REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA
NUMBER 71 OF 2019
ON
THE ORGANIZATION OF ELECTRONIC SYSTEMS AND TRANSACTIONS

BY THE GRACE OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that with the rapid development of information technology for the purpose of boosting the growth of the digital economy and enforcement of state sovereignty over electronic information in the territory of the Unitary State of the Republic of Indonesia, it has been deemed necessary to regulate the utilization of information technology and electronic transaction comprehensively;

b. that Regulation of the Government Number 82 of 2012 on the Organization of Electronic System and Transaction is no longer relevant with the development of public legal needs so it needs to be replaced;

c. that based on the considerations as referred to in letter a and letter b, it has been deemed necessary to establish Regulation of the Government on the Organization of Electronic System and Transaction;

Observing:

1. Article 5 paragraph (2) of the 1945 Constitution of the Republic of Indonesia;

2. Law Number 11 of 2008 on Electronic Information and Transaction (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 by Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952);

HAS DECIDED:

To establish:

REGULATION OF THE GOVERNMENT ON THE ORGANIZATION OF ELECTRONIC SYSTEM AND TRANSACTION.

CHAPTER I
GENERAL PROVISIONS

Article 1

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

1. Electronic System is a series of devices and electronic procedures which function to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate Electronic Information.

2. Electronic Transaction is a legal act which is conducted by using a computer, computer network, and/or other electronic media.
3. Electronic Agent is a device of an Electronic System which is made to conduct an automatic action on a certain Electronic Information which is conducted by a Person.
4. Electronic System Provider is any Person, state administrator, Business Entity, and the public which provides, manages, and/or operates Electronic System individually or jointly to Electronic System User for their own purposes and/or for other parties' purposes.
5. Electronic System Provider in the Public Sector is the organization of Electronic System by the State Administrator Agency or an institution which is appointed by the State Administrator Agency.
6. Electronic System Provider in the Private Sector is the organization of Electronic System by a Person, Business Entity, and public.
7. Ministry or Body is a State Administrator Agency whose duty is to supervise and issue regulations in its sector.
8. Electronic Information is one or a group of Electronic Data, including but not limited to text, voice, picture, map, design, photo, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or similar, letter, sign, number, Access code, symbol, or perforation which has been processed which has meaning or may be understood by people who are able to understand it.
9. Electronic Document is any Electronic Information which is made, forwarded, transmitted, received, or stored in the form of analog, digital, electromagnetic, optical, or similar, which may be seen, displayed and/or heard through computer or Electronic System, including but not limited to text, voice, picture, map, design, photo, or similar, letter, sign, number, Access code, symbol or perforation which has meaning or may be understood by people who are able to understand it.
10. Information Technology is a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.
11. Electronic System User is any Person, state administrator, Business Entity, and the public which utilizes goods, services, facilities, or information which are provided by the Electronic System Provider.
12. Hardware is one or a series of device which is connected to Electronic System.
13. Software is one or a group of computer program, procedure, and/or documentation which is related to the operation of Electronic System.
14. Electronic System Feasibility Test is a series of an objective assessment process for any component of the Electronic System, both conducted individually and/or conducted by an authorized and competent agency.
15. Access is an activity to conduct interaction with an Electronic System which is a stand-alone or in a network.
16. Organization of Electronic Transaction is a series of Electronic Transaction activity which is conducted by the Sender and Recipient by utilizing an Electronic System.
17. Electronic Contract is an agreement of the parties which is made through an Electronic System.
18. Sender is a legal subject who sends an Electronic Information and/or Electronic Document.
19. Recipient is a legal subject who receives an Electronic Information and/or Electronic Document from the Sender.
20. Electronic Certificate is an electronic certificate which contains a Digital Signature and identity which shows the legal subject status of the parties in an Electronic Transaction which is issued by an Electronic Certification Provider.
21. Electronic Certification Provider is a legal entity which functions as a party which is trustworthy, which provides and audits an Electronic Certificate.
22. Digital Signature is a signature which consists of Electronic Information which is adhered to,

associated or related to other Electronic Information which is utilized as a verification and authentication tool.

23. Signer is a legal subject who is associated or related to the Digital Signature.
24. Digital Signature Producing Device is a Software or Hardware which is configured and utilized to make a Digital Signature.
25. Digital Signature Producing Data is private code, biometric code, cryptography code, and/or code which are produced from the alteration of manual signature into Digital Signature, including other signatures which are produced from the development of Information Technology.
26. Reliability Certification Body is an independent body which is established by recognized professionals, validated, and supervised by the Government with authority to audit and issue a Reliability Certificate in an Electronic Transaction.
27. Reliability Certificate is a document which states that the Businesses which organize an Electronic Transaction had passed an audit or a conformity test from the Reliability Certification Body.
28. Businesses are any individuals or Business Entities, both incorporated and not incorporated as a legal entity, which are established and domiciled or carry out activities in the jurisdiction of the Republic of Indonesia, individually or jointly, through a business agreement in various economy sectors.
29. Personal Data is any data on a person which is identified and/or may be identified individually or combined with other information both directly and indirectly through an Electronic System and non-electronic system.
30. Electronic Data is a data in electronic form which is not limited to text, voice, picture, map, design, photo, electronic data interchange (Edi), electronic mail, telegram, telex, telecopy or similar, letter, sign, number, Access code, symbol, or perforation.
31. Domain Name is the internet address of a state administrator, Person, Business Entity, and/or public, which may be utilized in communication through the internet, which is in the form of code or unique character arrangement to show certain locations on the internet.
32. Domain Name Registry is the provider which is responsible for conducting management, operation, and maintenance of the organization of Domain Name Electronic System.
33. Domain Name Registrar is a Person, Business Entity, or public which provides Domain Name registration services.
34. Domain Name User is a Person, State Administrator Agency, or public which submits a registration to use Domain Name to the Domain Name Registrar.
35. State Administrator Agency from this point onwards is referred to as Agency is a legislative, executive, and judicative institutions at the central and regional government and other agencies which are formed with laws and regulations.
36. Person is an individual, both an Indonesian citizen, a foreigner, and a legal entity.
37. Business Entity is a private company or a partnership company, both of which is incorporated or not incorporated as a legal entity.
38. Government is the Minister or other officials who are appointed by the President.
39. Minister is the minister who is in charge of government affairs in the communication and informatics sector.

CHAPTER II

THE ORGANIZATION OF ELECTRONIC SYSTEM

Division One

General

Article 2

(1) The Organization of Electronic System is conducted by the Electronic System Provider.

(2) The Electronic System Provider as referred to in paragraph (1) shall consist of:

a. Electronic System Provider in the Public Sector; and

b. Electronic System Provider in the Private Sector.

(3) The Electronic System Provider in the Public Sector shall consist of:

a. the Agency; and

b. an institution which is appointed by the Agency.

(4) The Electronic System Provider in the Public Sector as referred to in paragraph (2) letter a does not include the Electronic System Provider in the Public Sector which is a regulatory and supervisory authority in the financial services sector.

(5) The Electronic System Provider in the Private Sector as referred to in paragraph (2) letter b shall consist of:

a. The Electronic System Provider which is regulated or supervised by the Ministry or Body based on laws and regulations; and

b. The Electronic System Provider which has an internet-based portal, website, or an application, which is utilized to:

1. provide, manage, and/or operate offering and/or trade goods and/or services;

2. provide, manage, and/or operate financial transaction services;

3. deliver material or paid digital content through data network by downloading through a portal, website, sending of emails, or through other applications to users' devices;

4. provide, manage, and/or operate communication services consisting of, but not limited to short text messages, voice call, video call, electronic mail, and digital chat room, networking services and social media;

5. search engine services, Electronic Information provider services which are in the form of text, voice, picture, animation, music, video, film, and games or partly and/or wholly combination of it; and/or

6. process Personal Data for operational activities which serve the public in relation to Electronic Transaction activities.

Article 3

(1) Any Electronic System Provider shall organize Electronic System in a reliable and safe manner as well as be responsible for the proper operation of the Electronic System.

(2) The Electronic System Provider shall be responsible for the organization of its Electronic Systems.

(3) The provisions as referred to in paragraph (2) do not apply in the event that the occurrence of force majeure, fault, and/or negligence of the Electronic System User may be proven.

Article 4

Insofar that it is not stated otherwise by separate laws and regulations, any Electronic System Provider must operate Electronic System which fulfills the minimum requirements as follows:

a. able to redisplay Electronic Information and/or Electronic Document as a whole in accordance with the retention period which is determined with laws and regulations;

b. able to protect the availability, integrity, authenticity, privacy, and accessibility of Electronic Information in the organization of such Electronic System;

c. able to operate in accordance with the procedures or guidelines in the organization of such Electronic System;

d. is equipped with procedures or guidelines which are announced with a language, information, or symbol which may be understood by the relevant party with the organization of such Electronic System; and

e. has a sustainable mechanism to maintain novelty, clarity and accountability of the procedures and guidelines.

Article 5

(1) The Electronic System Provider must ensure that their Electronic System does not contain Electronic Information and/or Electronic Document which are prohibited in accordance with laws and regulations.

