REGULATION OF THE MINISTER OF COMMUNICATION AND DIGITAL AFFAIRS OF THE REPUBLIC OF INDONESIA

NUMBER 5 OF 2025

ON

PUBLIC SCOPE ELECTRONIC SYSTEM ORGANIZER

BY THE GRACE OF GOD ALMIGHTY

THE MINISTER OF COMMUNICATION AND DIGITAL AFFAIRS OF THE REPUBLIC OF INDONESIA,

Considering:

that in order to implement the provisions of Article 5 paragraph (3), Article 6 paragraph (4), Article 20 paragraph (7), Article 81 paragraph (4), Article 89, Article 97 paragraph (5), and Article 98 paragraph (4) of Regulation of the Government Number 71 of 2019 on the Organization of Electronic Systems and Transactions and to fulfill the regulatory needs in the implementation of public electronic systems, it has been deemed necessary to establish Regulation of the Minister of Communication and Digital Affairs on Public Scope Electronic System Organizers;

Observing:

1. Article 17 paragraph (3) of the 1945 Constitution of the Republic of Indonesia;
2. Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843) as amended several times, most recently by Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905);
3. Law Number 39 of 2008 on State Ministries (State Gazette of the Republic of Indonesia of 2008 Number 166, Supplement to the State Gazette of the Republic of Indonesia Number 4916) as amended by Law Number 61 of 2024 on the Amendment to Law Number 39 of 2008 on State Ministries (State Gazette of the Republic of Indonesia of 2024 Number 225, Supplement to the State Gazette of the Republic of Indonesia Number 6994);
4. Law Number 23 of 2014 on Regional Government (State Gazette of the Republic of Indonesia of 2014 Number 244, Supplement to the State Gazette of the Republic of Indonesia Number 5587) as amended several times, most recently by Law Number 6 of 2023 on the Stipulation of Regulation of the Government in Lieu of Law Number 2 of 2022 on Job Creation into Law (State Gazette of the Republic of Indonesia of 2023 Number 41, Supplement to the State Gazette of the Republic of Indonesia Number 6856);
5. Regulation of the Government Number 71 of 2019 on the Organization of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400);
6. Regulation of the President Number 39 of 2019 on the Indonesia Single Data (State Gazette of the Republic of Indonesia of 2019 Number 112);
7. Regulation of the President Number 174 of 2024 on the Ministry of Communication and Digital Affairs (State Gazette of the Republic of Indonesia of 2024 Number 370);

8. Regulation of the Minister of Communication and Information Technology Number 1 of 2025 on the Organization and Work Procedures of the Ministry of Communication and Digital Affairs (Official Gazette of the Republic of Indonesia of 2025 Number 7);

HAS DECIDED:

To establish:

REGULATION OF THE MINISTER OF COMMUNICATION AND DIGITAL AFFAIRS ON PUBLIC SCOPE ELECTRONIC SYSTEM ORGANIZERS.

CHAPTER I

GENERAL PROVISIONS

Article 1

Under this Regulation of the Minister, the following definitions are employed:

1. Electronic System Organizers are any person, state administrator, business entity, and community that provides, manages, and/or operates Electronic Systems individually or jointly for Electronic System Users for their own needs and/or the needs of other parties.
2. Public Scope Electronic System Organizers, from this point onward are referred to as Public Scope PSE, are the Organization of Electronic Systems by State Organizing Agencies or Institutions appointed by State Organizing Agencies.
3. Public Scope PSE of User Generated Content is a Public Scope PSE where the provision, display, uploading, and/or exchange of Electronic Information and/or Electronic Documents is carried out by Electronic System Users.
4. Electronic Systems are a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, send, and/or distribute Electronic Information.
5. Electronic Information is one or a collection of Electronic Data, including but not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy or the like, letters, signs, numbers, Access codes, symbols, or perforations that have been processed which have meaning or can be understood by people who are able to understand them.
6. Electronic Documents are any Electronic Information created, forwarded, sent, received or stored in analog, digital, electromagnetic, optical or similar form, which can be viewed, displayed and/or heard via a computer or Electronic System, including but not limited to writing, sound, images, maps, designs, photographs or the like, letters, signs, numbers, Access codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand them.
7. Electronic Data is data in electronic form which is not limited to writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegrams, telex, telecopy or the like, letters, signs, numbers, Access codes, symbols or perforations.
8. Personal Data is data about an individual who is identified or can be identified individually or in combination with other information either directly or indirectly through an Electronic or non-electronic System.
9. Electronic Transactions are legal acts carried out using computers, computer networks, and/or other

electronic media.

10. Classification of Data According to Risk is a process to determine data groups from all types of Electronic Data owned by Public Scope PSE according to the risks posed.

11. Classified Data is a group of Electronic Data that has been classified according to risk level.

12. Archives are records of activities or events in various forms and media in accordance with developments in information and communication technology that are created and received by state institutions, regional governments, educational institutions, companies, political organizations, community organizations, and individuals in carrying out community, national and state life.

13. Data Reclassification is a reassessment of the risk level of Classified Data that has been determined based on a Review.

14. Review is the process of reviewing a group of Classified Data periodically or at any time as needed.

15. Cloud Computing is a model for providing uniform, easy, on-demand network access to a shared pool of configurable computing resources including networks, servers, storage, applications, and services that can be provisioned and released rapidly and with minimal management effort or service provider interaction.

16. Domain Name is the internet address of a state administrator, person, business entity, and/or community, which can be used to communicate via the internet, in the form of a code or arrangement of characters that is unique to indicate a particular location on the internet.

17. Agency Domain Name is an internet address of an Agency that can be used to communicate via the internet, in the form of a code or arrangement of characters that is unique to indicate a particular location on the internet.

18. Domain Name Registry is the organizer responsible for managing, operating and maintaining the organization of the Electronic Domain Name System.

19. Domain Name Official is an official appointed and designated by the Agency Official to register and manage Agency Domain Names.

20. Data Center is a facility used for the placement of Electronic Systems and other related components for the purposes of data placement, storage and processing, and data recovery.

21. Access is the activity of interacting with an Electronic System that is stand-alone or in a network.

22. Termination of Access is the act of blocking Access, closing accounts and/or deleting content.

23. Normalization is the process of restoring access to an Electronic System that has been closed so that it can be accessed again.

24. Ministry or Institution is a State Organizing Agency tasked with supervising and issuing regulations for its sector.

25. State Organizing Agencies, from this point onwards are referred to as Agencies, are legislative, executive and judicial institutions at the central and regional levels and other agencies established by laws and regulations.

26. Central Agencies are ministries, non-ministerial government agencies, state agency secretariats, non-structural agency secretariats, and other government agencies.

27. Regional Government is the regional head as an element of the regional government administration that leads the implementation of government affairs that fall under the authority of an autonomous region.

28. Institution appointed by the Agency, from this point onwards is referred to as Institution, is an institution that carries out the organization of public scope Electronic Systems on behalf of the appointing Agency.

29. Village Government is the village head or someone called by another name assisted by village apparatuses as elements of the regional government administration.

30. Agency Officials are middle high-ranking officials in Central Agencies, middle high-ranking officials in Provincial Governments, first-class high-ranking officials in Regency/City Regional Governments, heads of organizational units as assistant elements for leaders or leadership elements.

31. Data Supervisor is a Central Agency that is given the authority to carry out data-related coaching or a regional agency that is given the task to carry out data-related coaching as regulated in accordance with the provisions of laws and regulations in the field of Indonesia single data.

32. Data Producer is a unit in an Agency that produces data based on authority in accordance with the provisions of laws and regulations.

33. Data Guardian is a unit in an Agency that carries out the activities of collecting, examining, and managing Data submitted by Data Producers, as well as disseminating data.

34. Electronic System Users are any person, state administrator, business entity, and member of the community who utilizes goods, services, facilities, or information provided by Electronic System Organizers.

35. Indonesia Single Data Forum is a communication and coordination forum for Central Agencies and/or regional agencies for the implementation of Indonesia single data.

36. Internet Service Providers, from this point onward are abbreviated as ISP, are multimedia service providers that provide internet access services to connect to public internet networks.

37. Provider is a business actor who provides goods/services based on a contract.

38. Ministry of Communication and Digital Affairs, from this point onwards is referred to as Ministry, is a ministry that organizes government affairs in the field of communication and information.

39. Minister is the minister who organizes government affairs in the field of communication and information.

40. Director General is the director general whose duties and functions are in the field of organizing public scope electronic systems.

Article 2

The scope of this Regulation of the Minister shall include:

a. registration of Public Scope Electronic System Organizers;

b. governance and moderation of Electronic Information and/or Electronic Documents;

c. Termination of Access to prohibited Electronic Information and/or Electronic Documents;

d. organization of Agency Domain Names;

e. Classification of Data According to the Risks of Public Scope Electronic System Organizers; and

f. coaching and supervision.

Article 3

(1) Public Scope PSE includes:

  a. Agencies; and

  b. Institutions.

(2) Public Scope PSE as referred to in paragraph (1) does not include the Public Scope PSE which is the regulatory and supervisory authority for the financial sector.

(3) Institutions as referred to in paragraph (1) letter b must at least meet the following criteria:

a. have a registration certificate for Private Scope Electronic System Organizers in accordance with laws and regulations;

b. in the form of an Indonesian legal entity; and

c. has a data center located in the territory of the Unitary State of the Republic of Indonesia.

(4) The appointment of Institutions as referred to in paragraph (1) letter b is an assignment stipulated by laws and regulations.

CHAPTER II

REGISTRATION OF PUBLIC SCOPE ELECTRONIC SYSTEM ORGANIZERS

Division One

General

Article 4

(1) Every Public Scope PSE is required to register as the Public Scope PSE for the Electronic System it operates.

