REGULATION OF THE PRESIDENT OF THE REPUBLIC OF INDONESIA
NUMBER 47 OF 2023
ON
NATIONAL CYBER SECURITY STRATEGY AND CYBER CRISIS MANAGEMENT

BY THE BLESSINGS OF ALMIGHTY GOD

PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering :
a. that in order to protect the whole nation and national interests from misuse of cyber resources and to prepare early in dealing with cyber crises and recovering from cyber crises, it is necessary to realize national cyber security;
b. that technological advances have the potential to trigger cyber attacks that can cause social and economic losses, and threats to state sovereignty, so that it is necessary to prepare a cyber security strategy and cyber crisis management nationally;
c. that the establishment of a national cyber security strategy which is part of the national security strategy, including the development of a cyber security culture and the operation of emergency response handling is part of the role of the government to protect the public interest from all kinds of disturbances as an impact of the misuse of electronic information and electronic transactions that disturb public order as regulated in Government Regulation Number 71 of 2019 on Electronic System and Transaction Operations;
d. that based on the considerations as referred to in point a, point b, and, point c, it is necessary to issue a Presidential Regulation on National Cyber Security Strategy and Cyber Crisis Management;

Observing :
1. Article 4 section (1) of the 1945 Constitution of the Republic of Indonesia;
2. Government Regulation Number 71 of 2019 on Electronic System and Transaction Operations (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400);

HAS DECIDED:

To issue: PRESIDENTIAL REGULATION ON NATIONAL CYBER SECURITY STRATEGY AND CYBER CRISIS MANAGEMENT.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Presidential Regulation:

1. Cyber Security means an adaptive and innovative effort in order to protect all layers of cyberspace, including the information assets contained therein, from both technical and social cyber threats and attacks.
2. National Cyber Security Strategy means the direction of national policy in using all national cyber resources to realize Cyber Security in order to maintain and advance national interests.
3. Cyber Incident means one or a series of events that disrupt or threaten the operation of an electronic system.
4. Cyber Crisis means an emergency situation resulting from a Cyber Incident at the national level which impacts the security, integrity, and sovereignty of the state.
5. Cyber Crisis Management means the effective governance of the use of resources and handling measures that are carried out before, during, and after the Cyber Crisis.
6. Cyber Security Incident Response Team means a group of people who are responsible for handling Cyber Incidents in their defined scopes.
7. State Administering Institutions mean legislative, executive and judicial institutions at the central and regional levels and other Institutions established by legislation.
8. Stakeholders mean parties who have a role in implementing the National Cyber Security Strategy and Cyber Crisis Management.
9. Electronic System Operator (*Penyelenggara Sistem Elektronik*), hereinafter abbreviated as PSE, means any person, state administrator, business entity, and community who provides, manages, and/or operates electronic systems independently or jointly to electronic system users for their own needs and/or the needs of other parties.
10. National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*), hereinafter referred to as the Agency, means a government agency that carries out government duties in the field of cyber security and cryptography.

Article 2

The scope of this Presidential Regulation includes:

a. National Cyber Security Strategy; and
b. Cyber Crisis Management.

Article 3

The National Cyber Security Strategy and Cyber Crisis Management are references for State Administering Institutions and Stakeholders to realize cyber strength and capability in order to achieve Cyber Security stability.

Article 4

The National Cyber Security Strategy and Cyber Crisis Management aim:

a. to realize Cyber Security;
b. to protect the national digital economy ecosystem;
c. to increase the strength and capability of reliable and deterrent Cyber Security; and
d. to prioritize national interests and support the creation of an open, safe, stable, and responsible global cyberspace.

CHAPTER II
NATIONAL CYBER SECURITY STRATEGY

Article 5

The National Cyber Security Strategy consists of:

a. focus areas; and
b. national action plan of Cyber Security.

