuskan intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/</i> naskah final kebijakan keamanan informasi; 4.3 Menguasai kunci-kunci sukses dalam implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas implementasi |
|--------------------------------|--|--|--|

| | | | |
|---|---|--|---|
| | | | <p>suatu kebijakan keamanan informasi;</p> <p>4.4 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi kebijakan di instansi <i>benchmark</i>;</p> <p>4.5 Menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i> dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi.</p> |
| 12. Rekayasa Kriptografi | 4 | Mengevaluasi hasil rekayasa kriptografi. | <p>4.1 Mampu mengevaluasi hasil rekayasa kriptografi;</p> <p>4.2 Mampu mengevaluasi implementasi hasil rekayasa kriptografi;</p> <p>4.3 Mampu mengevaluasi desain protokol kriptografi.</p> |
| 13. Rancang Bangun Perangkat Keamanan Teknologi Informasi | 4 | Mengevaluasi perangkat keamanan TI hasil rancang bangun. | <p>4.1 Mampu mengevaluasi hasil rancang bangun perangkat keamanan TI;</p> <p>4.2 Mampu mengevaluasi implementasi hasil rancang bangun perangkat keamanan TI;</p> |
| 14. Pengkajian Teknologi Keamanan Siber dan | 4 | Mengevaluasi hasil pengkajian teknologi keamanan siber | 4.1 mampu mengevaluasi rekomendasi hasil audit keamanan informasi, keamanan siber dan |

| Sandi | | dan sandi. | persandian; 4.2 Mampu menilai tindak lanjut implementasi rekomendasi audit keamanan informasi, keamanan siber dan persandian; 4.3 Mampu mengevaluasi instrumen audit keamanan informasi, keamanan siber dan persandian. | | |
|--|----------------|-----------------------------------|--|---------|-------|
| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 4 | Mengevaluasi kegiatan penelitian. | 4.1 mampu mengevaluasi terhadap teknis/ metode/ sistem cara kerja menemu kenali kelebihan dan kekurangan melakukan pengembangan atau perbaikan cara kerja dari penelitian terkait teknologi keamanan siber dan sandi; 4.2 mampu menyusun pedoman, petunjuk teknis, atau cara kerja yang menjadi operasional standar penelitian; | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau | | | |

| | | Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
|--------------|---------------|---|--|---|--|
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan Algoritma Kriptografi | | X | |
| | | e. Pelatihan Desain Protokol Kriptografi | | X | |
| | | f. Pelatihan Desain | | X | |

| | | | | |
|--|---|--|---|--|
| | Manajemen Kunci | | | |
| | g. Pelatihan Infrastruktur Kunci Publik | | X | |
| | h. Pelatihan Protokol Kriptografi | | X | |
| | i. Pelatihan Bahasa Pemrograman | | X | |
| | j. Pelatihan Steganografi | | X | |
| | k. Pelatihan <i>Embedded System</i> | | X | |
| | l. Pelatihan Perancangan Piranti Lunak | | X | |
| | m. Pelatihan Perancangan Piranti Keras | | X | |
| | n. Pelatihan Kripanalisis | | X | |
| | o. Pelatihan Steganalisis | | X | |
| | p. Pelatihan Manajemen Proyek | | X | |
| | q. Pelatihan <i>Software Testing</i> | | X | |
| | r. Pelatihan <i>Hardware Testing</i> | | X | |
| | s. Pelatihan | | X | |

| | | | | | |
|------------------------------|---|---|---|---|--|
| | | Desain Keamanan Jaringan | | | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | |
| D. Pangkat | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | | |
| E. Indikator Kinerja Jabatan | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | | |

g. Fungsi Proteksi

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Madya |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| |
|--|
| JABATAN FUNSIONAL SANDIMAN AHLI MADYA |
| I. IKHTISAR JABATAN |

| | | | |
|-------------------------------|---|---|---|
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis sektoral dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, penyediaan layanan keamanan informasi, audit keamanan informasi, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 4 | Mampu menciptakan situasi kerja yang mendorong kepatuhan pada nilai, norma, dan etika organisasi. | <p>4.1. Menciptakan situasi kerja yang mendorong seluruh pemangku kepentingan mematuhi nilai, norma, dan etika organisasi dalam segala situasi dan kondisi;</p> <p>4.2. Mendukung dan menerapkan prinsip moral dan standar etika yang tinggi, serta berani menanggung konsekuensinya;</p> <p>4.3. Berani melakukan koreksi atau mengambil tindakan atas penyimpangan kode etik/nilai-nilai yang dilakukan oleh orang lain, pada tataran lingkup kerja setingkat instansi meskipun ada risiko.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | 4.1. Membangun sinergi antar unit kerja di lingkup instansi yang |

| | | | |
|---------------|---|---|--|
| | | | <p>dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | <p>Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan.</p> | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara</p> |

| | | | |
|-------------------------|---|--|--|
| | | | persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan. |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan |

| | | | |
|-------------------------------------|---|---|--|
| | | kepentingan yang transparan, objektif dan profesional. | <p>tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok.</p> |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program pengembangan jangka panjang dalam rangka | 4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, |

| | | | |
|------------------------|---|-------------------------------------|---|
| | | mendorong manajemen pembelajaran. | <p>termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar</p> |

| | | | |
|---------------------------|---|---|--|
| | | | unit kerja. |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 4 | Mendayagunakan perbedaan secara konstruktif dan kreatif untuk meningkatkan efektifitas organisasi | <p>4.1. Menginisiasi dan merepresentasikan pemerintah di lingkungan kerja dan masyarakat untuk senantiasa menjaga persatuan dan kesatuan dalam keberagaman dan menerima segala bentuk perbedaan dalam kehidupan bermasyarakat;</p> <p>4.2. Mampu mendayagunakan perbedaan latar belakang</p> |

| | | | |
|---|---|---|---|
| | | | <p>agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk mencapai kelancaran pencapaian tujuan;</p> <p>4.3. Mampu membuat program yang mengakomodasi perbedaan latar belakang agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 4 | Evaluasi penyelenggaraan manajemen keamanan siber dan persandian. | <p>4.1 Mampu menguji tingkat efektivitas dan efisiensi kontrol keamanan informasi;</p> <p>4.2 Mampu memvalidasi instrumen yang membantu dalam penyusunan kebijakan manajemen keamanan siber dan persandian;</p> <p>4.3 Mampu mensosialisasikan kebijakan manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 4 | Mampu melakukan harmonisasi kebijakan, meningkatkan efektivitas implementasi, | <p>4.1 Mampu melakukan penyalarsan (harmonisasi) dengan peraturan perundang-undangan yang lain;</p> <p>4.2 Mampu merumuskan</p> |

| | | | |
|--|--|---|--|
| | | <p><i>monitoring</i> dan evaluasi kebijakan komunikasi dan informatika.</p> | <p>intisari dari suatu kebijakan yang akan memberikan dampak positif dari maksud dan tujuan kebijakan bagi instansi dan masyarakat serta mampu menetapkan untuk menjadi <i>draft/</i> naskah final kebijakan keamanan informasi;</p> <p>4.3 Menguasai kunci-kunci sukses dalam implementasi suatu kebijakan, dan menerapkan praktik terbaik pendekatan implementasi kebijakan, mampu merumuskan solusi terhadap hambatan dalam implementasi suatu kebijakan dan mengembangkan pendekatan baru dalam implementasi, dan mampu memberikan dorongan dan mengambil keputusan untuk meningkatkan efektivitas implementasi suatu kebijakan keamanan informasi;</p> <p>4.4 Menguasai praktik terbaik pendekatan <i>monitoring</i> dan evaluasi</p> |
|--|--|---|--|