(2) The obligation to register as Public Scope PSE as referred to in paragraph (1) is carried out before the Electronic System begins to be used by Electronic System Users.

(3) In addition to the obligation to register as referred to in paragraph (1), Public Scope PSE are required to:

a. provide a security system that includes procedures and systems for preventing and responding to threats and attacks that cause disruption, failure and loss;

b. carry out protection of Personal Data; and

c. conducting Electronic System feasibility tests,

in accordance with the provisions of laws and regulations.

(4) Registration of Public Scope PSE as referred to in paragraph (1) is submitted to the Minister via electronic registration services.

Article 5

(1) Public Scope PSE must appoint a Public Scope PSE registration official.

(2) The Public Scope PSE registration official as referred to in paragraph (1) is a registration official who comes from:

a. Agencies; or

b. Institutions.

Article 6

(1) The Public Scope PSE registration official who comes from the Agency as referred to in Article 5 paragraph (2) letter a is a state civil servant who holds a position of at least:

a. administrator position in a work unit or regional apparatus that handles communications and informatics affairs; or

b. functional position of a middle expert who has competence in the field of information and communication technology in a work unit or regional apparatus that handles communication and informatics affairs.

(2) The Public Scope PSE registration official who comes from the Agency as referred to in paragraph (1) is assigned with a letter of assignment signed by the Agency Official.

Article 7

(1) The Public Scope PSE registration official who comes from the Institution as referred to in Article 5 paragraph (2) letter b is an employee with a permanent employment contract who leads the information and communication technology unit at the Institution.

(2) The Public Scope PSE registration official who comes from the Institution as referred to in paragraph (1) is assigned with a letter of assignment signed by the head of the Institution.

Article 8

(1) The Public Scope PSE registration official as referred to in Article 5 carries out the registration of the Public Scope PSE as referred to in Article 4 paragraph (1).

(2) In carrying out Public Scope registration as referred to in paragraph (1), the Public Scope PSE registration official must:

a. ensure the validity and accuracy of all Public Scope PSE registration data;

b. update the Public Scope PSE registration data in accordance with the current conditions of the Electronic System;

c. maintaining the confidentiality of Access consisting of user identity and password, as well as Public Scope PSE registration data;

d. fill in information on the implementation of procedures and systems, as well as the availability of security facilities in the organization of Electronic Systems; and

e. report the results of the Public Scope PSE registration activities to the Agency Official or Institutional Leader.

Article 9

(1) The Public Scope PSE registration official must prove the assignment to carry out the Public Scope PSE registration by uploading a letter of assignment via the electronic registration service.

(2) In addition to uploading the letter of assignment as referred to in paragraph (1), the Public Scope PSE registration official must provide information of the Public Scope PSE registration official regarding:

a. type of agency or institution;

b. name of agency or institution;

c. name of work unit;

d. telephone number of work unit;

e. status of the Public Scope PSE registration official:

f. full name of the Public Scope PSE registration official;

g. Employee Identity number of the Public Scope PSE registration official for Agencies, or employee number of the registration official for Institutions.

h. position title of the Public Scope PSE registration official;

i. mobile phone number of the Public Scope PSE registration official; and

j. official email address of the Agency as a Public Scope PSE.

(3) The information as referred to in paragraph (2) can utilize the personnel service application system.

(4) In terms of filling in information regarding the Public Scope PSE registration official as referred to in paragraph (2), the Public Scope PSE registration official who comes from an Institution must enclose the basis for appointing the Institution as referred to in Article 3 paragraph (4).

(5) The Ministry will verify information regarding Public Scope PSE registration officials as referred to in paragraph (2) and paragraph (4).

Article 10

(1) In the event of a change in the Public Scope PSE registration official as referred to in Article 9 Paragraph (1), the Public Scope PSE must assign an official to replace the Public Scope PSE registration official.

(2) The official who replaces the Public Scope PSE registration official as referred to in paragraph (1) must:

a. upload the letter of assignment as referred to in Article 9 paragraph (1); and

b. fill in the information as referred to in Article 9 paragraph (2) and paragraph (4).

(3) The Ministry will verify information regarding the official who replaces the Public Scope PSE registration official as referred to in paragraph (2).

Division Two

Registration of Electronic Systems Managed by Public Scope PSE

Article 11

(1) Registration of Electronic Systems managed by Public Scope PSE must be carried out by the Public Scope PSE registration official.

(2) The Public Scope PSE through the Public Scope PSE registration official provides correct information in filling out the registration form on the Electronic System managed by the Public Scope PSE regarding:

a. overview of the operation of the Electronic System;

b. fulfillment of obligations to ensure information security in accordance with the provisions of laws and regulations;

c. fulfillment of the obligation to provide a security system that includes procedures and systems for preventing and responding to threats and attacks that cause disruption, failure and loss in accordance with the provisions of laws and regulations;

d. fulfillment of the obligation to protect Personal Data in accordance with the provisions of laws and regulations;

e. fulfillment of the obligation to carry out electronic system suitability tests in accordance with the provisions of laws and regulations; and

f. fulfillment of the provisions of the national electronic-based government system architecture and the electronic-based government system architecture of Central Agencies and Regional Governments in accordance with the provisions of laws and regulations in the organization of electronic systems.

(3) The Ministry checks the completeness of the registration form on the Electronic System managed by the Public Scope PSE.

(4) In the event that the information as referred to in paragraph (2) has been submitted completely based on the checks as referred to in paragraph (3), the Ministry may approve the registration of the Electronic System managed by the Public Scope PSE.

(5) The registration approval as referred to in paragraph (4) is an approval of the completeness of the documents and information submitted by the Agency as referred to in paragraph (2).

Article 12

The Public Scope PSE registration official fills in information regarding the overview of the operation of the Electronic System as referred to in Article 11 paragraph (2) letter a, which consists of:

a. name of Electronic System;

b. Electronic System owner;

c. Electronic Systems sector/field;

d. information regarding the Electronic System contact person;

e. uniform resource locator (URL) of the website;

f. Domain name system and/or internet protocol (IP) address of the server;

g. a brief description of the Electronic System functions and the Electronic System business processes;

h. Electronic System categories based on risk principles;

i. Managed Classified Data;

j. information about the Personal Data processed; and

k. information on the location of management, processing and/or storage of Electronic Systems and Electronic Data.

Division Three

Issuance of Public Scope PSE Registration Certificate

Article 13

(1) The Minister issues a Public Scope PSE registration certificate if the registration of the Electronic System managed by the Public Scope PSE is approved as referred to in Article 11 paragraph (4).

(2) The Public Scope PSE registration certificate in paragraph (1) is placed in the Public Scope PSE list which is published on the website managed by the Ministry.

(3) The Public Scope PSE registration certificate as referred to in paragraph (2) contains at least the following information:

a. Ministry logo;

b. Public Scope PSE name;

c. Public Scope PSE registration number;

d. name of the Public Scope PSE registration official;

e. name of Electronic System;

f. Electronic System functions;

g. Electronic System version;

h. date of issue;

i. Public Scope PSE registration certificate barcode; and

j. name and signature of the official signing the PSE Public Scope registration certificate.

(4) Public Scope PSE registration officials can download the Public Scope PSE registration certificate that has been issued through electronic services provided by the Ministry.

(5) Public Scope PSE that has obtained a Public Scope PSE registration certificate as referred to in paragraph (1) must include said registration certificate on each Electronic System that has been registered.

(6) The Public Scope PSE registration certificate as referred to in paragraph (1) is a requirement for submitting an application for a shopping recommendation (clearance) for the development of Electronic Systems in an Agency.

Division Four

Update of Public Scope PSE Registration Certificate

Article 14

(1) In the event that the registration information for the Electronic System managed by the Public Scope PSE as referred to in Article 11 paragraph (2) changes, the Public Scope PSE through the Public Scope PSE registration official is required to update the contents of the registration form on the Electronic System managed by the Public Scope PSE.

(2) The Ministry carries out completeness checks on the updates to the registration form on the Electronic System managed by the Public Scope PSE as referred to in paragraph (1).

(3) If based on the checks as referred to in paragraph (2) the updates to the contents of the Electronic System registration form are declared complete, the Minister will update the Public Scope PSE registration certificate.

Division Five

Removal of Public Scope PSE Registration Certificate

Article 15

(1) In the event that the Electronic System is no longer in use, the Public Scope PSE registration official must submit a statement stating that the Electronic System is no longer in use through the electronic services provided by the Ministry.

(2) The certificate as referred to in paragraph (1) is signed by an Agency Official.

(3) The Minister shall remove the Public Scope PSE registration certificate after receiving the certificate as referred to in paragraph (2).

Division Six

Administrative Sanctions and Normalization

Article 16

(1) The Minister shall impose administrative sanctions on Public Scope PSE which:

a. does not register a Public Scope PSE as referred to in Article 4 paragraph (1);

b. does not fulfill the obligations as referred to in Article 4 paragraph (3); and/or

c. has a registration certificate but does not report changes to the registration information for the Electronic System managed by the Public Scope PSE as referred to in Article 14 paragraph (1).

(2) The imposition of administrative sanctions as referred to in paragraph (1) is carried out through coordination with the leadership of the relevant Ministry or Institution.

(3) In the event that a Public Scope PSE does not register as referred to in paragraph (1) letter a, the Minister will impose administrative sanctions in the form of Termination of Access in the form of blocking of the Electronic System (access blocking).

(4) In the event that the Public Scope PSE does not provide correct registration information as referred to in paragraph (1) letter b or has a registration certificate but does not report changes to the registration information as referred to in paragraph (1) letter c, the Minister will impose administrative sanctions in the form of:

a. written reprimands delivered via electronic mail and/or other electronic media, which are given to the Public Scope PSE 3 (three) times for every 7 x 24 (seven times twenty four) hours;

b. temporary suspension of the Public Scope PSE in the event of failure to heed the written reprimand within a period of 7 (seven) days from the time the third reprimand is sent as referred to in letter a; and/or

c. Termination of Access in the form of blocking of the Electronic System (access blocking) and removal from the Public Scope PSE list if the Public Scope PSE does not provide confirmation within a period of 7 (seven) days after the temporary suspension as referred to in letter b.