Article 6

The focus areas of the National Cyber Security Strategy as referred to in Article 5 point a consist of:

a. governance;
b. risk management;
c. preparedness and resilience;
d. strengthening of critical information infrastructure protection;
e. national cryptography autonomy;
f. increase of capability, capacity, and quality;
g. Cyber Security policy; and
h. international cooperation.

Article 7

Governance as referred to in Article 6 point a includes:

a. strengthening of the Cyber Security ecosystem including human resources, processes, and technology; and
b. increase of synergy and collaboration in the implementation of Cyber Security.

Article 8

Risk management as referred to in Article 6 point b includes:

a. optimization of risk identification, risk analysis, and risk treatment for Cyber Security;
b. increase of the effectiveness of national Cyber Security risk mitigation;
c. increase of synergy and collaboration among Stakeholders; and
d. increase of the quality of the preparation and implementation of risk-based Cyber Security policies.

Article 9

Preparedness and resilience as referred to in Article 6 point c include:

a. development of an effective and efficient Cyber Security Incident response capability;
b. formulation and determination of contingency plans for Cyber Crisis management;
c. operation of emergency response handling; and
d. strengthening of secured and highly-accessible exchange of information.

Article 10

(1) Strengthening of the critical information infrastructure protection as referred to in Article 6 point d includes:
    a. implementation of critical information infrastructure protection; and
    b. increase of the development and supervision of the operation of critical information infrastructure protection.
(2) Critical information infrastructure protection as referred to in section (1) is carried out in accordance with the provisions of legislation.

Article 11

National cryptography autonomy as referred to in Article 6 point e includes:

a. establishment of national cryptography policy;
b. enhancement of research, development, and innovation in the field of cryptography to support national development;
c. implementation of national cryptography policies to Stakeholders; and
d. establishment and development of the national cryptography industry.

Article 12

Increase of capability, capacity, and quality as referred to in Article 6 point f includes:

a. curriculum development related to Cyber Security in early childhood education, primary education, secondary education, and higher education;
b. development and implementation of human resource skill and training programs;
c. development and implementation of a coordinated and continuous Cyber Security awareness raising program;
d. strengthening of the capacity of Cyber Security technology;
e. enhancement of scientific and technological research, development, and innovation in the field of Cyber Security; and
f. development of specific programs for vulnerable sectors and groups in accordance with the needs.

Article 13

The Cyber Security Policy as referred to in Article 6 point g includes:

a. analysis and evaluation of Cyber Security policies;

b. formulation and provision of policy recommendations in the field of Cyber Security;
c. promotion of legal culture and increase of public legal awareness; and
d. law enforcement in the field of Cyber Security in an integrated manner.

Article 14

International cooperation as referred to in Article 6 point h includes:
a. establishment of policies and priorities for international cooperation in the field of Cyber Security;
b. enhancement of international cooperation initiatives in order to support the creation of a safe, peaceful, and open cyberspace as well as increase of national capacity in the field of Cyber Security;
c. increase of practical cooperation, information sharing, and best practices in dealing with Cyber Crisis; and
d. increase of Indonesia's role in bilateral, regional, and multilateral forums in the field of Cyber Security.

Article 15

(1) The national action plan of Cyber Security as referred to in Article 5 point b is a national action plan that contains planned and measurable efforts to describe and implement the focus areas of the National Cyber Security Strategy.
(2) The national action plan of Cyber Security is prepared for a period of 5 (five) years.
(3) The national action plan of Cyber Security as referred to in section (1) can be reviewed at any time.
(4) The national action plan of Cyber Security as referred to in section (1) takes into account:
    a. national development plan;
    b. development of science and technology; and
    c. strategic environment development.
(5) The national action plan of Cyber Security as referred to in section (1) contains at least:
    a. activity;
    b. success indicators;
    c. implementation time; and
    d. person in charge.
(6) The national action plan of Cyber Security as referred to in section (1) is prepared by the Agency by involving the relevant ministries/institutions.
(7) Further provisions regarding the national action plan of Cyber Security as referred to in section (1) are regulated by an Agency Regulation.