| | | | |
|---|---|---|---|
| | | | kebijakan di instansi <i>benchmark</i> ; 4.5 Menetapkan upaya perbaikan dan menetapkan langkah-langkah tindak lanjut dari hasil <i>monitoring</i> dan evaluasi, merumuskan perbaikan terhadap kebijakan keamanan informasi. |
| 12. Manajemen Risiko Keamanan Siber | 4 | Mengevaluasi manajemen risiko. | 4.1 mampu menilai tingkat kematangan manajemen risiko keamanan informasi suatu organisasi; 4.2 mampu mengevaluasi efektifitas dan efisiensi pelaksanaan manajemen risiko; 4.3 mampu mengevaluasi <i>risk treatment plan</i> yang sudah ada. |
| 13. Penyediaan Layanan Keamanan Informasi | 4 | Mengevaluasi penyelenggaraan penyediaan layanan keamanan informasi. | 4.1 Mampu mengevaluasi pelaksanaan layanan keamanan informasi; 4.2 Mampu mengevaluasi standar penyelenggaraan layanan keamanan informasi; 4.3 Mampu memberi rekomendasi perbaikan penyelenggaraan layanan keamanan informasi. |
| 14. Audit | 4 | Mengevaluasi | 4.1 Mampu mengevaluasi |

| | | | |
|---|---|--|--|
| Keamanan Informasi | | pelaksanaan kegiatan Audit Keamanan Informasi, keamanan siber dan persandian. | rekomendasi hasil audit keamanan informasi, keamanan siber dan persandian; 4.2 Mampu menilai tindak lanjut implementasi rekomendasi audit keamanan informasi, keamanan siber dan persandian; 4.3 Mampu mengevaluasi instrumen audit keamanan informasi, keamanan siber dan persandian. |
| 15. <i>Monitoring</i> Keamanan Jaringan | 4 | Mampu memberikan pertimbangan pelaksanaan <i>monitoring</i> keamanan jaringan. | 4.1 Mampu memutuskan ruang lingkup target <i>monitoring</i> jaringan; 4.2 Mampu menyimpulkan pola, metode, teknik serangan pada jaringan; 4.3 Mampu memprediksi ancaman dan kerawanan jaringan; 4.4 Mampu memberi pertimbangan terhadap tata cara pelaksanaan <i>monitoring</i> keamanan jaringan; 4.5 Mampu menilai efektivitas dan efisiensi terhadap tata cara pelaksanaan <i>monitoring</i> keamanan jaringan; 4.6 Mampu menyusun |

| | | | materi diseminasi keamanan jaringan; 4.7 Mampu meyakinkan pemangku kepentingan terkait manfaat <i>monitoring</i> keamanan jaringan. | | |
|---------------------------------|----------------|---|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-1/D-4 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |



| | | | |
|--|--|---|--|
| c. Pelatihan Kebijakan Keamanan Siber | | X | |
| d. Pelatihan <i>Secure Software Development</i> | | X | |
| e. Pelatihan Audit Keamanan Informasi | | X | |
| f. Pelatihan Arsitektur Keamanan Sistem | | X | |
| g. Pelatihan <i>Global Industrial Security/SCADA</i> | | X | |
| h. Pelatihan Keamanan Jaringan | | X | |
| i. Pelatihan Kontra Penginderaan | | X | |
| j. Pelatihan Keamanan Sistem Informasi | | X | |
| k. Pelatihan Peralatan Keamanan Siber dan Persandian | | X | |

| | | | | | |
|------------------------------|---------------|--|---|---|--|
| | | 1. Pelatihan Diplomasi Siber | | X | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian | X | | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Muda | | | |
| D. Pangkat | | IV/a (Pembina) IV/b (Pembina Tingkat I) IV/c (Pembina Utama Muda) | | | |
| E. Indikator Kinerja Jabatan | | Hasil evaluasi keamanan informasi, keamanan siber, dan persandian | | | |

4. STANDAR KOMPETENSI JABATAN FUNGSIONAL SANDIMAN AHLI UTAMA

a. Fungsi Sertifikasi dan Evaluasi Produk

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI UTAMA | | | |
|--|---|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi sertifikasi dan evaluasi produk dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan pengujian produk keamanan siber dan sandi negara, verifikasi algoritma kriptografi, <i>functional testing</i> , dan analisis kerawanan produk keamanan siber dan sandi. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi <i>role model</i> dalam penerapan standar keadilan dan etika di tingkat nasional. | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya; 5.2. Menjadi " <i>role model</i> " / keteladanan dalam penerapan standar keadilan dan etika yang |

| | | | |
|---------------|---|---|--|
| | | | tinggi di tingkat nasional; 5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi. |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | 4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin; 4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi; 4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi. |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi | 4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain |

| | | | |
|-------------------------|---|--|---|
| | | secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam</p> |

| | | | |
|---------------------|---|---|--|
| | | | rangkat meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | <p>4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang</p> |

| | | | |
|-------------------------------------|---|--|--|
| | | | berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara</p> |

| | | | |
|--------------------------|---|---|---|
| | | | konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya. |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi</p> |

| | | | |
|---------------------------|---|--|---|
| | | | dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | <p>5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat</p> |

| | | | |
|---|---|--|---|
| | | | kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik yang berdampak positif secara nasional. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan manajemen keamanan siber dan persandian | 5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian; 5.2 Mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran; 5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | 5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implemetasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi; 5.2 Mampu menyusun buku, pedoman, |

| | | | |
|---|---|--|---|
| | | | <p>petunjuk pelaksanaan, petunjuk teknis perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan <i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi.</p> |
| 12. Pengelolaan Pengujian Produk Keamanan | 5 | Mampu mengembangkan konsep, teori, kebijakan dan | 5.1 Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan |

| | | | |
|--------------------------------------|---|--|---|
| Siber dan Sandi Negara | | menjadi acuan bagi implementasi serta solusi dalam pelaksanaan layanan pengujian produk. | terkait pelaksanaan layanan pengujian produk serta mengupayakan peningkatan kualitasnya; 5.2 Mampu mengembangkan teori, konsep dan kebijakan terkait layanan pengujian produk dengan melibatkan para <i>stakeholder</i> ; 5.3 Mampu membuat regulasi yang menjadi acuan utama layanan pengujian produk. |
| 13. Verifikasi Algoritma Kriptografi | 5 | Mengembangkan konsep, metode, dan kebijakan terkait verifikasi algoritma kriptografi. | 5.1 Mampu merencanakan program pengembangan konsep, metode, dan kebijakan verifikasi algoritma kriptografi; 5.2 Mampu membangun konsep, metode, dan kebijakan verifikasi algoritma kriptografi; 5.3 Mampu membuat regulasi yang menjadi acuan utama verifikasi algoritma kriptografi. |
| 14. <i>Functional Testing</i> | 5 | Mampu mengembangkan konsep, teori, kebijakan dan menjadi acuan | 5.1 Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan |

| | | | |
|---|---|--|--|
| | | bagi implementasi serta solusi dalam pelaksanaan <i>functional testing</i> . | functional testing serta mengupayakan peningkatan kualitasnya; 5.2 Mampu mengembangkan teori, konsep dan kebijakan terkait pelaksanaan <i>functional testing</i> ; 5.3 Mampu membuat regulasi yang menjadi acuan utama <i>functional testing</i> . |
| 15. Analisis Kerawanan Produk Keamanan Siber dan Sandi Negara | 5 | Mampu mengembangkan konsep, teori, kebijakan dan menjadi acuan bagi implementasi serta solusi dalam pelaksanaan analisis kerawanan produk. | 5.4 Mampu mengidentifikasi dan menganalisis teori, konsep, kebijakan terkait pelaksanaan analisis kerawanan produk serta mengupayakan peningkatan kualitasnya; 5.5 Mampu mengembangkan teori, konsep dan kebijakan terkait pelaksanaan analisis kerawanan produk; 5.6 Mampu membuat regulasi yang menjadi acuan utama analisis kerawanan produk. |
| III. PERSYARATAN JABATAN | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan |

| | | Mutlak | Penting | Perlu |
|---------------|----------------|--|---------|-------|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | X | |
| | | b. Pelatihan Pengembangan Diri | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | X | |
| | | d. Pelatihan Teknik Komunikasi | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | X | |
| | | d. Pelatihan Standar Keamanan Modul Sandi | X | |
| | | e. Pelatihan Standar Keamanan | X | |
| | | | | |

| | | | | | |
|---------------------|--|---|--|---|--|
| | | Perangkat TI | | | |
| | | f. Pelatihan Metode Evaluasi Keamanan Modul Sandi | | X | |
| | | g. Pelatihan Metode Evaluasi Keamanan Perangkat TI | | X | |
| | | h. Pelatihan Persyaratan Umum Kompetensi Laboratorium Pengujian | | X | |
| | | i. Pelatihan Persyaratan Umum Lembaga Sertifikasi | | X | |
| | | j. Pelatihan Skema dan Layanan Sertifikasi Produk | | X | |
| | | k. Pelatihan Audit Internal Sistem Manajemen Mutu | | X | |
| | | 3. Fungsional Sandiman Utama | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan | X | | | |

| | | | | |
|------------------------------|--|--|--|--|
| | persandian paling sedikit 2 (dua) tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Madya | | | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian | | | |

b. Fungsi Investigasi Forensik Digital

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI UTAMA | | | |
|--|--|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi investigasi forensik digital dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, forensik digital, analisis kripto, <i>data science keamanan siber dan sandi negara</i> , dan investigasi siber. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi role model dalam penerapan standar keadilan dan etika | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan |

| | | | |
|--------------|---|----------------------------------|--|
| | | di tingkat nasional. | <p>sehari-hari yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya;</p> <p>5.2. Menjadi "role model" / keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional;</p> <p>5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi</p> |

| | | | |
|-------------------------|---|--|---|
| | | | dalam rangka pencapaian target kerja organisasi. |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> |

| | | | |
|---------------------|---|---|--|
| | | | 4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi; 4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/keompok/partai politik; |

| | | | |
|-------------------------------------|---|--|--|
| | | | 4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | 4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir; 4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi; 4.3. Mengembangkan orang-orang disekitarnya secara konsisten, |

| | | | |
|--------------------------|---|---|--|
| | | | melakukan kaderisasi untuk posisi-posisi di unit kerjanya. |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |

| B. Sosial Kultural | | | |
|---------------------------|---|--|--|
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | <p>5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik yang berdampak</p> |

| | | | |
|---|---|--|--|
| | | | positif secara nasional. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan Manajemen Keamanan Siber dan Persandian | <p>5.1 Mampu mengevaluasi kebijakan Manajemen Keamanan Siber dan Persandian;</p> <p>5.2 Mampu merumuskan kebijakan Manajemen Keamanan Siber dan Persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> <p>5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam Manajemen Keamanan Siber dan Persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | <p>5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implemetasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.2 Mampu menyusun buku, pedoman, petunjuk pelaksanaan, petunjuk teknis perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> |

| | | | |
|---------------------|---|--|--|
| | | | 5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan <i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi. |
| 12.Forensik Digital | 5 | Merumuskan keterangan ahli, rekomendasi dan kebijakan di bidang forensik digital | 5.1 Mampu merumuskan keterangan sebagai ahli forensik digital; 5.2 Mampu merumuskan rekomendasi forensik digital; 5.3 Mampu merumuskan kebijakan di bidang forensik digital. |
| 13.Analisis Kripto | 5 | merancang strategi, dan metode/ <i>tools code breaking</i> . | 5.1 Mampu merancang strategi <i>code breaking</i> ; 5.2 mampu memperbaiki metode <i>code breaking</i> ; 5.3 mampu mengembangkan |

| | | | | | |
|---|----------------|--|---|---------|-------|
| | | | metode/ tools code breaking. | | |
| 14. <i>Data Science</i> Keamanan Siber dan Sandi Negara | 5 | Merumuskan strategi rekomendasi dan kebijakan <i>data science</i> di bidang keamanan siber. | 5.1 Mampu menyusun strategi implementasi <i>data science</i> di bidang keamanan siber; 5.2 Mampu merumuskan rekomendasi <i>data science</i> ; 5.3 Mampu merumuskan kebijakan <i>data science</i> di bidang keamanan siber. | | |
| 15. Investigasi Siber | 5 | Merumuskan strategi, rekomendasi kebijakan, investigasi di bidang keamanan siber dan/atau persandian. | 5.1 Mampu merumuskan strategi investigasi di bidang keamanan siber dan/atau persandian; 5.2 Mampu merumuskan rekomendasi investigasi di bidang keamanan siber, dan/atau persandian; 5.3 Mampu merumuskan kebijakan investigasi di bidang keamanan siber, dan/atau persandian. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi | | | |

| | | Pembina | | | |
|--------------|---------------|---|--|---|--|
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Computer Forensic Analysis</i> | | X | |
| | | e. Pelatihan <i>Smartphone/Mobile Forensic Analysis</i> | | X | |
| | | f. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| | | g. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| | | h. Pelatihan <i>Anti-Forensic Analysis</i> | | X | |

| | | | | |
|---------------------|--|---------------------------|---|---|
| | i. Pelatihan <i>Media Digital Forensic Analysis</i> | | X | |
| | j. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| | k. Pelatihan <i>Cryptocurrency Forensic Analysis</i> | | X | |
| | l. Pelatihan <i>IoT Forensic Analysis</i> | | X | |
| | m. Pelatihan <i>Reverse-Engineering Malware</i> | | X | |
| | n. Pelatihan <i>Cloud Forensic Analysis</i> | | X | |
| | o. Pelatihan <i>Investigasi Siber</i> | | X | |
| | p. Pelatihan <i>Cyber Law Data Security and Investigation</i> | | X | |
| | q. Pelatihan <i>Incident Handling</i> | | X | |
| | r. Pelatihan <i>Threat Intelligence</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Utama | | X |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 | X | | |

| | | | | |
|------------------------------|--|--|--|--|
| | (dua) tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Madya | | | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian | | | |

c. Fungsi Penanggulangan dan Pemulihan

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI UTAMA | | | |
|---|---|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi penanggulangan dan pemulihan dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan CSIRT, manajemen insiden siber, manajemen krisis siber, dan frensik digital. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi role model dalam penerapan standar keadilan dan etika di tingkat nasional. | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari |

| | | | |
|--------------|---|----------------------------------|---|
| | | | <p>yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya;</p> <p>5.2. Menjadi <i>“role model”</i> / keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional;</p> <p>5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat</p> |

| | | | |
|-------------------------|---|--|---|
| | | | untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi. |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang | 4.1. Mendorong unit kerja di tingkat instansi untuk mencapai |

| | | | |
|---------------------|---|---|---|
| | | ditetapkan atau melebihi hasil kerja sebelumnya. | kinerja yang melebihi target yang ditetapkan; 4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi; 4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi; 4.2. Menjaga agar kebijakan pelayanan publik yang |

| | | | |
|-------------------------------------|---|--|---|
| | | | <p>diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok.</p> |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | 4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu |

| | | | |
|------------------------|---|-------------------------------------|---|
| | | | <p>untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan | 4 | Menyelesaikan | 4.1. Menyusun dan/atau |

| | | | |
|---------------------------|---|---|--|
| keputusan | | masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi; 4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain; 4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | 5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri; 5.2. Mampu mengkomunikasikan |