Article 17

(1) In the event that the Public Scope PSE has fulfilled the registration requirements as referred to in Article 5 to Article 12, the Minister will carry out Normalization of the Electronic System whose access has been terminated (access blocking) as referred to in Article 16 paragraph (3).

(2) In the event that the Public Scope PSE has correctly updated the registration information, the Minister will

carry out Normalization of the Electronic System which has been temporarily suspended as referred to in Article 16 paragraph (4) letter b.

(3) In the event that a Public Scope PSE has re-registered by providing correct registration information, the Minister will carry out Normalization of the Electronic System whose access has been terminated and has been removed from the Public Scope PSE list as referred to in Article 16 paragraph (4) letter c.

(4) Normalization as referred to in paragraph (1), paragraph (2) and paragraph (3) is carried out through the following stages:

a. Public Scope PSE through Agency Officials or Institutional Leaders submit a Normalization application to the Minister; and

b. The Normalization Application as referred to in letter a is submitted by enclosing:

1. written request letter; And

2. Public Scope PSE registration certificate.

CHAPTER III

GOVERNANCE AND MODERATION OF ELECTRONIC INFORMATION AND/OR ELECTRONIC DOCUMENTS

Division One

General

Article 18

(1) Public Scope PSE must organize Electronic Systems and manage Electronic Information and/or Electronic Documents in the Electronic System reliably, safely and responsibly.

(2) Public Scope PSE must provide instructions for using services in the Indonesian language in accordance with the provisions of laws and regulations.

(3) Public Scope PSE is required to ensure that its Electronic System:

a. does not contain; and

b. does not facilitate dissemination,

prohibited Electronic Information and/or Electronic Documents.

(4) Prohibited Electronic Information and/or Electronic Documents as referred to in paragraph (3) are Electronic Information and/or Electronic Documents with the following classifications:

a. violating the provisions of laws and regulations;

b. disturbing the community and disrupting public order; and

c. notify how or provide Access to prohibited Electronic Information and/or Electronic Documents.

(5) Prohibited Electronic Information and/or Electronic Documents as referred to in paragraph (4) are urgent if they contain:

a. terrorism;

b. child pornography; or

c. content that disturbs the community and disrupts public order.

(6) Prohibited Electronic Information and/or Electronic Documents as referred to in paragraph (4) letter b are determined by the Ministry or Institution in accordance with the provisions of laws and regulations.

(7) Public sector PSE that does not fulfill their obligations as referred to in paragraph (3) will have their access to the Electronic System terminated (access blocking).

Division Two

Obligations of Public Scope PSE of User Generated Content

Article 19

(1) In order to fulfill the obligations as referred to in Article 18 paragraph (3), the Public Scope PSE of User Generated Content is required to:

a. have governance regarding Electronic Information and/or Electronic Documents; and

b. provide reporting facilities.

(2) The governance as referred to in paragraph (1) letter a at least contains the following provisions:

a. obligations and rights of Electronic System Users in using Electronic System services;

b. obligations and rights of Public Sector PSE in carrying out Electronic System operations;

c. responsibility for Electronic Information and/or Electronic Documents uploaded by Electronic System Users; and

d. availability of facilities and services and resolution of complaints.

(3) The reporting facilities as referred to in paragraph (1) letter b must be accessible to the public and used to submit complaints and/or reports regarding prohibited Electronic Information and/or Electronic Documents contained in the Electronic System managed by the entity.

(4) In the case of complaints and/or reports regarding prohibited Electronic Information and/or Electronic Documents as referred to in paragraph (3), the Public Scope PSE of User Generated Content is required to:

a. provide responses to complaints and/or reports to the complaining party and/or reporting party;

b. conduct independent examinations of complaints and/or reports and/or request verification of complaints and/or reports to the Minister and/or the relevant Ministry or Institution;

c. provide notification to Electronic System Users regarding complaints and/or reports regarding Electronic Information and/or Electronic Documents uploaded by Electronic System Users; and

d. reject complaints and/or reports if the Electronic Information and/or Electronic Documents reported are not prohibited Electronic Information and/or Electronic Documents.

(5) Public Scope PSE of User Generated Content that does not fulfill the obligations as referred to in paragraph (1) and paragraph (4) will have their access to the Electronic System terminated (access blocking).

Article 20

(1) Public Scope PSE of User Generated Content can be exempted from legal responsibility regarding

prohibited Electronic Information and/or Electronic Documents as referred to in Article 18 paragraph (4) which are transmitted or distributed via its Electronic System in the event that Public Scope PSE of User Generated Content:

a. has carried out the obligations as referred to in Article 18 paragraph (3) and Article 19;

b. provide information to Electronic System Users who upload prohibited Electronic Information and/or Electronic Documents for the purposes of supervision and/or law enforcement; and

c. carry out Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents.

(2) Information of Electronic System Users as referred to in paragraph (1) letter b is Electronic Data controlled or managed by the Public Scope PSE of User Generated Content related to services used by Electronic System Users including:

a. information regarding the identity of Electronic System Users, including the name of the Electronic System User used in services on the Public Scope PSE of User Generated Content;

b. the residential address of the Electronic System User and other addresses that identify the location of the Electronic System User when registering or using the Public Scope PSE of User Generated Content service;

c. identification number used by Electronic System Users to register for services on the Public Scope PSE of User Generated Content; and

d. payment or billing information issued by the Public Scope PSE of User Generated Content to Electronic System Users regarding the location of equipment installation and duration of service.

CHAPTER IV

TERMINATION OF ACCESS TO PROHIBITED ELECTRONIC INFORMATION AND/OR ELECTRONIC DOCUMENTS

Division One

General

Article 21

(1) The Minister has the authority to:

a. perform Termination of Access; and

b. order the Public PSE to terminate Access,

toward prohibited Electronic Information and/or Electronic Documents as referred to in Article 18 paragraph (4).

(2) In addition to the authority referred to in paragraph (1), the Minister has the authority to carry out Normalization.

(3) The Minister assigns the Director General to carry out the authority as referred to in paragraph (1) and paragraph (2).

Article 22

Public Scope PSE is required to carry out Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents as referred to in Article 18 paragraph (4) based on the Minister's order.

Article 23

(1) An application for the Termination of Access to prohibited electronic information and/or electronic documents as referred to in Article 18 may be submitted by:

a. the community;

b. Ministry or Institution;

c. law enforcement officers; and/or

d. judicial institution.

(2) The application as referred to in paragraph (1) can be submitted via:

a. website and/or application;

b. non-electronic mail; and/or

c. electronic mail.

Division Two
Request for Termination of Access by the Community

Article 24

(1) Applications by the community regarding the Termination of Access to prohibited Electronic Information and/or Electronic Documents as referred to in Article 23 paragraph (1) letter a are submitted to:

a. the authorized Ministry or Institution, for requests for Termination of Access to:

1. Prohibited Electronic Information and/or Electronic Documents that are under its authority; and/or

2. Electronic Information and/or Electronic Documents that can facilitate access to prohibited Electronic Information and/or Electronic Documents that are under its authority,

based on the provisions of laws and regulations; or

b. the Director General, for requests for Termination of Access to:

1. Prohibited Electronic Information and/or Electronic Documents containing pornography and/or gambling; and/or

2. Electronic Information and/or Electronic Documents that can facilitate access to prohibited Electronic Information and/or Electronic Documents containing pornography and/or gambling.

(2) Requests for Termination of Access submitted by the community as referred to in paragraph (1) must be submitted in writing and must contain at least the following information:

a. applicant's identity;

b. images or screen captures displaying prohibited Electronic Information and/or Electronic Documents;

c. a specific link or Uniform Resource Locator (URL) that leads to the prohibited Electronic Information and/or Electronic Documents for which access is requested to be terminated; and

d. the reasons on which the application is based.

(3) The Ministry or Institution that receives a request for the Termination of Access from the community as referred to in paragraph (1) letter a submits a request for the Termination of Access to the Director General.

Division Three

Application for Termination of Access by the Ministry or Institution, Law Enforcement Officers and Judicial Institutions

Article 25

(1) The relevant Ministry or Institution coordinates with the Director General to terminate access to prohibited Electronic Information and/or Electronic Documents as referred to in Article 18 paragraph (4).

(2) Law enforcement officers may request the Director General to terminate access to prohibited electronic information and/or electronic documents as referred to in Article 18 paragraph (4).

(3) Judicial institutions may order the Termination of Access to prohibited Electronic Information and/or Electronic Documents as referred to in Article 18 paragraph (4) to the Director General.

(4) Termination of Access as referred to in paragraph (1), paragraph (2), and paragraph (3) is submitted by the Ministry or Institution, law enforcement officers, or Judicial Institutions in writing and at least by enclosing:

a. official letter from the Ministry or Institution, law enforcement officers, or a letter of court ruling and/or decision from a judicial institution;

b. legal analysis regarding prohibited Electronic Information and/or Electronic Documents;

c. images or screen captures that display prohibited Electronic Information and/or Electronic Documents; and

d. specific link or Uniform Resource Locator (URL) that lead to prohibited Electronic Information and/or Electronic Documents.

(5) A written request for Termination of Access from the Ministry or Institution, law enforcement officers, and/or judicial institutions is made by the contact person as referred to in Article 12 letter d.

(6) In the event that the Ministry or Institution, law enforcement officers and/or judicial institutions do not appoint a contact person as referred to in paragraph (5), the request for Termination of Access shall be made by the Public Scope PSE registration official.