(2) The Electronic System Provider must ensure their Electronic System does not facilitate the dissemination of prohibited Electronic Information and/or Electronic Document in accordance with laws and regulations.

(3) The provision on the obligation of the Electronic System Provider as referred to in paragraph (1) and paragraph (2) shall be regulated with Regulation of the Minister.

Division Two

Registration of Electronic System

Article 6

(1) Any Electronic System Provider as referred to in Article 2 paragraph (2) must conduct registration.

(2) The obligation to conduct registration for the Electronic System Provider shall be conducted before the Electronic System starts to be used by the Electronic System User.

(3) The registration of the Electronic System Provider as referred to in paragraph (1) shall be submitted to the Minister through the electronically integrated business licensing services in accordance with laws and regulations.

(4) Further provisions on the registration of Electronic System Provider as referred to in paragraph (3) shall refer to the norms, standards, procedures, and criteria which are regulated with Regulation of the Minister.

Division Three

Hardware

Article 7

(1) Hardware which is used by the Electronic System Provider shall:

a. meet the security, interconnectivity and compatibility aspects with the used system;

b. have technical support services, maintenance services, and/or aftersales services from the seller or the provider; and

c. have a service continuity warranty.

(2) The fulfillment of requirements as referred to in paragraph (1) shall be conducted through certification or other similar evidences.

Division Four

Software

Article 8

The Software which is utilized by the Electronic System Provider shall:

a. be guaranteed of the security and reliability of proper operation; and

b. ensure of the continuity of the services.

Article 9

(1) The developer who provides Software which is specifically developed for the Electronic System Provider in the Public Sector must submit the source code and documentation of the Software to the relevant Agency or institution.

(2) The relevant Agency or institution as referred to in paragraph (1) must retain the source code and documentation of the Software in a facility in accordance with laws and regulations.

(3) In the event that the facility as referred to in paragraph (2) is not yet available, the Agency or institution may retain the source code and documentation of the Software to a trusted third party which retains the source code.

(4) The developer must guarantee the acquisition and/or Access to the source code and documentation of the Software to the trusted third party as referred to in paragraph (3).

(5) The Electronic System Provider in the Public Sector must guarantee the confidentiality of the utilized Software source code and is only utilized for the benefit of the Electronic System Provider in the Public Sector.

(6) Further provisions on the obligation to transfer the source code and documentation of the Software to the Agency or institution as referred to in paragraph (1) and the retention of source code and documentation of the Software to a trusted third party as referred to in paragraph (3) shall be regulated with Regulation of the Minister.

Division Five

Experts

Article 10

(1) Experts who are recruited by the Electronic System Provider shall have the competency in Electronic System or Information Technology.

(2) Experts as referred to in paragraph (1) must comply with laws and regulations.

Division Six

Electronic System Governance

Article 11

(1) The Electronic System Provider shall guarantee:

a. the availability of service level agreement;

b. the availability of information security agreement on the utilized Information Technology services; and

c. the security of the organized information and internal communication facilities.

(2) The Electronic System Provider as referred to in paragraph (1) shall ensure that any component and integrity of all Electronic System operates properly.

Article 12

The Electronic System Provider shall apply risk management of the occurred damage or loss.

Article 13

The Electronic System Provider shall own a governance policy, operation work procedures, and mechanism for audit which is conducted periodically to the Electronic System.

Article 14

(1) The Electronic System Provider must implement the principles of Personal Data protection in processing Personal Data consisting of:

a. Personal Data collection is conducted in a limited and specific manner, legally valid, fair, with consent and agreement of the Personal Data owner;

b. Personal Data processing is conducted in accordance with its intention;

c. Personal Data processing is conducted by ensuring the rights of the Personal Data owner;

d. Personal Data processing is conducted accurately, completely, not misleading, up-to-date, accountable, and taking the intention of Personal Data processing into consideration;

e. Personal Data processing is conducted by protecting the Personal Data security from loss, misappropriation, Access and illegal disclosure, as well as alteration or destruction of Personal Data;

f. Personal Data processing is conducted by notifying the purpose of collection, processing activities, and failure in protecting Personal Data; and

g. Personal Data processing is destroyed and/or deleted unless in a retention period in accordance with the need based on laws and regulations.

(2) Personal Data processing as referred to in paragraph (1) shall consist of:

a. acquisition and collection;

b. processing and analysis;

c. retention;

d. improvement and update;

e. display, announcement, transfer, dissemination, or disclosure; and/or

f. deletion or destruction.

(3) Personal Data processing shall comply with the provisions of a valid agreement from the Personal Data owner for 1 (one) or certain purposes which have been delivered to the Personal Data owner.

(4) Other than the approval as referred to in paragraph (3), the Personal Data processing shall fulfill the provisions which are required for:

a. the fulfillment of contractual obligation in the event that the Personal Data owner is one of the parties or to fulfill the request of the Personal Data owner upon entering into an agreement;

b. fulfillment of legal obligation from the Personal Data controller in accordance with laws and regulations;

c. fulfillment of vital interest of the Personal Data owner;

d. implementation of Personal Data controller authority based on laws and regulations;

e. fulfillment of Personal Data controller obligation in public services for the public interest; and/or

f. fulfillment of other vital interests of the Personal Data controller and/or Personal Data owner.

(5) If there is a failure in protecting the managed Personal Data, the Electronic System Provider must notify in writing to the Personal Data owner.

(6) Provisions on technical processing of Personal Data are regulated with laws and regulations.

Article 15

(1) Any Electronic System Provider must delete irrelevant Electronic Information and/or Electronic Document which are under their control based on the request of the relevant person.

(2) The obligation to delete irrelevant Electronic Information and/or Electronic Document as referred to in paragraph (1) shall consist of:

a. erasure (right to erasure); and

b. delisting from search engine (right to delisting).

(3) The Electronic System Provider which must delete Electronic Information and/or Electronic Document as referred to in paragraph (1) is the Electronic System Provider which obtains and/or process Personal Data under their control.

Article 16

(1) Irrelevant Electronic Information and/or Electronic Document which is conducted by erasing (right to erasure) as referred to in Article 15 paragraph (2) letter a shall consist of Personal Data which:

a. are acquired and processed without the consent of the Personal Data owner;

b. its consent has been withdrawn by the Personal Data owner;

c. are acquired and processed illegally;

d. no longer in accordance with the acquisition purpose based on an agreement and/or laws and regulations;

e. its utilization has exceeded the period in accordance with an agreement and/or laws and regulations; and/or

f. are displayed by the Electronic System Provider which caused a loss for the Personal Data owner.

(2) The obligation to delete Electronic Information and/or Electronic Document as referred to in paragraph (1) does not apply in the event that the Electronic Information and/or Electronic Document must be retained or is prohibited from being deleted by the Electronic System Provider in accordance with laws and regulations.

Article 17

(1) The deletion of irrelevant Electronic Information and/or Electronic Document which is conducted by delisting from search engine list (right to delisting) as referred to in Article 15 paragraph (2) letter b is conducted based on a court decision.

(2) Petition to conduct delisting of the Electronic Information and/or Electronic Document to a local district court is conducted by the relevant person as the Personal Data owner in accordance with laws and regulations.

(3) Petition to conduct delisting as referred to in paragraph (2) shall contain:

a. identity of the petitioner;

b. identity of the Electronic System Provider and/or Electronic System address;

c. irrelevant Personal Data which is under the control of the Electronic System Provider; and

d. reasons for requesting delisting.

(4) In the event that the court grants the petition to conduct delisting as referred to in paragraph (2), the Electronic System Provider must conduct delisting of the irrelevant Electronic Information and/or Electronic Document.

(5) The court decision as referred to in paragraph (4) shall become the basis to request delisting of the irrelevant Electronic Information and/or Electronic Document by the relevant person to the Electronic System Provider.

Article 18

(1) Any Electronic System Provider must provide a mechanism to delete the irrelevant Electronic Information and/or Electronic Document in accordance with laws and regulations.

(2) The deletion mechanism as referred to in paragraph (1) shall at least contain provisions on:

a. provision of a communication channel between the Electronic System Provider with the Personal Data owner;

b. feature to delete irrelevant Electronic Information and/or Electronic Document which enables the Personal Data owner to delete their Personal Data; and

c. recordation for the request to delete irrelevant Electronic Information and/or Electronic Document.

(3) Further provisions on the deletion mechanism as referred to in paragraph (1) and paragraph (2) shall be regulated with Regulation of the Minister.

(4) Provisions on the deletion mechanism in certain sectors may be established by the Ministry or relevant Body after coordinating with the Minister.

Article 19

(1) The Electronic System Provider shall implement good and accountable governance for the Electronic System.

(2) The governance as referred to in paragraph (1) shall at least fulfill the following requirements:

a. the availability of procedures and guidelines in the organization of Electronic System which is documented and/or announced with a language, information, or symbol which is understood by the party who is in relation to the organization of such Electronic System;

b. there is a sustainable mechanism to maintain novelty and clarity of the implementing guidelines procedures;

c. there is an institutional and completeness of supporting personnel for the proper operation of Electronic System;

d. there is an implementation of performance management in the Electronic System which is organized to ensure that the Electronic system operates properly; and

e. there is a plan to maintain the continuity of the organization of the managed Electronic System.