| | | | |
|---|---|---|---|
| | | | <p>dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik yang berdampak positif secara nasional.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan manajemen keamanan siber dan persandian. | <p>5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian;</p> <p>5.2 mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> |

| | | | |
|---------------------------------------|---|--|---|
| | | | 5.3 mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian. |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | <p>5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implementasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.2 Mampu menyusun buku, pedoman, petunjuk pelaksanaan, petunjuk teknis perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan</p> |

| | | | |
|-----------------------|---|---|---|
| | | | <p><i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi.</p> |
| 12. Pengelolaan CSIRT | 5 | Mampu mengembangkan konsep, teori, kebijakan, dan menjadikannya sebagai standar acuan bagi pembangunan kapasitas CSIRT. | <p>5.1 Mampu mengembangkan konsep, teknik, atau kebijakan baru terkait asistensi CSIRT;</p> <p>5.2 Mampu mengembangkan konsep, teknik, atau kebijakan baru dalam kegiatan pembangunan kapasitas CSIRT untuk melakukan penanggulangan dan pemulihan insiden keamanan siber;</p> <p>5.3 Mampu perumusan rekomendasi atas kesiapan CSIRT dalam melakukan penanggulangan dan pemulihan insiden keamanan siber;</p> <p>5.4 Mampu perumusan</p> |

| | | | |
|-----------------------------|---|--|---|
| | | | rekomendasi terhadap atas kematangan CSIRT. |
| 13. Manajemen Insiden Siber | 5 | Mampu mengembangkan konsep, teori, kebijakan, teknik metode dan analisa manajemen insiden siber. | <p>5.1 Mampu mengembangkan kebijakan, rencana, dan strategi sesuai dengan hukum, peraturan, kebijakan, dan standar manajemen insiden siber;</p> <p>5.2 Mengidentifikasi, menganalisis, teori, konsep, kebijakan manajemen insiden siber, menemukan kelebihan dan kekurangan perbaikannya;</p> <p>5.3 Mengembangkan teori, konsep dan kebijakan terkait Manajemen Insiden Siber, meyakinkan unit kerja terkait di BSSN dan <i>stakeholder</i> untuk menerima konsep, terori dan kebijakan yang dikembangkan;</p> <p>5.4 Menjadi mentor dan sumber rujukan utama (nasional) dalam implementasi manajemen insiden siber.</p> |

| | | | |
|----------------------------|---|---|---|
| 14. Manajemen Krisis Siber | 5 | mampu mengembangkan konsep, teori, kebijakan, teknik metode dan analisa manajemen krisis siber. | <p>5.1 Mampu mengembangkan kebijakan, rencana, dan strategi sesuai dengan hukum, peraturan, kebijakan, dan standar manajemen krisis siber;</p> <p>5.2 Mengidentifikasi, menganalisis, teori, konsep, kebijakan manajemen krisis siber, menemukan kelebihan dan kekurangan perbaikannya;</p> <p>5.3 Mengembangkan teori, konsep dan kebijakan terkait manajemen krisis siber, meyakinkan unit kerja terkait di BSSN dan <i>stakeholder</i> untuk menerima konsep, terori dan kebijakan yang dikembangkan;</p> <p>5.4 Menjadi mentor dan sumber rujukan utama (nasional) dalam implementasi manajemen krisis siber.</p> |
| 15. Forensik Digital | 5 | Merumuskan keterangan ahli, rekomendasi dan | 5.1 mampu merumuskan keterangan sebagai ahli forensik digital; |

| | | kebijakan di bidang Forensik Digital. | 5.2 mampu merumuskan rekomendasi forensik digital; 5.3 mampu merumuskan kebijakan di bidang forensik digital. | | |
|---------------------------------|----------------|--|--|---------|-------|
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan | | X | |



| | | | |
|---|--|---|--|
| Persandian | | | |
| c. Pelatihan Kebijakan Keamanan Siber | | X | |
| d. Pelatihan Audit Keamanan Siber | | X | |
| e. Pelatihan CEH | | X | |
| f. Pelatihan <i>Management CSIRT</i> | | X | |
| g. Pelatihan Manajemen Insiden Siber | | X | |
| h. Pelatihan <i>Incident Handling</i> | | X | |
| i. Pelatihan <i>Log Analysis</i> | | X | |
| j. Pelatihan <i>Network Security</i> | | X | |
| k. Pelatihan <i>Artifak Handling</i> | | X | |
| l. Pelatihan <i>Disaster Recovery</i> | | X | |
| m. Pelatihan <i>Malware Forensic Analysis</i> | | X | |
| n. Pelatihan <i>Computer</i> | | X | |

| | | | | | |
|---------------------|---|--|---|---|--|
| | | <i>Forensic Analysis</i> | | | |
| | | o. Pelatihan <i>Smartphone/ Mobile Forensic Analysis</i> | | X | |
| | | p. Pelatihan <i>Digital Storage Forensic Analysis</i> | | X | |
| | | q. Pelatihan <i>Network Forensic Analysis</i> | | X | |
| | | r. Pelatihan Investigasi Siber | | X | |
| | | s. Pelatihan <i>Cyber Crisis Management Planning</i> | | X | |
| | | t. Pelatihan DFIR (<i>Digital Forensic for Incident Responder</i>) | | X | |
| | 3. Fungsional | Fungsional Sandiman Utama | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian | | X | | |

| | | | | |
|------------------------------|---|--|--|--|
| | paling sedikit 2 (dua) tahun | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Madya | | | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian | | | |

d. Fungsi Identifikasi dan Deteksi

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI UTAMA | | | |
|---|---|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi identifikasi dan deteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, intelijen siber, penilaian keamanan teknologi informasi, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi role model dalam penerapan standar keadilan dan etika di tingkat nasional. | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari |

| | | | |
|--------------|---|----------------------------------|---|
| | | | <p>yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya;</p> <p>5.2. Menjadi “<i>role model</i>”/keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional;</p> <p>5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan</p> |

| | | | |
|-------------------------|---|--|---|
| | | | tercapainya sinergi dalam rangka pencapaian target kerja organisasi. |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja</p> |

| | | | |
|---------------------|---|--|---|
| | | | <p>unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |
| 5. Pelayanan publik | 4 | <p>Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional.</p> | <p>4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh</p> |

| | | | |
|-------------------------------------|---|--|---|
| | | | <p>kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok.</p> |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan</p> |

| | | | |
|--------------------------|---|---|---|
| | | | <p>balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan</p> |

| | | | |
|---------------------------|---|---|--|
| | | | dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis | <p>5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi</p> |

| | | | |
|---|---|--|--|
| | | | perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i> , sosial ekonomi, preferensi politik yang berdampak positif secara nasional. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan manajemen keamanan siber dan persandian | <p>5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian;</p> <p>5.2 Mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> <p>5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | <p>5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implemetasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.2 Mampu menyusun buku, pedoman, petunjuk pelaksanaan, petunjuk teknis</p> |

| | | | |
|------------------------------------|---|--|---|
| | | | <p>perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan <i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi.</p> |
| 12.Manajemen Risiko Keamanan Siber | 5 | Menciptakan dan mengkreasikan sesuatu berhubungan dengan manajemen risiko. | <p>5.1 Mampu menyusun metodologi manajemen risiko keamanan informasi yang tepat dan komperhensif;</p> <p>5.2 Mampu merancang <i>framework</i> manajemen risiko keamanan</p> |