Article 16

(1) The national action plan of Cyber Security as referred to in Article 15 section (5) is obligated to be implemented by the State Administering Institutions.
(2) In implementing the national action plan of Cyber Security as referred to in section (1), State Administering Institutions can involve Stakeholders.

(3) In implementing the national action plan of Cyber Security as referred to in section (1), the Agency is responsible for:
   a. coordinating the implementation of the national action plan of Cyber Security;
   b. monitoring the implementation of the national action plan of Cyber Security;
   c. evaluating the implementation of the national action plan of Cyber Security national; and
   d. reporting the implementation results of the national action plan of Cyber Security.

(4) The implementation results of the national action plan of Cyber Security as referred to in section (3) point d are reported to the President periodically once every 1 (one) year or at any time if necessary.

CHAPTER III
CYBER CRISIS MANAGEMENT

Article 17

(1) The implementation of Cyber Crisis Management includes:
   a. before the Cyber Crisis;
   b. during the Cyber Crisis; and
   c. after the Cyber Crisis.

(2) The implementation of Cyber Crisis Management as referred to in section (1) is coordinated by the Agency by involving PSE.

Article 18

(1) In implementing the Cyber Crisis Management as referred to in Article 17, the Agency prepares:
   a. formulation of a Cyber Crisis contingency plan; and
   b. contingency plan simulation.

(2) In carrying out the preparations for the implementation as referred to in section (1), the Agency involves State Administering Institutions in formulating the Cyber Crisis contingency plan.

Article 19

Contingency plan simulation as referred to in Article 18 section (1) point b is carried out by:
a. training; and
b. role-play.

Article 20

The implementation of Cyber Crisis Management as referred to in Article 17 point a is carried out before the Cyber Crisis at least through:
a. Cyber Security Incident response;
b. Cyber Crisis early warning; and
c. determination of Cyber Crisis status.

Article 21

(1) Cyber Security Incident response as referred to in Article 20 point a is an action to respond to Cyber Security Incidents which continue to escalate and have the potential to become a crisis.
(2) The Cyber Security Incident response as referred to in section (1) is carried out in stages by the organizational Cyber Security Incident Response Team, the sectoral Cyber Security Incident Response Team, and the national Cyber Security Incident Response Team.

Article 22

(1) Cyber Crisis early warning as referred to in Article 20 point b is a warning delivered to PSE regarding an escalation of a Cyber Incident that leads to a Cyber Crisis.
(2) PSE as referred to in section (1) is obligated to follow up early warning information.

Article 23

(1) Determination of Cyber Crisis status as referred to in Article 20 point c is a determination of Cyber Security Incident situations that continue to escalate and fulfill the Cyber Crisis criteria.
(2) The Cyber Crisis status is determined by the President based on a recommendation from the Head of the Agency.
(3) Based on the determination as referred to in section (2), the President establishes a Cyber Crisis task force.

Article 24

Implementation of Cyber Crisis Management as referred to in Article 17 point b is carried out during the Cyber Crisis at least through:
a. Cyber Crisis response;
b. Cyber Crisis recovery;
c. reporting on Cyber Crisis handling; and
d. termination of Cyber Crisis status.

Article 25

Cyber Crisis Management as referred to in Article 24 point a is carried out through the following activities:
a. identification and analysis of the scope of electronic systems affected by the Cyber Crisis;
b. isolation of electronic systems affected by the Cyber Crisis;
c. collection and preservation of evidence from electronic systems affected by the Cyber Crisis;
d. investigation and eradication of the causes of the Cyber Crisis;
e. strengthening of systems that are not affected by the Cyber Crisis; and
f. coordination with Stakeholders in the context of implementing the Cyber Crisis communication protocol and controlling information to the public.