Division Four

Implementation of Termination of Access

Article 26

(1) The Director General orders the Public Scope PSE to carry out Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents.

(2) The Order for the Termination of Access in the form of content deletion (take down) as referred to in paragraph (1) is delivered via electronic mail or other Electronic Systems.

(3) Public Scope PSE that are ordered to carry out Termination of Access in the form of content deletion (take down) as referred to in paragraph (1) are required to carry out Termination of Access (take down) of the prohibited Electronic Information and/or Electronic Documents no later than 1 x 24 (one times twenty four) hours after the order for the Termination of Access is received.

(4) The Director General carries out Termination of Access and/or orders the ISP to carry out Termination of Access to the Electronic System in the form of blocking (access blocking) in the event that the Public Scope PSE does not carry out Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents as referred to in paragraph (3).

(5) Requests for Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents are deemed urgent as referred to in Article 18 paragraph (5), thus Public Scope PSE is required to carry out Termination of Access in the form of content deletion (take down) of prohibited Electronic Information and/or Electronic Documents as soon as possible without delay, no later than 4 (four) hours after the warning is received.

(6) The Director General carries out Termination of Access and/or orders the ISP to carry out Termination of Access in the form of blocking of Electronic Systems (access blocking) organized by the Public Scope PSE in the event that the Public Scope PSE does not carry out Termination of Access in the form of content deletion (take down) as referred to in paragraph (4).

Division Five
The Role of Internet Service Providers

Article 27

(1) ISP are required to carry out Termination of Access in the form of blocking of the Electronic Systems (access blocking) of the Public Scope PSE which are ordered by the Director General to have access terminated as referred to in Article 26 paragraph (4) and paragraph (6).

(2) Termination of Access in the form of blocking (access blocking) as referred to in paragraph (1) may only be carried out by the Director General.

(3) Termination of Access in the form of blocking (access blocking) by ISP as referred to in paragraph (1) and paragraph (2) is carried out using procedures, methods and/or technology determined by the Director General.

(4) ISP that does not carry out Termination of Access in the form of blocking (access blocking) as referred to in paragraph (1) will be subject to sanctions in accordance with the provisions of laws and regulations.

Article 28

(1) ISP are required to display a landing page when carrying out Termination of Access in the form of blocking of Electronic Systems (access blocking) containing prohibited Electronic Information and/or Electronic Documents and/or facilitating the dissemination of prohibited Electronic Information and/or Electronic Documents.

(2) The landing page as referred to in paragraph (1) does not contain prohibited Electronic Information and/or Electronic Documents and/or offer prohibited products in accordance with the provisions of laws and regulations.

Division Six
Normalization

Article 29

(1) An application for normalization shall be submitted to the Director General by:

a. Public Scope PSE whose access to its Electronic System has been terminated (access blocking); or

b. Ministry or Institution.

(2) Application for Normalization by a Public Scope PSE whose access to the Electronic System has been terminated (access blocking) as referred to in paragraph (1) letter a is submitted by enclosing:

a. written application letter;

b. identity of the person responsible for the Electronic System and a contactable contact number;

c. scan of the identity card of the owner and/or person in charge of the Electronic System;

d. images or screen captures and links (URL) that prove that the Electronic System no longer contains prohibited Electronic Information and/or Electronic Documents;

e. a letter of recommendation from a Ministry or Institution, law enforcement officer, or a court decision that has permanent legal force; and

f. other evidence supporting legitimacy as a Public Scope PSE.

(3) The person in charge as referred to in paragraph (2) letter b is:

a. Agency Officials; or

b. Institutional leaders.

(4) The application for normalization by the Ministry or Agency as referred to in paragraph (1) letter b is submitted via a written application letter.

(5) The Director General will follow up on application for normalization that meet the provisions as referred to in paragraph (2) and paragraph (4) no later than 2x24 (two times twenty four) hours.

(6) The Director General has the authority to reject applications for Normalization of Electronic Systems that have had their access terminated (access blocking) for more than 3 (three) times.

CHAPTER V
THE ORGANIZATION OF AGENCY DOMAIN NAMES

Division One
General

Article 30

The organization of Agency Domain Names in this Regulation of the Minister includes:

a. use of Agency Domain Names;

b. management of Agency Domain Names;

c. use of an Agency Domain Name's server; and

d. Agency Domain Name dispute resolution.

Division Two
Use of Agency Domain Names

Article 31

Agencies must use the Agency Domain Name and are responsible for the use of the Agency Domain Name used.

Article 32

(1) Agency Domain Names consist of:

a. Second Level Domain Name; and

b. Derived level Domain Name.

(2) The second level domain name as referred to in paragraph (1) letter a consists of:

a. .go.id Domain Name;

b. .desa.id. Domain Name; and

c. Other Domain Names related to other names of villages in accordance with the provisions of laws and regulations.

(3) go.id Domain Name as referred to as referred to in paragraph (2) letter a is used for:

a. official electronic address of the Agency;

b. national government administration services or national public services; and/or

c. national or international scale activities.

(4) .desa.id Domain Name as referred to in paragraph (2) letter b is used for the official electronic address of the Village Government.

(5) Other Domain Names related to other names of villages as referred to in paragraph (2) letter c and their use are determined by the Minister.

Article 33

(1) Vertical agencies of the Central Agency located in the regions or representatives abroad, or territorial apparatuses in the Regional Government, can use Agency Domain Name as the Agency's official electronic address.

(2) The official electronic address of a work unit at an agency uses a subdomain of the agency domain name.

(3) The Agency determines policies regarding the procedures for managing Domain Names and subdomains within the Agency.

Article 34

(1) Village Governments must use the Domain Name as referred to in Article 32 paragraph (4) for the implementation of village government.

(2) The official electronic address of the work unit in the Village Government uses a subdomain of the Village Government Domain Name.

Article 35

The use of Domain Names for national and/or international scale activities as referred to in Article 32 paragraph (3) letter c is carried out in accordance with the provisions of laws and regulations.

Division Three

Management of Agency Domain Names

Article 36

(1) Management of Agency Domain Names as referred to in Article 30 letter b includes:

a. registration of Agency Domain Name;

b. extension of Agency Domain Name;

c. deactivation and deletion of Agency Domain Name;

d. change of Agency Domain Name;

e. changes to the data of the Agency Domain Name's Official;

f. transfer of Agency Domain Name;

g. cancellation of Agency Domain Name;

h. Agency Domain Name recovery;

i. handling complaints regarding Agency Domain Name; and

j. monitoring, evaluation and financing.

(2) Management of Agency Domain Names as referred to in paragraph (1) is carried out through electronic services provided by the Ministry.

(3) Management of Agency Domain Names as referred to in paragraph (1) is exempted for management of Domain Names for military purposes which refer to regulations stipulated by the minister who organizes government affairs in the field of defense and security.

(4) Management of subdomains within the Agency is carried out by the work unit that manages information and communication technology.

Article 37

(1) The Minister is the Domain Name registrar for Agency Domain Names as referred to in Article 32 paragraph (1).

(2) In carrying out the registration of Agency Domain Names as referred to in paragraph (1), the Minister may assign the Director General.

Subdivision 1

Registration of Agency Domain Name

Article 38

(1) The Agency Official on behalf of the Agency Head submits a registration for .go.id Domain Name as referred to in Article 32 paragraph (3) to the Director General.

(2) The format for writing .go.id Domain Name as referred to in paragraph (1) must consist of:

a. characters which can be names or abbreviations or acronyms of the official names of agencies;

b. name of national government administration service;

c. name of national public service; and/or

d. name of national or international scale activities.

(3) Applications for registration of an Agency Domain Name used for the Agency's official electronic address as referred to in Article 32 paragraph (3) letter a must include:

a. Agency Domain Name application letter;

b. the legal basis which is the provision for the establishment of the Agency;

c. letter of appointment of Domain Name Official; And

d. civil servant card, TNI membership card, POLRI membership card, or permanent employee identity card of Domain Name Official.

(4) Applications for registration of Agency Domain Names used for national government administration services or national public services as referred to in Article 32 paragraph (3) letter b must include:

a. letter of application for an Agency Domain Name used for national government administration services or national public services;

b. the legal basis for the provision of national government administration services or national public services;

c. information regarding national government administration services or national public services including types of services and service beneficiaries;

d. letter of appointment of Domain Name Official; And

e. civil servant card, TNI membership card, POLRI membership card, or permanent employee identity card of Domain Name Official.

(5) Applications for registration of .go.id Domain Name used for national or international scale activities as referred to in Article 32 paragraph (3) letter c must include:

a. letter of application for an Agency Domain Name used for national or international scale activities;

b. the legal basis for the implementation of national or international scale activities;

c. information regarding national or international scale activities;

d. letter of appointment of Domain Name Official; and

e. civil servant card, TNI membership card, POLRI membership card, or permanent employee identity card of Domain Name Official.

Article 39

(1) The regency/city regional government must register the .desa.id domain name and/or other domain names related to other names for villages used for official electronic addresses.

(2) Registration of the .desa.id Domain Name and/or other Domain Names related to other names for villages by the regency/city Regional Government as referred to in paragraph (1) must be submitted to the Director General through the Agency Official.

(3) The Village Government coordinates with the Regency/City Regional Government in its area regarding the registration of the .desa.id Domain Name and/or other Domain Names related to other names for the village.

(4) The format for writing the .desa.id Domain Name and/or other Domain Names related to other names for villages must consist of characters that can be:

a. name or abbreviation of name; or

b. acronym,

of the official electronic address of the Village Government as referred to in Article 32 paragraph (4).