(3) Other than requirements as referred to in paragraph (2), the relevant Ministry or Body may determine other requirements which are established in laws and regulations.

Article 20

(1) The Electronic System Provider in the Public Sector must own a business continuity plan to overcome disturbance or disaster in accordance with the risk of the impact it causes.

(2) The Electronic System Provider in the Public Sector must conduct management, processing, and/or retention of the Electronic System and Data Electronic in Indonesian territory.

(3) The Electronic System Provider in the Public Sector may conduct management, processing, and/or retention of the Electronic System and Electronic Data outside of the Indonesian territory in the event that the retention technology is not available domestically.

(4) The retention technology criteria is not available domestically as referred to in paragraph (3) shall be determined by a committee consisting of the ministry who is in charge of governmental affairs in the communication and informatics sector, body who is in charge of affairs in technology review and implementation, body who is in charge of affairs in cybersecurity, and the relevant Ministry or Body.

(5) The establishment of the committee as referred to in paragraph (4) is determined by the Minister.

(6) In the event that the Electronic System Provider in the Public Sector utilizes third-party services, the Electronic System Provider in the Public Sector must conduct data classification in accordance with the inflicted risk.

(7) Further provisions on data classification in accordance with risk as referred to in paragraph (6) shall be regulated with Regulation of the Minister.

Article 21

(1) The Electronic System Provider in the Private Sector may conduct management, processing, and/or retention of the Electronic System and Electronic Data in Indonesian territory and/or outside of Indonesian territory.

(2) In the event that the Electronic System and Electronic Data are managed, processed, and/or retained outside of Indonesian territory, the Electronic System Provider in the Private Sector must ensure the effectiveness of supervision by the Ministry or Body and law enforcement.

(3) Electronic System Provider in the Private Sector must provide Access to the Electronic System and Electronic Data for the purpose of supervision and law enforcement in accordance with laws and regulations.

(4) Provisions on management, processing, and retention of Electronic System and Electronic Data for the Electronic System Provider in the Private Sector in the financial sector shall be further regulated by the regulatory and supervisory authority in the financial sector.

Division Seven

Security of Electronic System Organization

Article 22

(1) Electronic System Provider must provide an audit trail for all activities of the Electronic System organization.

(2) Audit trail as referred to in paragraph (1) is utilized for the purpose of supervision, law enforcement, dispute resolution, verification, testing, and other examinations.

Article 23

The Electronic System Provider must conduct security for the components of the Electronic System.

Article 24

(1) The Electronic System Provider must own and operate procedures and facilities for the security of the Electronic System in preventing disturbance, failure, and loss.

(2) The Electronic System Provider must facilitate a security system which covers the procedures and prevention and control system upon a threat and attack which causes a disturbance, failure, and loss.

(3) In the event that there is a system failure or disturbance which has a serious impact as a result of other parties action to the Electronic System, the Electronic System Provider must secure the Electronic Information and/or Electronic Document and shall immediately report in the first place to the law enforcement and the relevant Ministry or Body.

(4) Further provisions on the security system as referred to in paragraph (2) shall be regulated in regulation of the head of agency who is in charge of governmental affairs in the cybersecurity sector.

Article 25

The Electronic System Provider must redisplay the Electronic Information and/or Electronic Document as a whole in accordance with the format and retention period which is established based on laws and regulations.

Article 26

(1) The Electronic System Provider must maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of Electronic Information and/or Electronic Document in accordance with laws and regulations.

(2) In the organization of the Electronic System which is aimed at transferable Electronic Information and/or Electronic Document, the Electronic Information and/or Electronic Document shall be unique as well as explaining its possession and ownership.

Article 27

The Electronic System Provider shall ensure that the Electronic System functions in accordance with its designation by taking into consideration the interoperability and compatibility with the previous Electronic System and/or the relevant Electronic System.

Article 28

(1) The Electronic System Provider must provide education to the Electronic System User.

(2) The Education as referred to in paragraph (1) shall at least consist of the rights, obligations, and responsibilities of all related parties, as well as procedures to submit a complaint.

Article 29

The Electronic System Provider must provide information to the Electronic System User at least on:

a. identity of the Electronic System Provider;
b. the transacted object;
c. feasibility or security of the Electronic System;
d. procedures for device utilization;
e. contract terms;
f. procedures to reach agreement;
g. privacy and/or protection of Personal Data guarantee; and
h. phone number of the complaint center.

Article 30

(1) The Electronic System Provider must provide features in accordance with the characteristics of the utilized Electronic System.

(2) Features as referred to in paragraph (1) shall at least in the form of facilities to:

a. make correction;
b. cancel a command;
c. provide a confirmation or reconfirmation;
d. choose to continue or to stop the next activity;
e. view the submitted information in the form of Electronic Contract offers or advertisement;
f. check the success or failure of an Electronic Transaction; and
g. read an agreement before conducting an Electronic Transaction.

Article 31

The Electronic System Provider must protect its user and public from loss due to the organized Electronic System.

Article 32

(1) Any person who works within the Electronic Systems organization must secure and protect the facilities and infrastructure of Electronic System or information which are distributed through the Electronic System.

(2) The Electronic System Provider must provide, educate, and train the personnel whose duties and responsibilities are concerned with the security and protection of facilities and infrastructure of the Electronic System.

Article 33

For the purpose of criminal justice process, the Electronic System Provider must provide the Electronic Information and/or Electronic Data which are contained in the Electronic System or Electronic Information and/or Electronic Data which are processed by the Electronic System at a valid request from an investigator

for certain criminal act in accordance with the authority regulated in laws.

Division Eight

Feasibility Test for Electronic System

Article 34

(1) The Electronic System Provider must conduct a Feasibility Test for Electronic System.

(2) The obligation as referred to in paragraph (1) may be implemented to all components or parts of components in the Electronic System in accordance with the characteristics of the needs for protection and strategic nature of the organization of the Electronic System.

Division Nine

Supervision

Article 35

(1) The Minister is authorized to conduct supervision upon the organization of the Electronic System.

(2) The supervision as referred to in paragraph (1) shall consist of monitoring, controlling, examination, searching, and security.

(3) The provisions on supervision for the organization of Electronic systems in certain sectors must be established by the relevant Ministry or Body after coordinating with the Minister.

CHAPTER III

THE ELECTRONIC AGENT PROVIDER

Division One

Electronic Agent

Article 36

(1) The Electronic System Provider may organize its Electronic System independently or through an Electronic Agent.

(2) The Electronic Agent as referred to in paragraph (1) is a part of the Electronic System.

(3) The obligation of the Electronic System Provider shall apply mutatis mutandis for the Electronic Agent provider.

(4) The Electronic Agent may be in the form of:

a. visual;

b. audio;

c. Electronic Data; and

d. other forms.

Article 37

(1) The Electronic Agent Provider must include or deliver information to protect the rights of the user in the organized Electronic Agent, including at least information on:

a. the identity of the Electronic Agent provider;

b. the transacted object;

c. the feasibility or security of the Electronic Agent;

d. procedures for device utilization;

e. contract terms;

f. procedures to reach agreement;

g. privacy and/or protection of Personal Data guarantee; and

h. phone number of complaint centers.

(2) The Electronic Agent Provider must include or provide features for the purpose of protecting users' rights in the organized Electronic Agent in accordance with the characteristics of the utilized Electronic Agent.

(3) The features as referred to in paragraph (2) shall be in the form of facilities to:

a. make corrections;

b. cancel orders;

c. give confirmation or reconfirmation;

d. choose to continue or to stop the next activities;

e. see the submitted information in the form of an Electronic Contract offering or advertisement;

f. check the success or failure of a transaction; and/or

g. read an agreement before conducting a transaction.

(4) The Electronic Agent Provider shall provide a feature in the operated Electronic Agent which enables its users to make changes to the information which is still in the transaction process.

Article 38

(1) The Electronic Agent may be organized for more than 1 (one) interest of the Electronic System Provider which shall be based on an agreement between the parties.

(2) The agreement as referred to in paragraph (1) shall contain at least:

a. rights and obligations;

b. responsibilities;

c. a mechanism for complaint and dispute settlement;

d. time period;

e. fees;

f. scope of services; and

g. choice of law.

(3) In the event that the electronic Agent is organized for more than 1 (one) interest of the Electronic System Provider, the Electronic Agent provider must provide the same treatment for the Electronic System Provider which utilizes such Electronic Agent.

(4) In the event that the Electronic Agent is organized for more than 1 (one) Electronic System Provider,

such Electronic Agent provider is deemed as a separate Electronic System Provider.

Division Two

Obligations

Article 39

(1) In the organization of the Electronic Agent, the Electronic Agent provider shall take into considerations the following principles:

a. prudential;

b. security and integration of the Information Technology system;

c. security control for the Electronic Transaction activities;

d. cost-effectiveness and efficiency; and

e. consumers' protection in accordance with laws and regulations.

(2) The Electronic Agent provider must own and perform the standard operating procedures which fulfill the security control of users' data and Electronic Transaction principles.