| | | | |
|--|---|---|--|
| | | | <p>informasi;</p> <p>5.3 Mampu merumuskan rekomendasi manajemen risiko keamanan informasi secara nasional baik untuk sektor pemerintah, infrastruktur kritis maupun private;</p> <p>5.4 Mampu merumuskan strategi manajemen risiko keamanan informasi secara nasional.</p> |
| 13. Penilaian Keamanan Teknologi Informasi | 5 | Mampu merancang pelaksanaan penilaian keamanan teknologi informasi. | <p>5.1 Mampu merumuskan rekomendasi pengamanan teknologi informasi secara nasional;</p> <p>5.2 Mampu mengembangkan teknik, dan metode pelaksanaan penilaian keamanan teknologi informasi;</p> <p>5.3 Mampu merancang strategi kerjasama pertukaran informasi hasil penilaian keamanan teknologi informasi tingkat regional, bilateral atau multilateral;</p> <p>5.4 Mampu merancang strategi kerjasama</p> |

| | | | |
|---|---|--|---|
| | | | pertukaran informasi hasil penilaian keamanan teknologi informasi tingkat nasional. |
| 14. Intelijen Siber | 5 | Mampu merancang pelaksanaan intelijen siber. | <p>5.1 Mampu memberikan rekomendasi taktis, operasional dan strategis;</p> <p>5.2 Mampu mengembangkan teknik, dan metode pelaksanaan intelijen siber;</p> <p>5.3 Mampu merumuskan rekomendasi keamanan informasi, keamanan siber, dan persandian secara nasional.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 5 | Mampu merancang pelaksanaan <i>monitoring</i> keamanan jaringan. | <p>5.1 Mampu merancang implementasi pengamanan jaringan secara nasional;</p> <p>5.2 Mampu merancang strategi kerjasama pertukaran informasi hasil <i>monitoring</i> keamanan jaringan tingkat regional, bilateral;</p> <p>5.3 Mampu merancang strategi kerjasama pertukaran informasi hasil <i>monitoring</i> keamanan jaringan tingkat nasional;</p> |

| | | | 5.4 Mampu mengembangkan kebijakan pengamanan jaringan secara nasional; | | |
|---------------------------------|----------------|--|--|---------|-------|
| | | | 5.5 Mampu menilai kebijakan pengamanan jaringan secara nasional. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X | |
| | | b. Pelatihan Pengembangan Diri | | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | | X | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | | x | |
| | | b. Pelatihan | | X | |

| |
|--|
| |
|--|

| | | | |
|--|--|---|--|
| Manajemen Keamanan Siber dan Persandian | | | |
| c. Pelatihan Kebijakan Keamanan Siber | | X | |
| d. Pelatihan <i>Penetration Testing</i> | | X | |
| e. Pelatihan <i>Vulnerability Assessment</i> | | X | |
| f. Pelatihan <i>Secure Software Development</i> | | X | |
| g. Pelatihan Audit Keamanan Informasi | | X | |
| h. Pelatihan Arsitektur Keamanan Sistem | | X | |
| i. Pelatihan <i>Global Industrial Security/ SCADA</i> | | X | |
| j. Pelatihan Keamanan Jaringan | | X | |
| k. Pelatihan Investigasi | | X | |

| | | | | | |
|---------------------|--|--|--|---|--|
| | | Intelijen Siber | | | |
| | | l. Pelatihan <i>Cyber Threat Intelligence</i> | | X | |
| | | m. Pelatihan <i>Analysis Malware</i> | | X | |
| | | n. Pelatihan Kontra Penginderaan | | X | |
| | | o. Pelatihan <i>System Security</i> | | X | |
| | | p. Pelatihan <i>Cyberwarfare</i> | | X | |
| | | q. Pelatihan <i>Social Engineering</i> | | X | |
| | 3. Fungsional | Fungsional Sandiman Madya | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) | X | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Madya | | | | |

| | |
|------------------------------|--|
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian |

e. Fungsi Kendali Operasi Keamanan Siber

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI UTAMA | | | |
|--|---|---|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi kendali operasi keamanan siber dengan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, pengelolaan <i>security operation center</i> (SOC), pengelolaan pusat kontak siber nasional, manajemen insiden siber, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi <i>role model</i> dalam penerapan standar keadilan dan etika di tingkat nasional. | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya; |

| | | | |
|---------------|---|---|---|
| | | | <p>5.2. Menjadi “<i>role model</i>”/keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional;</p> <p>5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi | 4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk |

| | | | |
|-------------------------|---|--|---|
| | | secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangkai meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |

| | | | |
|---------------------|---|---|--|
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | <p>4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/keompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar</p> |
|---------------------|---|---|--|

| | | | |
|-------------------------------------|---|--|--|
| | | | objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelempok. |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | 4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin |

| | | | |
|---------------------------|---|---|--|
| | | | <p>terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko).</p> |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | 5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN |

| | | | |
|---|---|---|---|
| | | | <p>dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik yang berdampak positif secara nasional.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan Manajemen keamanan siber dan persandian. | <p>5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian;</p> <p>5.2 Mampu merumuskan kebijakan Manajemen Keamanan siber dan</p> |

| | | | |
|---------------------------------------|---|---|---|
| | | | <p>persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> <p>5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mampu mengembangkan konsep, kebijakan advokasi yang sinergis dan terintegrasi yang berdampak nasional atau internasional. | <p>5.1 Mampu mengembangkan konsep, kebijakan, teknik metode advokasi kebijakan keamanan siber, <i>monitoring</i>, dan evaluasi kebijakan keamanan siber</p> <p>5.2 Mampu mengembangkan strategi advokasi kebijakan, sinkronisasi, dan koordinasi implementasi kebijakan yang terintegrasi dan saling melengkapi (komplementer) dengan kebijakan lain yang dapat memberi dampak positif di tingkat nasional atau internasional;</p> <p>5.3 Mampu menjadi mentor dan rujukan nasional dalam pemecahan masalah advokasi kebijakan.</p> |

| | | | |
|--|---|--|---|
| 12. Pengelolaan <i>Security Operation Center</i> (SOC) | 5 | Mengembangkan pengelolaan SOC. | <p>5.1 Mampu menyusun kebijakan pengelolaan SOC;</p> <p>5.2 Mampu merumuskan kajian kebijakan pengelolaan SOC;</p> <p>5.3 Mampu menyusun strategi implementasi terkait pengelolaan SOC;</p> <p>5.4 Mampu mengembangkan infrastruktur/perangkat <i>/tools engineering</i> yang digunakan dalam operasional SOC.</p> |
| 13. Manajemen Insiden Siber | 5 | Mampu mengembangkan konsep, teori, kebijakan, teknik metode dan analisa manajemen insiden siber. | <p>5.1 Mampu mengembangkan kebijakan, rencana, dan strategi sesuai dengan hukum, peraturan, kebijakan, dan standar manajemen insiden siber;</p> <p>5.2 Mengidentifikasi, menganalisis, teori, konsep, kebijakan manajemen insiden siber, menemukan kelebihan dan kekurangan perbaikannya;</p> <p>5.3 Mengembangkan teori, konsep dan kebijakan terkait Manajemen Insiden Siber, meyakinkan unit kerja</p> |

| | | | |
|---|---|--|---|
| | | | <p>terkait di BSSN dan <i>stakeholder</i> untuk menerima konsep, teori dan kebijakan yang dikembangkan;</p> <p>5.4 Menjadi mentor dan sumber rujukan utama (nasional) dalam implementasi manajemen insiden siber.</p> |
| 14. Pengelolaan Pusat Kontak Siber Nasional | 5 | Mengembangkan pengelolaan pusat kontak siber. | <p>5.1 Mampu merumuskan kajian kebijakan pengelolaan pusat kontak siber;</p> <p>5.2 Mampu menyusun kebijakan pengelolaan pusat kontak siber;</p> <p>5.3 Mampu menyusun strategi implementasi terkait pengelolaan pusat kontak siber.</p> |
| 15. <i>Monitoring</i> Keamanan Jaringan | 5 | Mampu merancang pelaksanaan <i>monitoring</i> keamanan jaringan. | <p>5.1 Mampu merancang implementasi pengamanan jaringan secara nasional;</p> <p>5.2 Mampu merancang strategi kerjasama pertukaran informasi hasil <i>monitoring</i> keamanan jaringan tingkat regional, bilateral;</p> <p>5.3 Mampu merancang strategi kerjasama pertukaran informasi</p> |