(5) Applications for registration of the .desa.id Domain Name and/or other Domain Names related to other names for villages by Agency Officials as referred to in paragraph (2) must include:

a. letter of application for the .desa.id Domain Name and/or other Domain Names related to other names for the village from the Agency Official on behalf of the regent/mayor to the Director General;

b. legal basis for regency/city regional regulations regarding the establishment of village governments in regencies/cities;

c. letter of appointment of Domain Name Official;

d. power of attorney from the village head to submit the registration of the Village Government Domain Name to the Domain Name Official; and

e. State civil servant card of the Domain Name Official at the regency/city regional government.

Article 40

(1) The letter of appointment of a Domain Name Official as referred to in Article 38 paragraph (3) letter c, paragraph (4) letter d, paragraph (5) letter d, and Article 39 paragraph (5) letter c is determined by the Agency Official.

(2) The Domain Name Official appointed by the Agency Official as referred to in paragraph (1) is a state civil servant who holds a position of at least:

a. administrator position in a work unit or regional apparatus that handles communications and informatics affairs; or

b. functional position of a middle expert who has competence in the field of information and communication technology in a work unit or regional apparatus that handles communication and informatics affairs.

(3) The letter of appointment as referred to in paragraph (1) must contain at least:

a. employee name; and

b. employee identification number.

Article 41

(1) The Director General has the authority to approve or reject an application for registration of an Agency Domain Name no later than 5 (five) business days after the electronic registration application is received.

(2) The Director General may reject an application for registration of a Domain Name in the following cases:

a. does not meet the requirements as referred to in Article 38 for the .go.id Domain Name or Article 39 for the .desa.id Domain Name;

b. the application submitted does not originate from an Agency and/or is within the authority of the Agency in accordance with the provisions of laws and regulations;

c. the submitted Agency Domain Name has been used by another Agency; and/or

d. the submitted Agency Domain Name is in conflict with the provisions of laws and regulations.

Article 42

The Agency Domain Name that has been approved by the Director can be used by the Agency from the time the Domain Name is approved and activated.

Article 43

In the event that the Agency Domain Name has been approved as referred to in Article 42, the Domain Name Official must provide information regarding at least:

a. Domain Name to be registered;

b. domain zone;

c. server name;

d. hosting server location;

e. internet protocol address; and

f. Domain Name System Security Extension (DNSSEC).

Subdivision 2
Extension of Agency Domain Name

Article 44

(1) Agencies must renew the Agency Domain Name that is still in use.

(2) Extension of the Agency Domain Name as referred to in paragraph (1) for:

a. The .go.id Domain Name is carried out by the Agency Domain Name Official; or

b. The .desa.id Domain Name and/or other Domain Names related to other names for villages are carried out by the Regency/City Regional Government Domain Name Official.

(3) The extension as referred to in paragraph (1) must be carried out no later than 35 (thirty five) calendar days from the end of the validity period of the Agency Domain Name.

Subdivision 3

Deactivation and Deletion of Agency Domain Names

Article 45

(1) The Director General has the authority to deactivate an Agency Domain Name.

(2) Deactivation as referred to in paragraph (1) is carried out in the following cases:

a. The agency does not extend the Agency Domain Name no later than 35 (thirty five) calendar days from the end of the active period of the Agency Domain Name;

b. Agency Domain Name in the process of dispute resolution;

c. Agency Domain Name is under surveillance due to misuse issues.

d. done in bad faith;

e. violates the rights of other parties; and/or

f. violating the propriety prevailing in the community or the provisions of laws and regulations.

(3) The Director General shall provide notification to the Domain Name Official via electronic communication facilities no later than 5 (five) business days before carrying out the deactivation as referred to in paragraph (1) and shall coordinate with the Domain Name Registry.

Article 46

(1) The Director General provides recommendations for the deletion of Agency Domain Name to the Domain Name Registry.

(2) Recommendations for deleting an Agency Domain Name as referred to in paragraph (1) are made in the following cases:

a. the Agency Domain Name dispute resolution process decided a deletion;

b. the existence of a court or arbitration decision that is final and binding;

c. the Agency Domain Name is not renewed within a period of 1 (one) year from the date of deactivation;

d. official request from the Agency Official to delete the .go.id Domain Name;

e. the existence of an agreement that has the legal consequence of canceling the use of the registered Agency Domain Name by another party; and/or

f. official request from regency/city agency officials to delete the .desa.id domain name and/or other domain names related to other names for villages.

(3) The Domain Name Registry must carry out the deletion of the Agency Domain Name according to the Director's recommendation.

(4) Deletion of the Agency Domain Name as referred to in paragraph (3) is carried out by deleting the Agency Domain Name from the .id Domain Name zone file.

Article 47

(1) Agencies can use the deleted Agency Domain Name.

(2) In the event that an Agency uses an Agency Domain Name that has been deleted as referred to in paragraph (1), the Agency must register the Agency Domain Name as referred to in Article 38 for the .go.id Domain Name or Article 39 for the .desa.id Domain Name and/or other Domain Names related to other names for villages.

Subdivision 4

Change to Agency Domain Name

Article 48

(1) Agencies can apply for changes to the Agency Domain Name used.

(2) In the event of a change in the .go.id Domain Name, the Agency must submit a letter signed by an Agency Official and addressed to the Director General.

(3) In the event of a change in the .desa.id Domain Name and/or other Domain Names related to other names for villages, the regency/city Regional Government must submit a letter signed by an Agency Official and addressed to the Director General.

(4) Provisions on:

a. Domain Name writing format;

b. Domain Name character format; and

c. Domain Name registration application,

for the .go.id Domain Name as referred to in Article 38 and for the .desa.id Domain Name and/or other Domain Names related to other names of villages as referred to in Article 39 shall apply mutatis mutandis to changes in the Agency Domain Name.

Article 49

(1) Agencies that make changes to the Agency Domain Name as referred to in Article 48 may use the Domain Name prior to the change simultaneously.

(2) Use of the Agency Domain Name prior to the changes as referred to in paragraph (1) shall be no later than 2 (two) years from the date of the determination of the change to the Agency Domain Name.

Article 50

(1) The Director General has the authority to approve or reject an application for a change in an Agency Domain Name no later than 4 (four) business days from the time of electronic submission.

(2) The Director General may reject an application to change a Domain Name in the following cases:

a. does not meet the requirements as referred to in Article 38 for the .go.id Domain Name or Article 39 for the .desa.id Domain Name and/or other Domain Names related to other names of the village;

b. the application submitted does not originate from an Agency and/or is within the authority of the Agency in accordance with the provisions of laws and regulations;

c. the submitted Agency Domain Name has been used by another Agency; and/or

d. the submitted Agency Domain Name is in conflict with the provisions of laws and regulations.

(3) In the event that an application to change an Agency Domain Name is rejected as referred to in paragraph (1), the Agency may re-submit an application to change the Agency Domain Name.

Subdivision 5

Changes in Data on Agency Domain Names

Article 51

(1) In the event of a change in the Domain Name Official's data, the Agency must submit a change in the Domain Name Official's data through the Agency Official.

(2) Changes to the Domain Name Official data as referred to in paragraph (1) shall be submitted to the Director by sending a letter of request for changes to the Domain Name Official data signed by the Agency Official.

(3) The letter of request for changes to the Domain Name Official data as referred to in paragraph (2) must be accompanied by a letter of appointment as referred to in Article 40.

Article 52

(1) The Director General may approve an application for a change in Domain Name Official data if it meets the provisions of Article 51.

(2) In the event that the application for submitting a change to the Domain Name Official's data does not fulfill the provisions of Article 51, the Director General has the right to reject the application for submitting a change to the Domain Name Official's data.

(3) Approval or rejection as referred to in paragraph (1) and paragraph (2) shall be given no later than 4 (four) business days from the time the request for data changes is received electronically.

(4) In the event that an application for a change in Domain Name Official data is rejected as referred to in paragraph (2), the Agency may resubmit an application for a change in Domain Name Official data.

Subdivision 6

Transfer of Agency Domain Name

Article 53

(1) Agencies can transfer their agency domain names.

(2) Transfer of Agency Domain Names as referred to in paragraph (1) is carried out in the following cases:

a. changes to the Agency managing the Agency Domain Name;

b. using the same Agency Domain Name; and

c. the transferred Agency Domain Name is still active.

(3) Transfer of Agency Domain Names as referred to in paragraph (1) is submitted to the Director by sending:

a. letter of request for transfer of Agency Domain Name;

b. letter of handover of transfer of Agency Domain Name; and

c. the required documents as referred to in Article 38 for the .go.id Domain Name or Article 39 for the .desa.id Domain Name.

(4) The letter of application for transfer of the Agency Domain Name and the letter of handover of the transfer of the Agency Domain Name as referred to in paragraph (3) letters a and b are signed by the Agency Official.

Subdivision 7

Cancellation of Agency Domain Name

Article 54

(1) The use of an Agency Domain Name may be cancelled by the Director General.

(2) Cancellation of an Agency Domain Name is carried out when the Agency Domain Name:

a. was registered; or

b. are still in use.

(3) Cancellation of an Agency Domain Name as referred to in paragraph (2) is carried out based on a request from the applicant Agency.

(4) The application for cancellation of a Domain Name as referred to in paragraph (3) must be submitted via an official letter signed by an Agency Official to the Director.

Subdivision 8

Agency Domain Name Recovery

Article 55

(1) Agencies can submit an application for recovery of the Agency Domain Name to the Director General.

(2) The application for recovery of a Domain Name as referred to in paragraph (1) is carried out through the following stages:

a. The Agency Official submits an application to the Director General; and

b. The application for recovery of the Domain Name as referred to in paragraph (1) is submitted by enclosing:

1. written application letter;

2. a statement that improvements have been made based on the reasons for deactivating the Domain Name as referred to in Article 45 paragraph (2); and

3. documents proving that improvements have been made as referred to in number 2.

Subdivision 9

Handling of Complaints regarding Agency Domain Name

Article 56

(1) The Director General provides electronic complaint handling services for Agency Domain Names.