(3) The security control of users' data and Electronic Transaction principles as referred to in paragraph (2) shall consist of:

a. confidentiality;

b. integrity;

c. availability;

d. authenticity;

e. authorization; and

f. non-repudiation.

Article 40

(1) The Electronic Agent provider must:

a. conduct identity authenticity testing and examine the authorization of the Electronic System User which conducts the Electronic Transaction;

b. own and implement the policy and procedures to take measures if there is an indication of data theft;

c. ensure that the control of authorization and access rights to the system, database, and application of the Electronic Transaction;

d. formulate and implement methods and procedures to protect and/or conceal the integrity of data, record, and information in relation to the Electronic Transaction;

e. own and implement the standard and control of data utilization and protection if the service provider party has Access to such data;

f. own a business continuity plan including an effective contingency plan to ensure the availability of the Electronic Transaction system and services in a continuous manner; and

g. own a quick and precise procedure for the handling of unexpected events in order to reduce the impact of an incident, fraud, and failure of the Electronic System.

(2) The Electronic Agent provider must formulate and determine a procedure to secure the Electronic

Transaction, so that it is unable to be denied by the consumers.

CHAPTER IV
THE ORGANIZATION OF ELECTRONIC TRANSACTION

Division One
The Scope of Electronic Transaction Organization

Article 41

(1) The organization of Electronic Transactions may be conducted within the public or private scope.

(2) The organization of Electronic Transaction in the public sector shall consist of the organization of Electronic Transaction by:

a. the Agency;

b. institutions which are appointed by the Agency;

c. between Agencies;

d. between the appointed institutions;

e. between the Agency and the appointed institutions; and

f. between the Agency or institution and Businesses in accordance with laws and regulations.

(3) The organization of Electronic Transaction in the private sector shall consist of the following Electronic Transactions:

a. between Businesses;

b. between Businesses with consumers; and

c. between individuals.

Division Two
Requirements for the Organization of Electronic Transaction

Article 42

(1) The organization of Electronic Transaction must utilize the Electronic Certificate which is issued by an Indonesian Electronic Certification Provider.

(2) The organization of Electronic Transaction may utilize a Feasibility Certificate.

(3) In the event of using the Feasibility Certificate as referred to in paragraph (2), the Organization of Electronic Transaction must utilize the Feasibility Certificate which is issued by a registered Feasibility Certification Agency.

Article 43

The organization of Electronic Transaction which is conducted by the Electronic System Provider in the Public Sector shall take security, reliability, and efficiency aspects into consideration.

Article 44

(1) The Sender must ensure that the Electronic Information which is sent is valid and is not disturbing.

(2) Further provisions on the delivery of Electronic Information shall be regulated in Regulation of the Minister.

Division Three

Requirements for Electronic Transaction

Article 45

(1) Electronic Transaction which is conducted by the parties shall have legal implications to the parties.

(2) The Organization of Electronic Transaction which is conducted by the parties shall take the following aspects into considerations:

a. good faith;

b. prudential principles;

c. transparency;

d. accountability; and

e. fairness.

Article 46

(1) An Electronic Transaction may be conducted based on an Electronic Contract or other contractual forms as a form of agreement which is conducted by the parties.

(2) An Electronic Contract shall be deemed valid if:

a. there is an agreement between the parties;

b. is conducted by a legal subject which is capable or authorized to represent in accordance with laws and regulations;

c. there are certain matters; and

d. transaction object must not contradict with laws and regulations, decency, and public order.

Article 47

(1) The Electronic Contract and other contractual forms as referred to in Article 46 paragraph (1) which is addressed to Indonesian citizens shall be drawn up in Bahasa Indonesia.

(2) The Electronic Contract which is drawn up with a standard clause shall be in accordance with provisions on standard clause as regulated in laws and regulations.

(3) Electronic Contract shall at least consist of:

a. data of the parties' identities;

b. object and specification;

c. requirements for Electronic Transaction;

d. price and costs;

e. procedures in the event that there is a cancellation by the parties;

f. provisions which grant a right to the injured party to return the goods and/or request a replacement product if there is a latent defect; and

g. choice of law for the settlement of Electronic Transaction.

Article 48

(1) Businesses which offer products through an Electronic System shall provide complete and valid information in relation to contractual terms, producer, and the offered products.

(2) Businesses must provide information clarity on contract offering or advertisement.

(3) Businesses must give a time limit for the consumer and/or contract recipient to return the delivered goods and/or offered services if it is not in accordance with the contract or there is a latent defect.

(4) Businesses must provide information on goods which have been delivered and/or services which are offered.

(5) Businesses are unable to impose consumers on the obligation to pay the delivered goods and/or the offered services without a contract as the basis.

Article 49

(1) Electronic Transaction occurs when an agreement between the parties is reached.

(2) Unless specified otherwise, the agreement as referred to in paragraph (1) occurs when the transaction offering which is sent by the Sender has been received and approved by the Recipient.

(3) The agreement as referred to in paragraph (2) may be conducted by the following methods:

a. retrieval action which states an agreement; or

b. retrieval action and/or utilization of objects by the Electronic System User.

Article 50

(1) In the Organization of Electronic Transaction the parties shall guarantee:

a. the provision of valid data and information; and

b. the availability of facilities and services as well as complaint settlement.

(2) In the Organization of Electronic Transaction the parties shall determine the choice of law in an equal manner upon the implementation of Electronic Transaction.

CHAPTER V

THE ORGANIZATION OF ELECTRONIC CERTIFICATION

Division One

Electronic Certificate

Article 51

(1) The Electronic System Provider as referred to in Article 2 paragraph (2) must own an Electronic Certificate.

(2) The Electronic System User may utilize an Electronic Certificate in an Electronic Transaction.

(3) To own an Electronic Certificate, the Electronic System Provider and the Electronic System User shall submit an application to the Indonesian Electronic Certification Provider.

(4) If necessary, the Ministry or Body may require the Electronic System User to utilize an Electronic Certificate in an Electronic Transaction.

(5) Further provisions on the utilization of Electronic Certificate as referred to in paragraph (4) shall be regulated by the Ministry or Body.

(6) Further provisions on procedures to own an Electronic Certificate shall be regulated in Regulation of the Minister.

Division Two

The Electronic Certification Provider

Article 52

The Electronic Certification Provider is authorized to:

a. examine the prospective owner and/or holder of the Electronic Certificate, issuance of Electronic Certificate, the extension of Electronic Certificate validity period, blocking and revocation of Electronic Certificate, validation of Electronic Certificate; and making a list of active and revoked Electronic Certificate; and

b. making, verification, and validation of Digital Signature and/or other services which utilize Electronic Certificate.

Article 53

(1) The Electronic Certification Provider shall consist of:

a. Indonesian Electronic Certification Provider; and

b. Foreign Electronic Certification Provider.

(2) The organization of Indonesian electronic certification shall adhere to single parent principle.

(3) The organization of Indonesian Electronic Certification must obtain an acknowledgment from the Minister with a stance to the parent Electronic Certification Provider which is organized by the Minister.

(4) Indonesian Electronic Certification Provider shall obtain an assessment from a certification body of the accredited Electronic Certification Provider.

(5) Foreign Electronic Certification Provider which operates in Indonesia shall be registered in Indonesia.

(6) Further provisions on registration of foreign Electronic Certification Provider as referred to in paragraph (5) shall be regulated with Regulation of the Minister.

Article 54

(1) The acknowledgment of the Indonesian Electronic Certification Provider as referred to in Article 53 paragraph (3) shall be granted by the Minister after the Indonesian Electronic Certification Provider fulfills the requirement for acknowledgment process which is regulated in Regulation of the Minister.

(2) The acknowledgement list of the Indonesian Electronic Certification Provider shall include the organized services and shall be made, maintained, and published by the Minister.

(3) Further provisions on procedures for the acknowledgement of Indonesian Electronic Certification Provider shall be regulated in Regulation of Minister.

Article 55

(1) The Indonesian Electronic Certification Provider is entitled to obtain revenue by imposing services fees from the Electronic Certificate users.

(2) The Indonesian Electronic Certification Provider must deposit any revenue from the utilization of Electronic Certificate services fee which is calculated from the revenue percentage to the state.

(3) The revenue as referred to in paragraph (1) and paragraph (2) is a non-tax state revenue.

Division Three

Supervision

Article 56

(1) The Minister shall conduct supervision upon:

a. the organization of the Indonesian electronic certification; and

b. the Organization of the foreign Electronic Certification.

(2) Supervision for the organization of the Indonesian electronic certification as referred to in paragraph (1) letter a shall consist of:

a. acknowledgment; and

b. the operation of parent Electronic Certification Provider facilities for the Indonesian Electronic Certification Provider.

(3) Further provisions on the supervision of the organization of the Indonesian electronic certification and the Organization of the foreign Electronic Certification shall be regulated in Regulation of the Minister.

Division Four

Electronic Certification Provider Services

Sub-Division 1

General

Article 57

(1) The Indonesian Electronic Certification Provider shall provide certified services.

(2) The services as referred to in paragraph (1) shall consist of:

a. Digital Signature; and/or

b. other services which utilize Electronic Certificate.