| | | | hasil <i>monitoring</i> keamanan jaringan tingkat nasional; | | |
|--------------------------|----------------|--|--|-------|---|
| | | | 5.4 Mampu mengembangkan kebijakan pengamanan jaringan secara nasional; | | |
| | | | 5.5 Mampu menilai kebijakan pengamanan jaringan secara nasional. | | |
| III. PERSYARATAN JABATAN | | | | | |
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | | |
| | | Mutlak | Penting | Perlu | |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan pengembangan diri | | X | |
| | | b. Pelatihan budaya integritas dan anti korupsi | | X | |
| | | c. Pelatihan pelayanan prima | | X | |
| | 2. Teknis | a. Pelatihan manajemen risiko siber | | | X |
| | | b. Pelatihan | | | X |

| | | | | | |
|--|---------------------|---|---|---|---|
| | | manajemen keamanan siber dan persandian | | | |
| | | c. Pelatihan kebijakan keamanan siber | | X | |
| | | d. Pelatihan <i>Automation and Continuous Security Monitoring</i> | | | X |
| | | e. Pelatihan <i>cyber threat intelligence analysis</i> | | | X |
| | | f. Pelatihan manajemen insiden | | | X |
| | | g. Pelatihan <i>Cyber Defence Evaluation</i> | | X | |
| | | h. Pelatihan <i>System Test and Evaluation</i> | | | X |
| | | i. Pelatihan arsitektur keamanan jaringan | | | X |
| | 3. Fungsional | Fungsional Sandiman Utama | | X | |
| | C. Pengalaman Kerja | a. Memiliki | X | | |

| | | | | |
|------------------------------|--|--|--|--|
| | pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun b. Telah menduduki Jabatan Sandiman Ahli Madya | | | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian | | | |

f. Fungsi Pengkajian

| | | |
|-------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNSIONAL SANDIMAN AHLI UTAMA | |
|--|--|
| I. IKHTISAR JABATAN | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi pengkajian dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, rekayasa kriptografi, rancang bangun perangkat keamanan teknologi informasi, pengkajian teknologi keamanan siber dan sandi, |

| | | pengelolaan penelitian teknologi keamanan siber dan sandi negara. | |
|-------------------------------|-------|--|--|
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi role model dalam penerapan standar keadilan dan etika di tingkat nasional. | <p>5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya;</p> <p>5.2. Menjadi "role model" / keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional;</p> <p>5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan norma-norma yang sejalan dengan nilai strategis organisasi.</p> |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target</p> |

| | | | |
|-------------------------|---|---|---|
| | | | <p>kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | <p>Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan.</p> | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | <p>Mendorong unit kerja mencapai target yang</p> | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang</p> |

| | | | |
|---------------------|---|---|--|
| | | ditetapkan atau melebihi hasil kerja sebelumnya. | melebihi target yang ditetapkan; 4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi; 4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi. |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional. | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi; 4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, |

| | | | |
|-------------------------------------|---|--|--|
| | | | <p>netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh kepentingan pribadi/kelompok.</p> |
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan</p> |

| | | | |
|--------------------------|---|---|---|
| | | | <p>umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara aktif di lingkup unit kerjanya secara berkala;</p> <p>4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja.</p> |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | <p>4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi;</p> <p>4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain;</p> <p>4.3. Membuat keputusan dan mengantisipasi dampak</p> |

| | | | |
|---------------------------|---|--|---|
| | | | keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | <p>5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial</p> |

| | | | |
|---|---|--|---|
| | | | ekonomi, preferensi politik yang berdampak positif secara nasional. |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan manajemen keamanan siber dan persandian. | <p>5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian;</p> <p>5.2 Mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> <p>5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | <p>5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implementasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.2 Mampu menyusun buku, pedoman, petunjuk pelaksanaan, petunjuk teknis perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> |

| | | | |
|-------------------------|---|---|---|
| | | | <p>5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan <i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi.</p> |
| 12.Rekayasa Kriptografi | 5 | Membangun dan mengembangkan algoritme/protokol / manajemen kunci kriptografi. | <p>5.1 Mampu merumuskan <i>grand design</i> implementasi hasil Pengkajian Teknologi keamanan siber dan sandi;</p> <p>5.2 Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi;</p> <p>5.3 Mampu merancang desain algoritme/protokol/mana jemen kunci kriptografi.</p> |

| | | | |
|--|---|--|---|
| 13. Rancang Bangun Perangkat Keamanan Teknologi Informasi | 5 | Membangun perangkat keamanan TI. | 5.1 Mampu merumuskan <i>grand design</i> implementasi hasil Pengkajian Teknologi keamanan siber dan sandi; 5.2 Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi; 5.3 Mampu merancang desain perangkat keamanan TI. |
| 14. Pengkajian Teknologi Keamanan Siber dan Sandi | 5 | Mengembangkan hasil pengkajian teknologi keamanan siber dan sandi. | 5.1 Mampu merumuskan <i>grand design</i> implementasi hasil pengkajian teknologi keamanan siber dan sandi; 5.2 Mampu merumuskan kebijakan strategis implementasi hasil kajian teknologi keamanan siber dan sandi; |
| 15. Pengelolaan Penelitian Teknologi Keamanan Siber dan Sandi Negara | 5 | Mengembangkan konsep, teori, atau kebijakan terkait penelitian teknologi keamanan siber dan sandi. | 5.1 Mampu merekomendasikan strategi kerjasama kemitraan penelitian; 5.2 Mampu mengajar (edukasi/ literasi) keamanan siber dan sandi; |
| III. PERSYARATAN JABATAN | | | |
| Jenis Persyaratan | | Uraian | Tingkat pentingnya terhadap jabatan |

| | | Mutlak | Penting | Perlu |
|---------------|----------------|--|---------|-------|
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | |
| B. xPelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | X | |
| | | b. Pelatihan Pengembangan Diri | X | |
| | | c. Pelatihan Budaya Integritas dan Anti Korupsi | X | |
| | | d. Pelatihan Teknik Komunikasi | X | |
| | 2. Teknis | a. Pelatihan Manajemen Risiko Siber | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | X | |
| | | d. Pelatihan Algoritma Kriptografi | X | |
| | | e. Pelatihan | X | |
| | | | | |

| |
|--|
| |
|--|

| | | | |
|---|--|---|--|
| Desain Protokol Kriptografi | | | |
| f. Pelatihan Desain Manajemen Kunci | | X | |
| g. Pelatihan Infrastruktur Kunci Publik | | X | |
| h. Pelatihan Protokol Kriptografi | | X | |
| i. Pelatihan Bahasa Pemrograman | | X | |
| j. Pelatihan Steganografi | | X | |
| k. Pelatihan <i>Embedded System</i> | | X | |
| l. Pelatihan Perancangan Piranti Lunak | | X | |
| m. Pelatihan Perancangan Piranti Keras | | X | |
| n. Pelatihan Kripanalisis | | X | |
| o. Pelatihan Steganalisis | | X | |
| p. Pelatihan Manajemen Proyek | | X | |
| q. Pelatihan <i>Software</i> | | X | |

| | | | | | |
|------------------------------|--|--|--|---|--|
| | | <i>Testing</i> | | | |
| | | r. Pelatihan <i>Hardware Testing</i> | | X | |
| | | s. Pelatihan Desain Keamanan Jaringan | | X | |
| | 3. Fungsional | Fungsional Sandiman Utama | | X | |
| C. Pengalaman Kerja | | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | | X | |
| | | b. Telah menduduki Jabatan Sandiman Ahli Madya | | X | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | | |
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian | | | | |

g. Fungsi Proteksi

| | | |
|------------------|---|---------------------|
| Nama Jabatan | : | Sandiman Ahli Utama |
| Kelompok Jabatan | : | Jabatan Fungsional |

| | | |
|-------------------|---|--|
| Urusan Pemerintah | : | |
| Kode Jabatan | : | |

| JABATAN FUNGSIONAL SANDIMAN AHLI UTAMA | | | |
|---|---|--|---|
| I. IKHTISAR JABATAN | | | |
| Ikhtisar Jabatan | Melaksanakan kegiatan keamanan siber, keamanan informasi, dan persandian di tataran strategis nasional dengan menjalankan fungsi proteksi dengan melakukan manajemen keamanan siber dan persandian, advokasi kebijakan keamanan siber, manajemen risiko keamanan siber, audit keamanan informasi, penyediaan layanan keamanan informasi, dan <i>monitoring</i> keamanan jaringan. | | |
| II. STANDAR KOMPETENSI | | | |
| Kompetensi | Level | Deskripsi | Indikator Kompetensi |
| A. Manajerial | | | |
| 1. Integritas | 5 | Mampu menjadi role model dalam penerapan standar keadilan dan etika di tingkat nasional. | 5.1. Mempertahankan tingkat standar keadilan dan etika yang tinggi dalam perkataan dan tindakan sehari-hari yang dipatuhi oleh seluruh pemangku kepentingan pada lingkup instansi yang dipimpinnya; 5.2. Menjadi "role model" / keteladanan dalam penerapan standar keadilan dan etika yang tinggi di tingkat nasional; 5.3. Membuat konsep kebijakan dan strategi penerapan sikap integritas dalam pelaksanaan tugas dan |

| | | | |
|---------------|---|--|---|
| | | | norma-norma yang sejalan dengan nilai strategis organisasi. |
| 2. Kerjasama | 4 | Membangun komitmen tim, sinergi. | <p>4.1. Membangun sinergi antar unit kerja di lingkup instansi yang dipimpin;</p> <p>4.2. Memfasilitasi kepentingan yang berbeda dari unit kerja lain sehingga tercipta sinergi dalam rangka pencapaian target kerja organisasi;</p> <p>4.3. Mengembangkan sistem yang menghargai kerja sama antar unit, memberikan dukungan/semangat untuk memastikan tercapainya sinergi dalam rangka pencapaian target kerja organisasi.</p> |
| 3. Komunikasi | 4 | Mampu mengemukakan pemikiran multidimensi secara lisan dan tertulis untuk mendorong kesepakatan dengan tujuan meningkatkan kinerja secara keseluruhan. | <p>4.1. Mengintegrasikan informasi-informasi penting hasil diskusi dengan pihak lain untuk mendapatkan pemahaman yang sama;</p> <p>4.2. Berbagi informasi dengan pemangku kepentingan untuk tujuan meningkatkan kinerja secara keseluruhan;</p> |

| | | | |
|-------------------------|---|---|--|
| | | | <p>4.3. Menuangkan pemikiran/konsep yang multidimensi dalam bentuk tulisan formal;</p> <p>4.4. Menyampaikan informasi secara persuasif untuk mendorong pemangku kepentingan sepakat pada langkah-langkah bersama dengan tujuan meningkatkan kinerja secara keseluruhan.</p> |
| 4. Orientasi pada hasil | 4 | Mendorong unit kerja mencapai target yang ditetapkan atau melebihi hasil kerja sebelumnya. | <p>4.1. Mendorong unit kerja di tingkat instansi untuk mencapai kinerja yang melebihi target yang ditetapkan;</p> <p>4.2. Memantau dan mengevaluasi hasil kerja unitnya agar selaras dengan sasaran strategis instansi;</p> <p>4.3. Mendorong pemanfaatan sumber daya bersama antar unit kerja dalam rangka meningkatkan efektivitas dan efisiensi pencapaian target organisasi.</p> |
| 5. Pelayanan publik | 4 | Mampu memonitor, mengevaluasi, memperhitungkan dan mengantisipasi dampak dari isu-isu jangka panjang, | 4.1. Memahami dan memberi perhatian kepada isu-isu jangka panjang, kesempatan atau kekuatan politik yang mempengaruhi |

| | | | |
|--|--|--|---|
| | | <p>kesempatan, atau kekuatan politik dalam hal pelayanan kebutuhan pemangku kepentingan yang transparan, objektif dan profesional.</p> | <p>organisasi dalam hubungannya dengan dunia luar, memperhitungkan dan mengantisipasi dampak terhadap pelaksanaan tugas-tugas pelayanan publik secara obyektif, transparan, dan profesional dalam lingkup organisasi;</p> <p>4.2. Menjaga agar kebijakan pelayanan publik yang diselenggarakan oleh instansinya telah selaras dengan standar pelayanan yang objektif, netral, tidak memihak, tidak diskriminatif, serta tidak terpengaruh kepentingan pribadi/kelompok/partai politik;</p> <p>4.3. Menerapkan strategi jangka panjang yang berfokus pada pemenuhan kebutuhan pemangku kepentingan dalam menyusun kebijakan dengan mengikuti standar objektif, netral, tidak memihak, tidak diskriminatif, transparan, tidak terpengaruh</p> |
|--|--|--|---|

| | | | kepentingan pribadi/kelompok. |
|-------------------------------------|---|--|--|
| 6. Pengembangan diri dan orang lain | 4 | Menyusun program jangka pengembangan jangka panjang dalam rangka mendorong manajemen pembelajaran. | <p>4.1. Menyusun program pengembangan jangka panjang bersama-sama dengan bawahan, termasuk didalamnya penetapan tujuan, bimbingan, penugasan dan pengalaman lainnya, serta mengalokasikan waktu untuk mengikuti pelatihan/ pendidikan/ pengembangan kompetensi dan karir;</p> <p>4.2. Melaksanakan manajemen pembelajaran termasuk evaluasi dan umpan balik pada tataran organisasi;</p> <p>4.3. Mengembangkan orang-orang disekitarnya secara konsisten, melakukan kaderisasi untuk posisi-posisi di unit kerjanya.</p> |
| 7. Mengelola perubahan | 4 | Memimpin perubahan pada unit kerja. | <p>4.1. Mengarahkan unit kerja untuk lebih siap dalam menghadapi perubahan termasuk memitigasi risiko yang mungkin terjadi;</p> <p>4.2. Memastikan perubahan sudah diterapkan secara</p> |

| | | | |
|---------------------------|---|---|---|
| | | | aktif di lingkup unit kerjanya secara berkala; 4.3. Memimpin dan memastikan penerapan program-program perubahan selaras antar unit kerja. |
| 8. Pengambilan keputusan | 4 | Menyelesaikan masalah yang mengandung risiko tinggi, mengantisipasi dampak keputusan, membuat tindakan pengamanan; mitigasi risiko. | 4.1. Menyusun dan/atau memutuskan konsep penyelesaian masalah yang melibatkan beberapa/seluruh fungsi dalam organisasi; 4.2. Menghasilkan solusi dari berbagai masalah yang kompleks, terkait dengan bidang kerjanya yang berdampak pada pihak lain; 4.3. Membuat keputusan dan mengantisipasi dampak keputusannya serta menyiapkan tindakan penanganannya (mitigasi risiko). |
| B. Sosial Kultural | | | |
| 9. Perekat Bangsa | 5 | Wakil pemerintah untuk membangun hubungan sosial psikologis. | 5.1. Menjadi wakil pemerintah yang mampu membangun hubungan sosial psikologis dengan masyarakat sehingga menciptakan kelekatan yang kuat antara ASN dan para pemangku kepentingan serta |