(2) The electronic complaint handling service for Agency Domain Names as referred to in paragraph (1) contains at least:

a. the contact person’s contact number;

b. the contact person's email address;

c. frequently asked questions; and

d. service submission ticket system.

(3) Agencies and/or the public who submit complaints regarding Agency Domain Names through the electronic Agency Domain Name complaint handling service must include at least:

a. name of the reporting party;

b. origin of agency/organization/general public;

c. contact number;

d. reporting party's address;

e. identity card number; and

f. complaint description.

(4) The Director General can coordinate with the Domain Name Registry in handling complaints regarding Agency Domain Names.

Subdivision 10
Monitoring and Evaluation

Article 57

(1) Monitoring and evaluation of the management of Agency Domain Names is carried out by the Director General.

(2) Monitoring and evaluation as referred to in paragraph (1) is carried out on Domain Names regulated in this Regulation of the Minister.

(3) Monitoring and evaluation as referred to in paragraph (1) is carried out through coordination with the Domain Name Registry.

(4) The results of monitoring and evaluation as referred to in paragraph (2) are used as consideration for the management of Agency Domain Names.

(5) The results of monitoring and evaluation as referred to in paragraph (2) are reported to the Minister through the Director General at least 1 (one) time in 1 (one) year.

Division Four
Agency Domain Name Server Usage

Article 58

(1) Agencies that use Agency Domain Names must use Domain Name servers located in the jurisdiction of the Unitary State of the Republic of Indonesia.

(2) Agencies must use the Domain Name server provided by the Ministry for .go.id Domain Names.

(3) The Village Government can use the Domain Name server provided by the Ministry for the .desa.id Domain Name and/or other Domain Names related to other names of the village.

(4) Agencies that use the Agency Domain Name server must use an internet protocol address (IP address) located in the jurisdiction of the Unitary State of the Republic of Indonesia.

Division Five

Agency Domain Name Dispute Resolution

Article 59

(1) Agency Domain Name Disputes are disputes over Agency Domain Names registered according to this Regulation of the Minister.

(2) Disputes regarding Agency Domain Names as referred to in paragraph (1) shall be in the following matters:

a. The Agency Domain Name is identical and/or similar to another Agency Domain Name; and/or

b. The Agency Domain Name is used by another Agency.

(3) In the event that an Agency Domain Name dispute involves a party other than the Agency, resolution of the Agency Domain Name dispute will be carried out based on the provisions regulated by the Domain Name Registry.

(4) The Agency shall submit applications for the resolution of Agency Domain Name disputes to the Director General through official services organized by the Ministry.

(5) The mechanism for resolving Agency Domain Name disputes is through the following stages:

a. The Director General receives applications for the resolution of Agency Domain Name disputes submitted by Agencies;

b. The Director General together with the Domain Name Registry conducts discussions on applications for the resolution of Agency Domain Name disputes submitted by Agencies;

c. resolution of Agency Domain Name disputes is determined by the Director General; and

d. determination of Agency Domain Name disputes is submitted by the Director General to the Agencies involved in the dispute.

CHAPTER VI

DATA CLASSIFICATION ACCORDING TO THE RISK OF PUBLIC ELECTRONIC SYSTEM ORGANIZERS

Division One

General

Article 60

The scope of Data Classification arrangements according to the Risk of Public Scope PSE includes:

a. Classified Data;

b. executor of Data Classification According to Risk;

c. implementation of Data Classification According to Risk;

d. management, processing and/or storage of Classified Data;

e. Follow-up of Data Classification According to Risk; and

f. Classified Data retention.

Article 61

In carrying out Data Classification According to Risk, Public Scope PSE must at least:

a. ensure that Electronic Data can be accessed by authorized parties in accordance with the provisions of laws and regulations; and

b. ensure the confidentiality and security of Electronic Data managed, processed and/or stored at the National Data Center and Agencies.

Article 62

(1) Public Scope PSE is required to carry out Data Classification According to Risk.

(2) Data Classification According to Risk carried out by the Public Scope PSE as referred to in paragraph (1) is the basis for the management, processing and/or storage of Electronic Data at the National Data Center and/or Agency.

(3) Data Classification According to Risk as referred to in paragraph (1) is carried out on Electronic Data managed by Public Scope PSE.

(4) Data Classification According to Risk as referred to in paragraph (1) is carried out in the following stages:

a. determination of risk impact areas;

b. determination of impact criteria; and

c. determining risk levels,

in accordance with the provisions of laws and regulations.

Article 63

(1) Public Scope PSE must use Classified Data which is part of the data list determined by the head of the Agency or regional head in accordance with the provisions of laws and regulations in the field of Indonesia single data.

(2) In the event that the Classified Data as referred to in paragraph (1) has not been determined by the head of the Agency or the regional head, discussion of the Classified Data will be carried out through the mechanism of the Indonesia Single Data Forum in accordance with the provisions of laws and regulations

in the field of Indonesia Single Data.

(3) In the event that there is a dispute regarding the discussion of Classified Data as referred to in paragraph (2), the dispute resolution will be carried out through the mechanism of the Indonesia Single Data Forum at the central level.

(4) The results of the discussion on Data Classification According to Risk as referred to in paragraph (2) are reported to the Indonesia Single Data Forum at the central level.

(5) The results of the discussion on Classification of Data According to Risk as referred to in paragraph (3) include a list of Data which is Priority Data which is then determined by the minister who carries out government affairs in the field of national development planning.

(6) Further provisions related to the implementation of the Indonesia Single Data Forum at the central level are implemented in accordance with the provisions of laws and regulations in the field of Indonesian Single Data.

Division Two

Classified Data

Article 64

(1) Classified Data consists of:

a. Open Electronic Data;

b. Limited Electronic Data; and

c. Closed Electronic Data.

(2) Open Electronic Data as referred to in paragraph (1) letter a has a low risk level.

(3) Limited Electronic Data as referred to in paragraph (1) letter b has a medium risk level.

(4) Closed Electronic Data as referred to in paragraph (1) letter c has a high risk level.

(5) Classified data as referred to in paragraph (1) constitutes an archive in accordance with the provisions of laws and regulations regarding archiving.

Division Three

Executor of Data Classification According to Risk

Subdivision 1

Executor of Data Classification According to Risk of the Central Agency

Article 65

The implementation of Data Classification According to the Risk of the Central Agency is carried out by the executors of Data Classification According to the Risk of the Central Agency which consists of:

a. Head of Central Agency;

b. Agency Officials;

c. Data Supervisor;

d. Central level data guardian;

e. Central level Data Producer;

f. Central Agency's single data forum; and

g. Indonesia Single Data Forum at the central level.

Article 66

In implementing the Classification of Data According to Risk, the head of the Central Agency as referred to in Article 65 letter a has the following functions:

a. establish Classified Data;

b. determine the results of Data Reclassification; and

c. provide Electronic Data Access approval for closed Electronic Data.

Article 67

(1) In implementing Data Classification According to Risk, Agency Officials as referred to in Article 65 letter b have the following functions:

  a. coordinate the implementation of Data Classification According to Risk at least regarding:

    1. preparation of an inventory of Electronic Data to be classified;

    2. classification implementation schedule; and

    3. Classified Data determination process.

  b. give approval to the proposed Review; and

  c. submit Classified Data and the results of Data Reclassification to the head of the Central Agency for determination.

(2) The Agency Official as referred to in paragraph (1) is the coordinator of the Central Agency's single data forum in accordance with the provisions of laws and regulations in the field of Indonesia single data.

Article 68

In the implementation of Data Classification According to Risk, the Data Supervisor as referred to in Article 65 letter c has the function of providing recommendations and guidance on Data Classification According to Risk within the scope of implementing Indonesia single data.

Article 69

(1) In implementing Data Classification According to Risk, the central level Data Guardian as referred to in Article 65 letter d has the following functions:

  a. collecting Classified Data from central level Data Producers;

  b. verifying Classified Data and Data Reclassification results;

  c. validating Classified Data and Data Reclassification results;

d. grouping Electronic Data according to Classified Data;

e. grouping Classified Data according to Data Reclassification;

f. creating and updating the list of Classified Data;

g. managing Classified Data that has been determined by the head of the Central Agency;

h. submitting a list of Classified Data and the results of Data Reclassification to Agency Officials;

i. preparing a study on the needs for a Review;

j. submitting a proposal for Review of Classified Data;

k. providing approval for Access to Limited Electronic Data; and

l. assisting central level Data Producers in performing Data Classification and Data Reclassification.

(2) The List of Classified Data as referred to in paragraph (1) letter f contains at least:

a. reference code;

b. Classified Data group;

c. Electronic Data name;

d. month of Classified Data determination; and

e. year of Classified Data determination.

(3) The central level data guardian as referred to in paragraph (1) is the central level data guardian in accordance with the provisions of laws and regulations in the field of Indonesia single data.

Article 70

In implementing the Classification of Data According to Risk, the central level Data Producer as referred to in Article 65 letter e has the following functions:

a. perform Data Classification According to Risk;

b. perform Data Reclassification; and

c. submit Classified Data and Data Reclassification results to the central level Data guardian for verification and validation.

Article 71

In the implementation of Data Classification According to Risk, the Central Agency's single data forum as referred to in Article 65 letter f has the function of a forum for internal communication and coordination regarding discussions on Data Classification According to Risk.

Article 72

In the implementation of Data Classification According to Risk, the Indonesia Single Data Forum at the central level as referred to in Article 65 letter g has the function as a forum for reporting the results of Classified Data that have been determined by the head of the central agency.