(3) Other services as referred to in paragraph (2) letter b shall consist of:

a. electronic seal;

b. electronic timer;

c. recorded electronic delivery services;

d. website authentication; and/or

e. preservation of Digital Signature and/or electronic seal.

Article 58

(1) The Indonesian Electronic Certification Provider shall endure the loss which is resulted by intention or negligence to Person, Business Entity or Agency due to the failure in complying its obligations as regulated in this Regulation of the Government.

(2) The Indonesian Electronic Certification Provider is considered to be intentional or negligent unless such Indonesian Electronic Certification Provider is able to prove that the loss does not occur due to their intentional or negligence.

(3) The burden of proof for the intention or negligence which is conducted by the party which is not the Indonesian Electronic Certification shall become the responsibility of the injured Person, Business Entity or Agency.

Sub-Division 2

Digital Signature

Article 59

(1) A Digital Signature which is utilized in Electronic Transaction may be produced through various signing procedures.

(2) In the event that the utilization of a Digital Signature represents a Business Entity, its Digital Signature is referred to as an electronic seal.

(3) The Digital Signature as referred to in paragraph (1) and paragraph (2) shall have valid legal force and legal implications insofar that it fulfills the following requirements:

a. Digital Signature Producing Data is only related to the Signer;

b. Digital Signature Producing Data upon the electronic signing process is only in the authority of the Signer;

c. any changes to the Digital Signature which occur after the singing is discoverable;

d. any changes to the Electronic Information which is related to such Digital Signature after the signing is discoverable;

e. there are certain methods which are used to identify who is the Signer; and

f. there are certain methods to show that the Signer has provided approval for the relevant Electronic Information.

Article 60

(1) A Digital Signature shall function as the authentication and verification for:

a. the identity of the Signer; and

b. the integrity and authenticity of Electronic Information.

(2) A Digital Signature shall consist of:

a. a certified Digital Signature; and

b. an uncertified Digital Signature.

(3) The Certified Digital Signature as referred to in paragraph (2) letter a shall:

a. fulfill the validity of legal force and legal implications of a Digital Signature as referred to in Article 59 paragraph (3);

b. utilize an Electronic Certificate which is made by the service of the Indonesian Electronic Certification Provider; and

c. be made by using a certified Digital Signature Producing Device.

(4) The Uncertified Digital Signature as referred to in paragraph (2) letter b is made without using the services of the Indonesian Electronic Certification Provider.

Sub-Division 3

Digital Signature Producing Data

Article 61

(1) Digital Signature Producing Data shall uniquely refer only to the Signer and able to be utilized to identify the Signer.

(2) The Digital Signature Producing Data as referred to in paragraph (1) may be established by the Electronic Certification Provider.

(3) The Digital Signature Producing Data as referred to in paragraph (1) and paragraph (2) shall fulfill the following provisions:

a. if using the cryptography code, the Digital Signature Producing Data shall be difficult to be known from the verification data of the Digital Signature through certain calculation, in a certain period, and with a reasonable device;

b. The Digital Signature Producing Data shall be retained in an electronic media which is in possession of the Signer; and

c. The data which is in relation to the Signer must be retained in a place or data storage facilities which utilize a trusted system owned by the Electronic Certification Provider which may detect changes and fulfills the following requirements:

1. only the authorized person is able to input new data, change, exchange, or replace data;

2. the authenticity of identity information of the Signer may be examined; and

3. other technical changes which violate the security requirements may be detected or discovered by the provider.

d. if the Digital Signature Producing Data is made by the Electronic Certification Provider, therefore the whole process of making Digital Signature Producing Data shall be guaranteed of its security and confidentiality by the Electronic Certification Provider.

(4) The Signer shall maintain confidentiality and be responsible for the Data of Digital Signature Establishment.

Article 62

(1) In the signing process, a mechanism shall be conducted to ensure the verification data of the Digital Signature is related to the Digital Signature Producing Data and is still valid or not revoked.

(2) In the signing process, a mechanism shall be conducted to ensure the Digital Signature Producing Data:

a. is not reported missing;

b. is not reported transferred to an unauthorized person; and

c. is in the authority of the Signer.

(3) Before the signing, the Electronic Information which will be signed shall be known and understood by the Signer.

(4) Approval of the Signer upon the Electronic Information which will be signed with a Digital Signature shall utilize an affirmation mechanism and/or other mechanisms which indicate the purpose and objectives of the Signer to be bound in an Electronic Transaction.

(5) The Digital Signature in an Electronic Information shall at least:

a. is made by utilizing Digital Signature Producing Data; and

b. include the signing time.

(6) Changes to the Digital Signature and/or Electronic Information which is signed after the signing shall be known, detected, or identified by certain methods or certain means.

Article 63

(1) The Signer may entrust the Digital Signature Producing Data to the Electronic Certification Provider.

(2) The Digital Signature Producing Data as referred to in paragraph (1) may be entrusted only to the Indonesian Electronic Certification Provider.

(3) In the event that the Electronic Certification Provider retains Data of Digital Signature Establishment, the Electronic Certification Provider must:

a. ensure the utilization of the Digital Signature Producing Data is only in the authority of the Signer;

b. utilize a certified Digital Signature Establishment Device in the preparation process of Digital Signature Producing Data; and

c. ensure the utilized mechanism for the utilization of Digital Signature Producing Data for Digital Signature applies a minimum combination of 2 (two) authentication factors.

(4) The provisions on certified Digital Signature Producing Device as referred to in paragraph (3) letter b is established in Regulation of the Minister.

Article 64

(1) Prior to the utilization of the Digital Signature, the Electronic Certification Provider must ensure the initial identification of the Signer by the following methods:

a. the Signer shall submit the identity to the Electronic Certification Provider;

b. the Signer shall conduct registration to the Electronic Certification Provider; and

c. if necessary, the Electronic Certification Provider may transfer in private the identity data of the Signer to other Electronic Certification Provider with the approval from the Signer.

(2) The utilized mechanism for the utilization of the Digital Signature Producing Data for Digital Signature shall apply minimum combination of 2 (two) authentication factors.

(3) The verification process of the signed Electronic Information may be conducted by examining the Digital Signature verification data to track any changes to the signed data.

Sub-Division 4

Electronic Seal

Article 65

Regulation of Digital Signature shall apply mutatis mutandis upon the regulation of the electronic seal.

Sub-Division 5

Electronic Timer

Article 66

Electronic timer services shall consist of:

a. certified electronic timer services; and

b. uncertified electronic timer services.

Article 67

(1) Requirements for a certified electronic timer shall fulfill the following provisions:

a. bind the date and time on the Electronic Information and/or Electronic Document to prevent the possibility of the Electronic Information and/or Electronic Document is changed without being detected;

b. refer to the accurate time source which is related to the coordinated universal time;

c. utilize Electronic Certification which is made by the service of Indonesian Electronic Certification Provider; and

d. is signed by using Digital Signature or electronic seal which is organized by the Indonesian Electronic Certification Provider or by using an equal method.

(2) The certified electronic timer shall provide:

a. date and time accurately; and

b. the integrity of the Electronic Information and/or Electronic Document which is in relation to the date and time.

(3) Uncertified electronic timer service is made without using the services of the Indonesian Electronic Certification Provider.

(4) Further provisions on the certified electronic timer shall be regulated with regulation of the Minister.

Division 6

Recorded Electronic Delivery Service

Article 68

Recorded Electronic Delivery Service shall consist of:

a. certified recorded electronic delivery services; and

b. uncertified recorded electronic delivery services.

Article 69

(1) Certified Electronic Certification Provider which organizes certified recorded electronic delivery services must ensure:

a. the integrity of the transmitted data;

b. the data sender may be identified;

c. the data receiver may be identified; and

d. the accuracy of delivery date and time and data retrieval.

(2) Certified recorded electronic delivery services as referred to in paragraph (1) shall fulfill requirements at least:

a. is organized by 1 (one) Indonesian Electronic Certification Provider or more;

b. able to identify the Sender accurately;

c. may identify the Recipient address before sending the data;

d. delivery and retrieval of data shall be secured by a Digital Signature and electronic seal from the Indonesian Electronic Certification Provider;

e. changes to data in the delivery process or data retrieval may be known by the Sender and the Recipient; and

f. time and date delivery, retrieval, and changes to data may be displayed with a certified electronic timer.

(3) If the data delivery involves 2 (two) Indonesian Electronic Certification Providers or more, all the requirements as referred to in paragraph (2) shall apply to all the involved Indonesian Electronic Certification Providers.

(4) Uncertified recorded electronic delivery service is made without using the service of Indonesian Electronic Certification Provider.

(5) Further provisions on recorded electronic delivery services shall be regulated with Regulation of the Minister.

Sub-Division 7

Website Authentication

Article 70

Website authentication shall consist of:

a. certified website authentication; and

b. uncertified website authentication.

Article 71

(1) The Electronic Certification Provider which provides website authentication services shall own a reliable method which is able to identify a Person or a Business Entity which is responsible for the organization of website which utilizes the website authentication services.

(2) Website authentication is aimed to ensure trust in a transaction electronically through a website.

(3) Certified websites authentication shall utilize Electronic Certificate which is made by the services of the Indonesian Electronic Certification Provider.