| | | | |
|---|---|---|---|
| | | | <p>diantara para pemangku kepentingan itu sendiri;</p> <p>5.2. Mampu mengkomunikasikan dampak risiko yang teridentifikasi dan merekomendasikan tindakan korektif berdasarkan pertimbangan perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik untuk membangun hubungan jangka panjang;</p> <p>5.3. Mampu membuat kebijakan yang mengakomodasi perbedaan latar belakang, agama/kepercayaan, suku, <i>gender</i>, sosial ekonomi, preferensi politik yang berdampak positif secara nasional.</p> |
| C. Teknis | | | |
| 10. Manajemen Keamanan Siber dan Persandian | 5 | Merumuskan manajemen keamanan siber dan persandian. | <p>5.1 Mampu mengevaluasi kebijakan manajemen keamanan siber dan persandian;</p> <p>5.2 Mampu merumuskan kebijakan manajemen keamanan siber dan persandian yang lugas</p> |

| | | | |
|---------------------------------------|---|--|--|
| | | | <p>dan jelas untuk menghindari <i>dispute</i> dalam penafsiran;</p> <p>5.3 Mampu merumuskan saran perbaikan guna menutup celah dalam manajemen keamanan siber dan persandian.</p> |
| 11. Advokasi Kebijakan Keamanan Siber | 5 | Mengembangkan teori, konsep, penyusunan, implementasi dan <i>monitoring</i> evaluasi kebijakan keamanan informasi. | <p>5.1 Mengembangkan teori, konsep, teknik, metode tahapan perumusan kebijakan, implemetasi kebijakan, dan/atau <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.2 Mampu menyusun buku, pedoman, petunjuk pelaksanaan, petunjuk teknis perumusan dan penyusunan, implementasi, <i>monitoring</i> dan evaluasi kebijakan keamanan informasi;</p> <p>5.3 Menjadi sumber rujukan utama dan mentor (nasional) dalam penyusunan kebijakan, implementasi kebijakan, <i>monitoring</i> dan evaluasi kebijakan, serta pemecahan masalah dalam penyusunan, penerapan dan</p> |

| | | | |
|-------------------------------------|---|--|---|
| | | | <p><i>monitoring</i> evaluasi kebijakan pengelolaan sumber daya dan perangkat keamanan informasi, penyelenggaraan keamanan informasi, penatakelolaan aplikasi keamanan informasi, dan/atau pengelolaan keamanan informasi.</p> |
| 12. Manajemen Risiko Keamanan Siber | 5 | Menciptakan dan mengkreasikan sesuatu berhubungan dengan manajemen risiko. | <p>5.1 Mampu menyusun metodologi manajemen risiko keamanan informasi yang tepat dan komperhensif;</p> <p>5.2 Mampu merancang <i>framework</i> manajemen risiko keamanan informasi;</p> <p>5.3 Mampu merumuskan rekomendasi manajemen risiko keamanan informasi secara nasional baik untuk sektor pemerintah, infrastruktur kritis maupun private;</p> <p>5.4 Mampu merumuskan strategi manajemen risiko keamanan informasi secara nasional.</p> |
| 13. Audit Keamanan | 5 | Merumuskan konsep kebijakan | 5.1 Mampu menyusun kebijakan dan standar |

| | | | |
|---|---|---|--|
| Informasi | | dan standar sebagai acuan pelaksanaan audit keamanan informasi, keamanan siber, dan persandian. | audit keamanan informasi, keamanan siber, dan persandian; 5.2 Mampu merumuskan kajian kebijakan dan standar audit keamanan informasi, keamanan siber, dan persandian; 5.3 Mampu menyusun strategi implementasi terkait audit keamanan informasi, keamanan siber, dan persandian. |
| 14. Penyediaan Layanan Keamanan Informasi | 5 | Merumuskan kebijakan dan strategi penyediaan layanan keamanan informasi. | 5.1 Mampu mengembangkan kebijakan penyelenggaraan layanan keamanan informasi; 5.2 Mampu merumuskan kebijakan penyediaan layanan keamanan informasi; 5.3 Mampu menyusun strategi implementasi layanan keamanan informasi. |
| 15. <i>Monitoring</i> Keamanan Jaringan | 5 | Mampu merancang pelaksanaan <i>monitoring</i> keamanan jaringan. | 5.1 Mampu merancang implementasi pengamanan jaringan secara nasional; 5.2 Mampu merancang strategi kerjasama pertukaran informasi hasil <i>monitoring</i> |

| | | | keamanan jaringan tingkat regional, bilateral; | |
|--------------------------|----------------|--|---|-------|
| | | | 5.3 Mampu merancang strategi kerjasama pertukaran informasi hasil <i>monitoring</i> keamanan jaringan tingkat nasional; | |
| | | | 5.4 Mampu mengembangkan kebijakan pengamanan jaringan secara nasional; | |
| | | | 5.5 Mampu menilai kebijakan pengamanan jaringan secara nasional. | |
| III. PERSYARATAN JABATAN | | | | |
| Jenis Persyaratan | Uraian | Tingkat pentingnya terhadap jabatan | | |
| | | Mutlak | Penting | Perlu |
| A. Pendidikan | 1. Jenjang | Berijazah paling rendah S-2 | | |
| | 2. Bidang Ilmu | Komputer, Matematika, Teknik atau Rekayasa Komputer, Teknik atau Rekayasa Elektro, Persandian, Forensik Digital atau bidang lain yang ditetapkan oleh Instansi Pembina | | |
| B. Pelatihan | 1. Manajerial | a. Pelatihan Pelayanan Prima | | X |
| | | b. Pelatihan Pengembangan Diri | | X |
| | | c. Pelatihan Budaya | | X |

| | | | | | |
|--|-----------|--|--|---|--|
| | 2. Teknis | Integritas dan Anti Korupsi | | | |
| | | d. Pelatihan Teknik Komunikasi | | X | |
| | | a. Pelatihan Manajemen Risiko Siber | | X | |
| | | b. Pelatihan Manajemen Keamanan Siber dan Persandian | | X | |
| | | c. Pelatihan Kebijakan Keamanan Siber | | X | |
| | | d. Pelatihan <i>Secure Software Development</i> | | X | |
| | | e. Pelatihan Audit Keamanan Informasi | | X | |
| | | f. Pelatihan Arsitektur Keamanan Sistem | | X | |
| | | g. Pelatihan <i>Global Industrial Security/SCADA</i> | | X | |
| | | h. Pelatihan Keamanan | | X | |

| | | | | | |
|---------------------|---|--|--|---|--|
| | | Jaringan | | | |
| | | i. Pelatihan Kontra Penginderaan | | X | |
| | | j. Pelatihan Keamanan Sistim Informasi | | X | |
| | | k. Pelatihan Peralatan Keamanan Siber dan Persandian | | X | |
| | | l. Pelatihan Diplomasi Siber | | X | |
| | 3. Fungsional | Fungsional Sandiman Utama | | X | |
| C. Pengalaman Kerja | a. Memiliki pengalaman di bidang keamanan informasi, keamanan siber, dan persandian paling sedikit 2 (dua) tahun | X | | | |
| | b. Telah menduduki Jabatan Sandiman Ahli Madya | | | | |
| D. Pangkat | IV/d (Pembina Utama Madya) IV/e (Pembina Utama) | | | | |

| | |
|------------------------------|--|
| E. Indikator Kinerja Jabatan | Hasil rekomendasi keamanan informasi, keamanan siber, dan persandian |
|------------------------------|--|

MENTERI PENDAYAGUNAAN APARATUR
NEGARA DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA,

ttd.

TJAHJO KUMOLO