Article 26

(1) Cyber Crisis Recovery as referred to in Article 24 point b is an effort to recover affected electronic systems.
(2) The effort to recover the affected electronic system as referred to in section (1) is carried out by:
    a. restoration of affected data and systems; or
    b. the use of backup and/or alternative resources.
(3) After the effort to recover the affected electronic system as referred to in section (2), re-testing of vital functions and supporting functions is carried out to ensure that the recovery is achieved.
(4) The achieved recovery as referred to in section (2) is assessed based on:
    a. the recovery time below the maximum time limit set under the Cyber Crisis contingency plan;
    b. the amount of data recovered in accordance with the minimum amount of data set based on the Cyber Crisis contingency plan; and/or
    c. vital functions and supporting functions recovered in accordance with the minimum limits of vital functions and supporting functions determined based on the Cyber Crisis contingency plan.

Article 27

(1) The reporting on the Cyber Crisis handling as referred to in Article 24 point c is the submission of the final report on the Cyber Crisis handling from the Cyber Crisis task force to the President.
(2) The final report on the Cyber Crisis handling as referred to in section (1) contains at least:
    a. results of analysis and achievements of the Cyber Crisis handling; and
    b. follow-up recommendations for the Cyber Crisis handling.

Article 28

Termination of Cyber Crisis status as referred to in Article 24 point d is a determination of termination of Cyber Crisis status by the President based on the report of the Cyber Crisis task force.

Article 29

(1) The implementation of Cyber Crisis Management after the Cyber Crisis as referred to in Article 17 point c is carried out after the Cyber Crisis at least through:
    a. calculation of the estimated value of damage and losses due to the Cyber Crisis;
    b. calculation of estimated recovery costs due to Cyber Crisis; and
    c. evaluation of Cyber Crisis handling.
(2) The implementation after the Cyber Crisis as referred to in section (1) is coordinated by the Agency by involving PSE.

Article 30

Calculation of the estimated value of damage and losses due to the Cyber Crisis as referred to in Article 29 section (1) point a is a calculation as a replacement for the value of damaged assets and economic losses arising from temporarily damaged assets.

Article 31

The calculation of the estimated recovery costs due to the Cyber Crisis as referred to in Article 29 section (1) point b is the calculation of the estimated costs required to restore the electronic system to its initial state before the Cyber Crisis.

Article 32

(1) Evaluation of the Cyber Crisis handling as referred to in Article 29 section (1) point c is an activity to assess the process of the Cyber Crisis handling that has been carried out in accordance with the contingency plan.
(2) The results of the evaluation as referred to in section (1) will be taken into consideration in establishing Cyber Security policies.

Article 33

Further provisions regarding the implementation of Cyber Crisis Management as referred to in Article 18 to Article 32 are regulated in an Agency Regulation.

CHAPTER IV
FUNDING

Article 34

Funding for implementing the National Cyber Security Strategy and Cyber Crisis Management comes from:
a. State Budget;
b. Local Budget; and
c. other sources that are legal and non-binding in accordance with the provisions of legislation.

CHAPTER V
CLOSING PROVISION

Article 35

This Presidential Regulation comes into force on the date of its promulgation.

In order that every person may know hereof, it is ordered to promulgate this Presidential Regulation by its placement in the State Gazette of the Republic of Indonesia.

Issued in Jakarta
on 20 July 2023

PRESIDENT OF THE REPUBLIC OF INDONESIA,

signed

JOKO WIDODO

Promulgated in Jakarta
on 20 July 2023

MINISTER OF STATE SECRETARY
OF THE REPUBLIC OF INDONESIA,

signed

PRATIKNO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2023 NUMBER 99

Jakarta, 20 November 2023
Has been translated as an Official Translation
on behalf of Minister of Law and Human Rights
of the Republic of Indonesia

DIRECTOR GENERAL OF LEGISLATION,

DIREKTUR JENDERAL PERATURAN PERUNDANG-UNDANGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA PENGAYOMAN

ASEP N. MULYANA