(4) The information which shall be contained in an Electronic Certificate which is utilized for websites authentication shall consist of, but not limited to:

a. name of the Person, Business Entity, or Agency which organizes the website;

b. address of the Person, Business Entity, or Agency which at least explains the domicile city where the Person, Business Entity, or the Agency operates;

c. Domain Name which is operated by the website administrator;

d. the validity period of the Electronic Certificate;

e. identity of the Electronic Certification Provider which issues the Electronic Certificate; and

f. Electronic Certificate number.

(5) Uncertified website authentication is made without using the service of the Indonesian Electronic Certification Provider.

(6) Further provisions on certified website authentication as referred to in paragraph (3) shall be regulated with Regulation of the Minister.

Sub-Division 8

Preservation of Digital Signature and/or Electronic Seal

Article 72

(1) Preservation of Digital Signature and/or electronic seal shall consist of:

a. preservation of a certified Digital Signature and/or electronic seal; and

b. preservation of an uncertified Digital Signature and/or electronic seal.

(2) Preservation of certified Digital Signature and/or electronic seal shall fulfill the following provisions:

a. utilize an Electronic Certificate which is made by the service of Indonesian Electronic Certification Provider; and

b. the certified Digital Signature and/or electronic seal which is contained in Electronic Information and/or Electronic Document is still able to be validated although the validity period of the Electronic Certificate has elapsed.

(3) Preservation of an uncertified Digital Signature and/or electronic seal is made without using the service of the Indonesian Electronic Certification Provider.

(4) Further provisions on the preservation of a certified Digital Signature and/or electronic seal shall be regulated with Regulation of Minister.

CHAPTER VI

RELIABILITY CERTIFICATION BODY

Article 73

(1) Businesses which organize Electronic Transaction may be certified by the Reliability Certification Body.

(2) Reliability Certification Body shall be domiciled in Indonesia.

(3) Reliability Certification Body shall be established by professionals.

(4) The Professionals who establish the Reliability Certification Body as referred to in paragraph (3) shall at least consist of the following profession:

a. Information Technology consultant;

b. Information Technology auditor; and

c. legal consultant in the Information Technology sector.

(5) The Reliability Certification Body shall be registered in the list of Reliability Certification Body which is issued by the Minister.

(6) Further provisions on requirements for the establishment of the Reliability Certification Body shall be regulated with Regulation of the Minister.

Article 74

(1) A Reliability Certificate is intended to protect consumers in an Electronic Transaction.

(2) The Reliability Certificate as referred to in paragraph (1) is a guarantee that the Businesses have fulfilled the criteria which are determined by the Reliability Certification Body.

(3) Businesses which have fulfilled the criteria as referred to in paragraph (2) have the right to utilize the Reliability Certificate on a page and/or other Electronic System.

Article 75

(1) The Reliability Certification Body may issue a Reliability certificate through a Reliability Certification process.

(2) The Reliability Certification Process as referred to in paragraph (1) shall include the examination upon complete and valid information from Businesses along with its Electronic System.

(3) The Complete and valid information as referred to in paragraph (2) shall include but not limited to information which:

a. contains the identity of the Business Entity;

b. contains the policy and procedures for privacy protection;

c. contains the policy and procedures for system security; and

d. contains a guarantee statement for the offered goods and/or services.

Article 76

(1) The Reliability Certificate which is issued by the Reliability Certification Body shall consist of the following categories:

a. identity registration;

b. Electronic System security; and

c. privacy policy.

(2) The fulfillment of categorization as referred to in paragraph (1) shall determine the level of the Reliability Certificate.

(3) Further provisions on the regulation of Reliability Certificate Level as referred to in paragraph (2) shall be regulated with Regulation of Minister.

Article 77

Supervision of Reliability Certification Body shall be implemented by the Minister.

Article 78

(1) In order to obtain acknowledgement for the Reliability Certification Body, administration fees shall be

imposed.

(2) Any revenue from the administration fees as referred to in paragraph (1) is a non-tax state revenue.

CHAPTER VII
THE MANAGEMENT OF DOMAIN NAME

Article 79

(1) The management of Domain Name shall be organized by Domain Name administrator.

(2) Domain Name shall consist of:

a. high-level generic Domain Name;

b. high-level Indonesian Domain Name;

c. second-level Indonesian Domain Name; and

d. derivative-level Indonesian Domain Name.

(3) The Domain Name administrato as referred to in paragraph (1) shall consist of:

a. Domain Name Registry; and

b. Domain Name Registrar.

Article 80

(1) Domain Name Administrator as referred to in Article 79 paragraph (2) may be organized by the Government and/or public.

(2) Public as referred to in paragraph (1) shall be incorporated as an Indonesian legal entity.

(3) Domain Name Administrator shall be determined by the Minister.

Article 81

(1) Domain Name Registry as referred to in Article 79 paragraph (3) letter a shall implement the management of high-level generic Domain Name and high-level Indonesian Domain Name.

(2) Domain Name Registry may give registration authority of high-level generic Domain Name and high-level Indonesian Domain Name to the Domain Name Registrar.

(3) Domain Name Registry shall function to:

a. provide a suggestion for the plan to regulate Domain Name to the Minister;

b. conduct supervision upon Domain Name Registrar; and

c. settle the dispute of Domain Name.

(4) Further provisions on dispute settlement of Domain Name as referred to in paragraph (3) letter c shall be regulated with Regulation of the Minister.

Article 82

(1) Domain Name Registrar as referred to in Article 79 paragraph (3) letter b shall conduct the management of second-level Indonesian Domain Name and derivative-level Indonesian Domain Name.

(2) Domain Name Registrar shall consist of:

a. Agency Domain Name Registrar; and

b. Non-Agency Domain Name Registrar.

(3) Agency Domain Name Registrar shall implement the registration of second-level Indonesian Domain Name and derivative-level Indonesian Domain Name for Agency needs.

(4) Agency Domain Name Registrar as referred to in paragraph (3) shall be implemented by the Minister.

(5) For military purposes, Agency Domain Name Registrar as referred to in paragraph (3) shall be implemented by the minister who is in charge of governmental affairs in the defense and security sector.

(6) Non-Agency Domain Name Registrar shall conduct registration of second-level Indonesian Domain Name for commercial and non-commercial users.

(7) Non-Agency Domain Name Registrar must be registered with the Minister

Article 83

(1) Registration of Domain Name is implemented based on the first registrant principle.

(2) The registered Domain Name as referred to in paragraph (1) shall fulfill the following requirements:

a. in accordance with laws and regulations;

b. propriety in society; and

c. good faith.

(3) Domain Name Registry and Domain Name Registrar are authorized to:

a. reject the registration of a Domain Name if the Domain Name fails to fulfill the requirements as referred to in paragraph (2);

b. temporarily deactivate the utilization of Domain Name; or

c. delete Domain Name if the Domain Name users violate the provisions in this Regulation of the Government.

Article 84

(1) Domain Name Registry and Domain Name Registrar must organize the management of Domain Name in an accountable manner.

(2) In the event that the Domain Name Registry or Domain Name Registrar is intended to terminate its management, the Domain Name Registry or Domain Name Registrar must transfer all management of Domain Name to the Minister within 3 (three) months before.

Article 85

(1) Domain Name which indicates an Agency may only be registered and/or utilized by the relevant Agency.

(2) The Agency shall utilize the Domain Name in accordance with the name of the relevant Agency.

Article 86

(1) Domain Name Registry and Domain Name Registrar shall approve the registration of Domain Name upon request of the Domain Name User.

(2) Domain Name User as referred to in paragraph (1) shall be responsible for the Domain Name which they register.

Article 87

(1) Domain Name Registry and/or Domain Name Registrar has the right to earn income by imposing Domain Name registration and/or utilization fees from the Domain Name User.

(2) In the event that the Domain Name Registry and Domain Name Registrar as referred to in paragraph (1) is the administrator of Non-Agency Domain Name, Domain Name Registry and Domain Name Registrar must deposit part of the revenue from the Domain name registration and utilization which is calculated from the revenue percentage to the state.

(3) Revenue as referred to in paragraph (1) and state revenue as referred to in paragraph (2) is a non-tax state revenue.

Article 88

Supervision of the management of Domain Name shall be implemented by the Minister.

Article 89

Further provisions on requirements and procedures for the determination of Domain Name administrator shall be regulated in Regulation of the Minister.

CHAPTER VII

GOVERNMENT ROLE

Article 90

Government Role in the organization of the Electronic system and Transaction shall consist of:

a. facilitating the utilization of Information Technology and Electronic Transaction in accordance with laws and regulations;

b. protecting the public interest from any kinds of disturbance due to misuse of Electronic Information and Electronic Transaction which disturbs the public order, in accordance with laws and regulations;

c. preventing the dissemination and utilization of Electronic Information and/or Electronic Document which has prohibited content in accordance with laws and regulations; and

d. determining an Agency or institution which has strategic Electronic Data which must be protected.

Article 91

Government Role to facilitate the utilization of Information Technology and Electronic Transaction as referred to in Article 90 letter a shall consist of:

a. policy determination;

b. policy implementation;

c. infrastructure facilitation;

d. promotion and education; and

e. supervision.