Subdivision 2

Executor of Data Classification According to the Risk of Regional Governments

Article 73

Implementation of Data Classification According to the Risk of Regional Governments is carried out by:

a. Regional head;

b. Agency Officials;

c. Regional level Data Supervisor;

d. Regional level data guardian;

e. Supporting data guardian;

f. Regional level Data Producers;

g. Indonesia Single Data Forum at the regional level; and

h. Indonesia Single Data Forum at the central level.

Article 74

In implementing Data Classification According to Risk, regional heads as referred to in Article 73 letter a have the following functions:

a. determine Classified Data and the results of Data Reclassification; and

b. provide Electronic Data Access approval for closed Electronic Data.

Article 75

(1) In implementing Data Classification According to Risk, Agency Officials as referred to in Article 73 letter b have the following functions:

a. coordinate the implementation of Data Classification According to Risk regarding at least:

1. preparation of an inventory of Electronic Data to be classified;

2. classification implementation schedule; and

3. Classified Data determination process.

b. submit Classified Data and the results of Data Reclassification to the regional head for determination; and

c. give approval to the proposed Review.

(2) The Agency Official as referred to in paragraph (1) is the coordinator of the Indonesia Single Data Forum at the regional level in accordance with the provisions of laws and regulations in the field of Indonesia Single Data.

Article 76

In the implementation of Data Classification According to Risk, the regional level Data Supervisor as referred to in Article 73 letter c has the function of providing recommendations and guidance on Data Classification According to Risk within the scope of the implementation of Indonesia single data at the regional level.

Article 77

(1) In implementing Data Classification According to Risk, the Regional level Data Guardian as referred to in Article 73 letter d has the following functions:

a. collect Classified Data from regional level Data Producers;

b. assist regional level Data Producers in carrying out Risk Based Data Classification and Data Reclassification;

c. conducting checks on the conformity of the Risk Based Data Classification process with the Regional Government data classification guidelines;

d. verify Classified Data and Data Reclassification results;

e. validate Classified Data and Data Reclassification results;

f. grouping Classified Data;

g. create and update the list of Classified Data;

h. manage Classified Data that has been determined by the regional head;

i. submit a proposal for Review of Classified Data; and

j. granting Access approval for limited Electronic Data.

(2) The Classified Data List as referred to in paragraph (1) letter g at least contains:

a. Reference code;

b. Classified Data group;

c. Data name;

d. month of Classified Data determination; and

e. year of Classified Data determination.

(3) The regional level data guardian as referred to in paragraph (1) is the regional level data guardian in accordance with the provisions of laws and regulations in the field of Indonesia single data.

Article 78

In the implementation of Data Classification According to Risk, the Supporting Data Guardian as referred to in Article 73 letter e has the function of assisting the regional level Data Guardian.

Article 79

In implementing Data Classification According to Risk, regional level Data Producers as referred to in Article 73 letter f have the following functions:

a. perform Data Classification According to Risk;

b. perform Data Reclassification; and

c. submit Classified Data and Data Reclassification results to the Regional level Data Guardian for verification and validation.

Article 80

In the implementation of Data Classification According to Risk, the Indonesia Single Data Forum at the regional level as referred to in Article 73 letter g, has the function of a forum for internal regional communication and coordination regarding discussions on Data Classification According to Risk.

Article 81

In the implementation of Data Classification According to Risk, the Indonesia Single Data Forum at the central level as referred to in Article 73 letter h, has the function as a forum for reporting the results of Classified Data that has been determined by the regional head.

Division Four

Implementation of Data Classification According to Risk

Subdivision 1

Implementation of Data Classification According to the Risk of the Central Agency

Article 82

(1) The implementation of Data Classification According to the Risk of the Central Agency must be documented.

(2) The Head of the Central Agency determines Classified Data.

(3) Implementation of Data Classification at the central level involves the Central Agency’s Single Data Forum.

Subdivision 2

Implementation of Data Classification According to the Risk of Regional Governments

Article 83

(1) The implementation of Data Classification According to the Risk of Regional Governments must be documented.

(2) Implementation of Data Classification According to the Risk of Regional Governments must pay attention to the Regional Government data classification guidelines issued by the minister who handles domestic affairs after coordinating with the Minister and the minister who handles development planning affairs.

(3) The regional head determines Classified Data by a decree of the regional head.

(4) The implementation of Risk Based Data Classification at the regional level involves Indonesia Single Data Forum at the regional level.

Subdivision 3

Data Review and Reclassification

Article 84

(1) The determination of Classified Data as referred to in Article 82 paragraph (2) and Article 83 paragraph (3) may be subject to Data Review and Reclassification.

(2) The review as referred to in paragraph (1) is carried out periodically:

a. 1 (one) time in 3 (three) years for open Electronic Data;

b. 1 (one) time in 5 (five) years for limited Electronic Data; and

c. 1 (one) time in 15 (fifteen) years for closed Electronic Data.

(3) The review as referred to in paragraph (2) may be carried out at any time as needed based on:

a. reassessment of risk levels;

b. results of monitoring and evaluation of the implementation of Risk Based Data Classification;

c. changes in national policy; and/or

d. changes in business process.

(4) The results of the review as referred to in paragraph (3) include:

a. Data Reclassification; or

b. Maintaining the level of Data Classification According to Risk.

(5) Data Reclassification as referred to in paragraph (4) letter a may:

a. increase the Classified Data level; or

b. lowering the Classified Data level.

Article 85

The Head of the Central Agency determines the results of changes to Data Reclassification.

Article 86

The regional head determines the results of changes to Data Reclassification.

Division Five

Management, Processing and/or Storage of Classified Data

Article 87

(1) Public Scope PSE are required to manage, process, and/or store Classified Data in the territory of the Unitary State of the Republic of Indonesia by ensuring appropriate security controls and measures.

(2) Management, processing and/or storage of Classified Data as referred to in paragraph (1) is carried out at:

a. National Data Center; and/or

b. Agency.

(3) Management, processing and/or storage of Classified Data as referred to in paragraph (2) must take the following into account:

a. Open and restricted Electronic Data is placed in the National Data Center; and

b. Closed Electronic Data is placed in the National Data Center and/or Agency.

(4) Management, processing, and/or storage of open and limited Electronic Data as referred to in paragraph (3) letter a is carried out at the national Data Center which consists of:

a. government Data Center facility services;

b. government Cloud Computing services; and

c. third party services involved in organizing the national Data Center in accordance with the provisions of laws and regulations.

(5) Management, processing and/or storage of closed Electronic Data as referred to in paragraph (3) letter b is carried out at:

a. government Data Center facility services; or

b. storage containers placed in the Agency's computing center.

Article 88

(1) In the event that storage technology is not available domestically, Public Scope PSE may manage, process, and/or store Electronic Systems and Electronic Data outside the territory of the Unitary State of the Republic of Indonesia.

(2) The criteria for storage technology not available domestically as referred to in paragraph (1) are determined by a committee consisting of the Ministry, institutions in charge of technology assessment and application, institutions that carry out government duties in the field of cyber security and encryption, and relevant Ministry or Institution.

(3) The committee as referred to in paragraph (2) is appointed by the Minister.

Article 89

(1) In the case of closed Electronic Data being stored at an Agency as referred to in Article 87 paragraph (3) letter b, the Agency must provide and use encrypted media storage containers.

(2) The encrypted media storage container as referred to in paragraph (1) is placed in the Agency's computing center.

(3) Management, processing, and/or storage of closed Electronic Data at the Agency Data Center must meet the requirements for Classified Data Access in accordance with the provisions in this Regulation of the Minister.

Article 90

Restricted and closed Electronic Data is stored (at-rest) in an encrypted state.

Division Six

Follow-up of Data Classification According to Risk

Subdivision 1
Online Electronic Data Transmission

Article 91

(1) Online Electronic Data transmission for open Electronic Data as referred to in Article 64 paragraph (1) letter a must pay attention to the authenticity and integrity of the Electronic Data.

(2) Online Electronic Data transmission for limited Electronic Data as referred to in Article 64 paragraph (1) letter b must be done at least:

a. by guaranteeing the authenticity and integrity of Electronic Data;

b. through intra-government networks; and

c. by being sent (in-transit) in an encrypted state.

(3) Closed Electronic Data as referred to in Article 64 paragraph (1) letter c cannot be shared via online.

(4) In the case of Electronic Data as referred to in paragraph (1) to paragraph (3) being strategic Electronic Data, the Agency or Institution must create electronic documents and electronic backups and connect them to a specific data center in accordance with the provisions of laws and regulations.

Subdivision 2
Offline Electronic Data Transmission

Article 92

(1) In the event that there are obstacles in online Electronic Data transmission and/or the file size is too large to access, then Data can be transmitted offline.

(2) Offline Electronic Data transmission for open Electronic Data must pay attention to the authenticity and integrity of the Electronic Data.

(3) Offline Electronic Data transmission for limited Electronic Data requires:

a. encryption of Electronic Data in media using unpublished cryptographic algorithms provided by institutions that carry out government duties in the field of cybersecurity and cryptography; and

b. sealed media storage containers labeled “Restricted” provided by the Agency requiring Electronic Data.

(4) Closed Electronic Data Transmission cannot be transmitted offline and/or via any media.

Subdivision 3
Classified Data Access Requirements

Article 93

(1) Access to Classified Data may be granted in accordance with Access requirements.

(2) Access to open Electronic Data must meet the following requirements:

a. still pay attention to the authenticity and integrity of Electronic Data; and

b. can be downloaded and saved on many media.

(3) Access to limited Electronic Data must meet the following requirements:

a. obtain approval from the Guardian; and

b. can be downloaded and stored in encrypted media.

(4) The data guardian as referred to in paragraph (3) letter a must supervise Classified Data Access.

(5) The Approval Requirements as referred to in paragraph (3) letter a are determined by the Agency that owns the Electronic Data.