Article 92

Infrastructure facilitation as referred to in Article 91 letter c shall consist of:

a. development and organization of national Electronic System gateway;

b. development and organization of Information Technology forensic facilities;

c. organization of parent electronic certification;

d. organization of data center and national disaster recovery center in an integrated manner for the purpose of organizing electronic-based government affairs;

e. Electronic System security facilities to prevent attacks against vital information infrastructure in strategic sectors;

f. facilities to deposit or retain source code and documentation of software for Agency; and

g. other facilities which are required to facilitate the utilization of Information Technology and Electronic Transaction based on laws and regulations.

Article 93

(1) Promotion and education as referred to in Article 91 letter d shall be implemented by the Agency in accordance with its authority based on laws and regulations to realize the utilization of Information Technology and Electronic Transaction which is safe, ethical, smart, creative, productive, and innovative.

(2) The implementation of promotion and education may involve stakeholders, including the public and/or Information Technology and Electronic Transaction activities.

Article 94

(1) Government Role to protect the public interest from any kinds of disturbance due to misuse of Electronic Information and Electronic Transaction which disturb public order as referred to in Article 90 letter b shall consist of:

a. determination of national cybersecurity strategy which is a part of the national security strategy including the development of cybersecurity culture;

b. regulating the information security standards;

c. regulating the protection for vital information infrastructure;

d. regulating the risk management for the organization of Electronic System;

e. regulating human resources in the organization of Electronic System protection;

f. development and supervision of the protection for vital information infrastructure;

g. development and supervision of risk management for the organization of Electronic System;

h. development and supervision of human resources in Electronic System protection;

i. organizing the security of Electronic Information;

j. organizing the handling of an information security incident;

k. organizing the handling of emergency response; and

l. other functions which are required to protect the public interest from any kind of disturbance.

(2) The authority as referred to in paragraph (1) may be implemented through a cooperation with other parties.

Article 95

Government Role to prevent dissemination and utilization of Electronic Information and/or Electronic Document which has prohibited content in accordance with laws and regulations as referred to in Article 90 letter c in the form of:

a. Access termination; and/or

b. order the Electronic System Provider to terminate the Access

to the Electronic Information and/or Electronic Document.

Article 96

Access Termination is conducted to Electronic Information and/or Electronic Document as referred to in Article 95 with the following classifications:

a. violate laws and regulations;

b. unsettling public and disturb public disorder; and

c. inform the methods or provide Access to Electronic Information and/or Electronic Document which contains prohibited content in accordance with laws and regulations.

Article 97

(1) The public may submit an application for the termination of Access to Electronic Information and/or Electronic Document as referred to in Article 96 to the Minister.

(2) The relevant Ministry or Body shall coordinate with the Minister for the termination of Access to Electronic Information and/or Electronic Document as referred to in Article 96.

(3) Law enforcement officers may request for the termination of Access to Electronic Information and/or Electronic Document as referred to in Article 96 to the Minister.

(4) Justice institutions may order the termination of Access to Electronic Information and/or Electronic Document as referred to in Article 96 to the Minister.

(5) The provisions on procedures for the application for Access termination as referred to in paragraph (1) until paragraph (4) are regulated with Regulation of the Minister.

Article 98

(1) Electronic System Provider must terminate the Access to Electronic Information and/or Electronic Document as referred to in Article 96.

(2) The Electronic System Provider as referred to in paragraph (1) shall consist of internet Access service provider, network and telecommunication services provider, and link provider which provides Electronic Information and/or Electronic Document traffic network.

(3) The Electronic System Provider which fails to terminate Access may be legally liable based on laws and regulations.

(4) Further provisions on the implementation of Access termination obligation as referred to in paragraph (1) shall be regulated with Regulation of the Minister.

Article 99

(1) The Government shall determine the Agency or institution which has strategic Electronic Data which

must be protected.

(2) The Agency or institution which has strategic Electronic Data which must be protected as referred to in paragraph (1), shall consist of:

a. government administration sector;

b. energy and mineral resources sector;

c. transportation sector;

d. financial sector;

e. health sector;

f. information technology and communication sector;

g. food sector;

h. defense sector; and

i. other sectors which are determined by the President.

(3) Agency or institution which has strategic Electronic Data as referred to in paragraph (1) shall formulate an Electronic Document and its electronic backup as well as connect it to a certain data center for the purpose of data security.

(4) Further provisions on the obligation to formulate the Electronic Document and its electronic backup as well as connect it to the certain data center as referred to in paragraph (3) shall be regulated in regulation of the head of agency who is in charge of cybersecurity.

CHAPTER IX

ADMINISTRATIVE SANCTIONS

Article 100

(1) Violation upon the provisions of Article 4, Article 5 paragraph (1) and paragraph (2), Article 6 paragraph (1), Article 9 paragraph (1) and paragraph (4), Article 14 paragraph (1) and paragraph (5), Article 15 paragraph (1), Article 17 paragraph (4), Article 18 paragraph (1), Article 21 paragraph (2) and paragraph (3), Article 22 paragraph (1), Article 23, Article 24 paragraph (1), paragraph (2), and paragraph (3), Article 25, Article 26 paragraph (1), Article 28 paragraph (1), Article 29, Article 30 paragraph (1), Article 31, Article 32 paragraph (1) and paragraph (2), Article 33, Article 34 paragraph (1), Article 37 paragraph (1) and paragraph (2), Article 38 paragraph (3), Article 39 paragraph (2), Article 40 paragraph (1) and paragraph (2), Article 42 paragraph (1) and paragraph (3), Article 51 paragraph (1), Article 53 paragraph (3), Article 55 paragraph (2), Article 63 paragraph (3), Article 64 paragraph (1), Article 69 paragraph (1), Article 82 paragraph (7), Article 84 paragraph (1) and paragraph (2), Article 87 paragraph (2), and Article 98 paragraph (1), shall be imposed on administrative sanctions.

(2) Administrative sanctions as referred to in paragraph (1) may be in the form of:

a. Written reprimand;

b. administrative fine;

c. temporary suspension;

d. Access termination; and/or

e. removal from the list.

(3) The administrative sanction shall be imposed by the Minister in accordance with laws and regulations.

(4) The imposition of administrative sanctions as referred to in paragraph (2) letter c and letter d is

conducted through coordination with the head of the relevant Ministry or Body.

(5) The imposition of administrative sanctions as referred to in paragraph (2) and paragraph (3) does not eliminate the criminal and civil responsibilities.

Article 101

Further provisions on procedures for the imposition of administrative sanctions and objection for the imposition of administrative sanctions shall be regulated in Regulation of the Minister.

CHAPTER X

TRANSITIONAL PROVISIONS

Article 102

(1) Upon the effective enforcement of this Regulation of the Government, the Electronic System Provider which has operated before the promulgation of this Regulation of the Government, must adjust with the provisions of Article 6 paragraph (1) within 1 (one) year period.

(2) Upon the effective enforcement of this Regulation of the Government, the Electronic System Provider in the Public Sector which has operated before the promulgation of this Regulation of the Government, must adjust with the provision of Article 20 paragraph (2) within 2 (two) years period.

CHAPTER XI

CLOSING PROVISIONS

Article 103

(1) Upon the effective enforcement of this Regulation of the Government, implementing regulations of Regulation of the Government Number 82 of 2012 on the Organization of Electronic System and Transaction shall be declared to remain valid insofar that it does not contravene or have not been replaced with the new ones based on this Regulation of the Government.

(2) Upon the effective enforcement of this Regulation of this Government, Regulation of the Government Number 82 of 2012 on the Organization of Electronic System and Transaction (State Gazette of the Republic of Indonesia of 2012 Number 189, Supplement to the State Gazette of the Republic of Indonesia Number 5348) is revoked and is declared invalid.

Article 104

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

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

Established in Jakarta,

On 4 October 2019

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Signed.

JOKO WIDODO

Promulgated in Jakarta,

On 10 October 2019

THE CARETAKER OF THE MINISTER OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,

Signed.

TJAHJO KUMOLO

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2019 NUMBER 185

ELUCIDATION OF

REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

NUMBER 71 OF 2019

ON

THE ORGANIZATION OF ELECTRONIC SYSTEM AND TRANSACTION

I. GENERAL

Several provisions in Law Number 11 of 2008 on Electronic Information and Transaction mandate further regulation in Regulation of the Government, namely regulation on Reliability Certification Body, Digital Signature, Electronic Certification Provider, Electronic System Provider, Electronic Transaction Provider, Electronic Agent provider, and management of Domain Name which have been regulated in Regulation of the Government Number 82 of 2012 on the Organization of Electronic System and Transaction. However, Regulation of Government Number 82 of 2012 on the Organization of Electronic System and Transaction need to be adjusted with technology development and public needs.