(6) Access to closed Electronic Data must meet the following requirements:

a. obtain written permission from the head of the Agency that owns the Electronic Data;

b. Access is granted only to state officials and/or ASN/TNI/POLRI with the lowest position of first-class high-ranking leader appointed by the head of the Agency that owns the Electronic Data;

c. a special room is available to access Electronic Data;

d. Electronic Data Access can only be carried out at certain times and is subject to Access time restrictions in accordance with policies jointly determined by the National Data Center Manager and/or Agency as the owner of the Electronic Data;

e. Electronic Data Access can be done via devices that have been registered with the Agency;

f. Electronic Data can only be read (read only) by the designated party as referred to in letter b;

g. Supervision must be carried out on all access by the head of the agency that owns the electronic data; and

h. must go through the Electronic Data Access application process.

(7) The written permission requirements as referred to in paragraph (6) letter a are determined by the Agency that owns the Electronic Data.

(8) The specifications for special rooms as referred to in paragraph (6) letter c include:

a. implementation of security perimeter;

b. special room guarding with appropriate security control mechanisms;

c. design and implementation of physical security for offices, rooms and special room facilities;

d. design and implementation of physical protection against natural disasters, malicious attacks, and unexpected events;

e. design and implementation of procedures for working in special rooms; and

f. Determination of Access points where unauthorized parties can enter a special room must be controlled and isolated to avoid unauthorized Access.

(9) The process for proposing Electronic Data Access as referred to in paragraph (6) letter h is carried out by submitting a letter of application to the manager of the National Data Center and/or Agency as the owner of the Electronic Data by stating:

a. profile of state officials and/or ASN/TNI/POLRI with the lowest position being a first-class high-ranking position appointed by the head of the Agency that owns the Electronic Data;

b. Electronic Data Access time;

c. device data that will be used to perform Electronic Data Access; and

d. written permission from the head of the Central Agency or regional head.

Division Seven
Classified Data Retention

Article 94

(1) Classified Data Retention is the storage of Classified Data.

(2) The retention period for Classified Data is determined by the Agency that owns the Data in accordance with the provisions of laws and regulations.

(3) The agency that owns Electronic Data determines the retention of Classified Data, in accordance with the provisions of laws and regulations.

Article 95

(1) The agency that owns the Data must carry out the safe destruction of Classified Data in accordance with the provisions of laws and regulations.

(2) Destruction of Classified Data as referred to in paragraph (1) includes ensuring the destruction of Classified Data controlled by third party Cloud Computing service providers.

(3) Destruction of Classified Data as referred to in paragraph (2) must meet the following requirements:

a. retention has expired;

b. has no usage value;

c. in accordance with the provisions of laws and regulations; and

d. not related to the resolution of the process of a case.

Division Eight
Cloud Computing Services

Article 96

(1) Public Scope PSE must utilize Cloud Computing services hosted at the national Data Center.

(2) Cloud Computing Services hosted at the National Data Center as referred to in paragraph (1) consist of:

a. government Cloud Computing services; and

b. third party Cloud Computing services,

which meets certain requirements in accordance with the provisions of laws and regulations.

(3) Government Cloud Computing Services as referred to in paragraph (2) letter a are services for sharing application data and infrastructure by Agencies via intra-government networks or secured internet networks provided by the Ministry.

(4) Third party Cloud Computing Services as referred to in paragraph (2) letter b are provided by third party Cloud Computing Service Providers registered with the Ministry.

(5) The national data centers as referred to in paragraph (2) letters a and c are interconnected.

(6) Third party Cloud Computing service providers registered with the Ministry as referred to in paragraph (4) must be auditable in accordance with the provisions of laws and regulations.

(7) In the event that a Public Scope PSE uses a third-party Cloud Computing service provider, the Public Scope PSE is required to carry out Data Classification According to Risk for the Electronic Data it manages as referred to in Article 64.

(8) Guidelines for the implementation of the National Data Center as referred to in paragraph (1) are determined by the Minister.

Article 97

(1) The Minister publishes a list of third-party Cloud Computing service providers registered with the Ministry as referred to in Article 96 paragraph (4).

(2) Third party Cloud Computing service providers registered with the Ministry as referred to in paragraph (1) must meet the requirements.

(3) Provisions regarding the requirements as referred to in paragraph (2) are determined by the Minister.

Article 98

(1) The format of:

a. letter of assignment from the Public Scope PSE registration official from the Agency as referred to in Article 6 paragraph (2);

b. letter of assignment from the Public Scope PSE registration official originating from the Institution as referred to in Article 7 paragraph (2);

c. certificate of Electronic System which is no longer used as referred to in Article 15;

d. landing page as referred to in Article 28;

e. characters which can be names or abbreviations or acronyms of the official names of agencies as referred to in Article 38 paragraph (2) letter a;

f. the character of the .desa.id Domain Name and/or other Domain Names related to other names of villages as referred to in Article 39 paragraph (4);

g. letter of handover of transfer of Agency Domain Name as referred to in Article 53 paragraph (3) letter b; and

h. letter of application for settlement of disputes regarding Agency Domain Names as referred to in Article 59 paragraph (4),

are listed in Appendix I which constitutes an integral part of this Regulation of the Minister.

(2) Examples of:

a. The Agency Domain Name used for the Agency's official electronic address as referred to in Article 32 paragraph (3) letter a;

b. Agency Domain Names used for national government administration services or national public services as referred to in Article 32 paragraph (3) letter b;

c. The Agency Domain Name used for national and/or international scale activities as referred to in Article 32 paragraph (3) letter c; and

d. The Agency Domain Name used for the official electronic address of the Village Government as referred to in Article 32 paragraph (4),

are listed in Appendix II which constitutes an integral part of this Regulation of the Minister.

(3) Mechanisms related to:

a. Stages of Data Classification According to Risk as referred to in Article 62 paragraph (4);

b. Determination of Data Classification According to Risk as referred to in Article 63 paragraph (1);

c. Implementation of Data Classification According to Risk of the Central Agency as referred to in Article 82;

d. Implementation of Data Classification According to the Risk of Regional Governments as referred to in Article 83;

e. Implementation of Review and Reclassification of Central Level Agency Data as referred to in Article 85; and

f. Implementation of the Review and Reclassification of Regional Level Agency Data as referred to in Article 86,

are listed in Appendix III which constitutes an integral part of this Regulation of the Minister.

CHAPTER VII
DEVELOPMENT AND SUPERVISION

Division One
Development

Article 99

(1) The Minister provides development on the implementation of public scope electronic systems.

(2) Development for Public Scope PSE as referred to in paragraph (1) is carried out for:

a. Public Scope PSE registration official;

b. domain name official; and

c. data guardian.

(3) The development as referred to in paragraph (1) is carried out in the form of facilitation, consultation, education and training, and/or development activities.

Division Two
Supervision

Article 100

(1) The Minister supervises the implementation of public scope electronic systems.

(2) Supervision as referred to in paragraph (1) includes monitoring, control, inspection, inquiry and safeguarding.

CHAPTER VIII
TRANSITIONAL PROVISIONS

Article 101

(1) Public Scope PSE that has organized Electronic Systems before this Regulation of the Minister comes into force are required to register no later than 1 (one) year after this Regulation of the Minister comes into force.

(2) Public Scope PSE that has registered before this Regulation of the Minister comes into force are required to register in accordance with the provisions of this Regulation of the Minister no later than 1 (one) year after this Regulation of the Minister comes into force.

(3) Public Scope PSE are required to adjust the implementation of their Electronic Systems in accordance with the provisions in this Regulation of the Minister no later than 1 (one) year after this Regulation of the Minister comes into force.

Article 102

Public Scope PSs that use third-party Cloud Computing service providers before this Regulation of the Minister comes into force must use third-party Cloud Computing service providers registered with the Ministry no later than:

a. 1 (one) year since the Minister publishes a list of third-party Cloud Computing service providers as referred to in Article 97 paragraph (1); or

b. after the Public Scope PSE contract period with the previous third-party Cloud Computing service Provider ends.

CHAPTER IX
CLOSING PROVISION

Article 103

Upon the effective enforcement of this Regulation of the Minister:

a. Regulation of the Minister of Communication and Information Technology Number 5 of 2015 on Domain Name Registrars of State Organizing Agencies (Official Gazette of the Republic of Indonesia Number 209); and

b. Regulation of the Minister of Communication and Information Technology Number 10 of 2015 on Procedures for the Registration of Electronic Systems of State Organizing Agencies (Official Gazette of the Republic of Indonesia Number 320),

are repealed and declared invalid.

Article 104

This Regulation of the Minister comes into force from the date of its promulgation.

For public cognizance, it is hereby ordered that this Regulation of the Minister be promulgated in the Official Gazette of the Republic of Indonesia.

Established in Jakarta
on 18 March 2025
THE MINISTER OF COMMUNICATION AND DIGITAL AFFAIRS OF THE REPUBLIC OF INDONESIA,
Signed.
MEUTYA VIADA HAFID

Promulgated in Jakarta
on 25 March 2025
THE DIRECTOR GENERAL OF LAWS AND REGULATIONS OF
THE MINISTRY OF LAW OF THE REPUBLIC OF INDONESIA,
Signed.
DHAHANA PUTRA

OFFICIAL GAZETTE OF THE REPUBLIC OF INDONESIA OF 2025 NUMBER 225

DISCLAIMER

"This translation was produced by Hukumonline for the purpose of understanding Indonesian law only and does not constitute an official translation published by the Indonesian Government. Hukumonline has made every effort to ensure the accuracy and completeness of the information that is contained within this translation, however, we are not responsible for any errors, omissions and/or mistakes that occur in the source text. Hukumonline reserves the right to change, modify, add or remove any errors or omissions without any prior notification being given. These services are not intended to be used as legal references, advice and/or opinions and no action should be taken as regards the reliability of any of the information contained herein without first seeking guidance from professional services."