The establishment of this Regulation of the Government is also intended to further regulate several provisions in Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction which is established to ensure the acknowledgement as well as to respect the rights and freedoms of others and to meet fair demands in accordance with the considerations of security and public order in a democratic society. Several provisions which require further regulation, namely:

a. the obligation for any Electronic System Provider to delete irrelevant Electronic Information and/or Electronic Document which is under their control on the request of the relevant Person based on a court decision; and

b. Government role in facilitating the utilization of Information Technology and Electronic Transaction, protecting public interest from any kind of disturbance as a result of misuse of Electronic Information and Electronic Transaction which disturb public order, and preventing the dissemination and utilization of Electronic Information and/or Electronic Document which contains prohibited content in accordance with laws and regulations.

The material contents of this Regulation of the Government consist of:

a. category of the Electronic System Provider;

b. the obligations of the Electronic System Provider;

c. Access deletion and/or blocking upon irrelevant Electronic Information and/or Electronic Document;

d. placement of Electronic System and Electronic Data;

e. supervision of the Electronic System organization;

f. organization of Electronic Agent;

g. organization of Electronic Transaction;

h. organization of Electronic Certification;

i. management of Domain Name;

j. Government role in the organization of Electronic System and Transaction; and

k. administrative sanctions.

II. ARTICLE BY ARTICLE

Article 1

Self-explanatory.

Article 2

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

Self-explanatory.

Letter b

“institution which is appointed by the Agency” is referred to the institution which implements the organization of Electronic System within the public sector on behalf of the appointing Agency.

Paragraph (4)

“regulatory and supervisory authority in the financial sector” is among others authority in the sectors of the monetary, payment system, macro prudential, banking, capital market, as well as insurance, pension fund, financing institution, and other financial services institutions.

Paragraph (5)

Letter a

Self-explanatory.

Letter b

“Electronic System Provider which has an internet-based portal, website, or application” is referred to the Electronic System Provider which Electronic System is utilized in Indonesian territory, and/or is offered in Indonesian territory.

Number 1

Self-explanatory.

Number 2

Self-explanatory.

Number 3

Self-explanatory.

Number 4

Self-explanatory.

Number 5

Self-explanatory.

Number 6

Personal Data processing shall consist of acquisition and collection, processing and analyzing, improvement and update, display, announcement, transfer, dissemination, or disclosure, and/or deletion or destruction of Personal Data.

Article 3

Paragraph (1)

"reliable" is referred to the Electronic System which has a capability in accordance with the users' needs.

"safe" is referred to Electronic System which is protected physically and non-physically.

"proper operation of Electronic System" is referred to Electronic System which has a capability in accordance with its specification.

Paragraph (2)

"responsible" is referred to the Electronic System Provider which is legally responsible for the organization of such Electronic System.

Paragraph (3)

Self-explanatory.

Article 4

Self-explanatory.

Article 5

Self-explanatory.

Article 6

Self-explanatory.

Article 7

Paragraph (1)

Letter a

"interconnectivity" is referred to the ability to be connected to each other, so that it may function properly. Interconnectivity shall consist of the interoperability ability.

"compatibility" is referred to the suitability of an Electronic System with the other Electronic System.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (2)

Certification proof may be acquired through an accredited third party in Indonesia or other proof as supporting evidence which states the fulfillment of the requirements from certification body outside of Indonesia.

Article 8

Letter a

"be guaranteed the security and reliability of proper operation" are referred to the Electronic System Provider shall guarantee that software does not contain any other instructions other than it should or illegal hidden instructions (malicious code), such as, time bomb instructions, virus program, trojan, worm, and backdoor. This security may be conducted by examining the source code.

Letter b

Self-explanatory.

Article 9

Paragraph (1)

"source code" is referred to a series of orders, statements, and/or declaration which is written in computer programming language which may be read and understood by people.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"trusted third party which retains the source code (source code escrow)" is a profession or an independent party which is competent to organize retention services for computer program or Software to be able to be accessed, acquired, or transferred the source code by the provider to the users' party.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 10

Paragraph (1)

"experts" are referred to manpower who has the knowledge and special skills in the Electronic System sector which may be accounted academically or practically.

Paragraph (2)

Self-explanatory.

Article 11

Paragraph (1)

Letter a

"service level agreement" is a statement on service quality level of an Electronic System.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (2)

Self-explanatory.

Article 12

“apply risk management” is conducting risk analysis and formulating mitigation measures and countermeasures to overcome the threat, disturbance and obstacles to the Electronic System which it manages.

Article 13

“governance policy” is namely, including on the activity to develop organization structure, business process, and performance management, as well as providing supporting personnel for Electronic System operation to ensure the Electronic System may operate properly.

Article 14

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

“valid approval” is an approval which is delivered explicitly, must not be hidden or on the basis of oversight, negligence, or coercion.

Paragraph (4)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Vital interest is referred to the needs/necessity to protect very important matters about a person’s location.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 15

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

The obligation to delist from search engines (right to delisting) shall include the Electronic System Provider which operates a search engine to remove the appearance and/or block the Access to the irrelevant Electronic Information and/or Electronic Documents based on a court decision.

Paragraph (3)

Self-explanatory.

Article 16

Self-explanatory.

Article 17

Self-explanatory.

Article 18

Self-explanatory.

Article 19

Paragraph (1)

IT Governance shall include the process of planning, implementation, operation, and documentation.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 20

Paragraph (1)

“business continuity plan” is referred to a series of processes which is conducted to ensure the continuity of activities in disturbance or disaster conditions.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Paragraph (7)

Self-explanatory.

Article 21

Self-explanatory.

Article 22

Paragraph (1)

Audit trail mechanism shall consist of:

a. maintain the transaction log in accordance with the provider data retention policy, in accordance with laws and regulations;

b. give notification to the consumer if a transaction has been conducted;

c. ensure the availability of audit trail function to be able to detect an effort and/or incursion which must be reviewed or evaluated periodically; and

d. in the event that the processing and audit trail are the responsibilities of the third party, then such audit trail process shall be in accordance with the standard which has been determined by the Electronic System Provider.

Paragraph (2)

“other examinations” are namely examination for the purpose of mitigation or incident response.

Article 23

Electronic System Component shall consist of:

a. Software;

b. Hardware;

c. experts;

d. Electronic System security system; and

e. Electronic System governance.

Article 24

Paragraph (1)

“disturbance” is referred to any action which is destructive or has a serious impact on the Electronic

System, so that the Electronic System does not work properly.

“failure” is referred to the cessation of part or all of the Electronic System functions which are essential so that the Electronic System does not function properly.

“loss” is referred to the impact of damage to the Electronic System which has legal consequences for users, providers, and other third parties both material and immaterial.

Paragraph (2)

"prevention and control system" shall include antivirus, anti-spamming, firewall, intrusion detection, prevention system, and/or management of information security management system.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 25

Self-explanatory.

Article 26

Paragraph (1)

Self-explanatory.

Paragraph (2)

“transferable Electronic Information and/or Electronic Document” is referred to securities or valuable letters in electronic form.

“electronic Information and/or Electronic Document shall be unique” is referred to Electronic Information and/or Electronic Document and/or recordation of the Electronic Information and/or Electronic Document is the only one which represents a certain value.

“electronic Information and/or Electronic Document shall explain possession” is referred to the possession nature which is represented with a control system or recordation system of the relevant Electronic Information and/or Electronic Document.

“electronic Information and/or Electronic Document shall explain its ownership” is that the Electronic Information and/or Electronic Document shall explain the ownership nature which is represented by the existence of technology control which guarantees that there is only one single authoritative copy and permanent.

Article 27

"interoperability" is referred to the ability of different Electronic Systems to be able to work in an integrated manner.

"compatibility" is referred to the compatibility of one Electronic System with another Electronic System.

Article 28

Paragraph (1)

Self-explanatory.

Paragraph (2)

Education which may be delivered to the Electronic System User namely:

a. explain to the Electronic System User the importance to maintain the security of Personal Identification Number (PIN)/password) namely:
    1. keep PIN/password in secret and do not tell it to anyone including the provider officers;
    2. change the PIN/password periodically;
    3. use PIN/password which is difficult to be guessed, such as the use of personal identity in the form of birthdate;
    4. do not record PIN/password; and
    5. PIN/password for one product should be different from the PIN/password of other products.
b. explain to the Electronic System User on various modes of Electronic Transaction crime; and
c. explain to the Electronic System User on procedures to submit a claim.

Article 29

The obligation to submit information to Electronic System Users is intended to protect the interests of Electronic System Users.

Article 30

Paragraph (1)

The provision of features is intended to protect the rights or interests of the Electronic System Users.

Paragraph (2)

Self-explanatory.

Article 31

Self-explanatory.

Article 32

Self-explanatory.

Article 33

Self-explanatory.

Article 34

Self-explanatory.

Article 35

Self-explanatory.

Article 36

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

"visual form" is referred to a display which can be seen or read, including a graphical display of a website.

Letter b

"audio form" is referred to anything which can be heard, including telemarketing services.

Letter c

“data Electronic form” such as electronic data capture (EDC), radio frequency identification (RFI), and barcode recognition. Electronic data capture (EDC) is an Electronic Agent for and behalf of the Electronic System Provider which cooperates with a network provider. EDC may be used independently by bank financial institutions and/or jointly by financial institutions and other non-financial institutions.

In the event that the Electronic Transaction is conducted by using Bank X card on EDC which belongs to Bank Y, then Bank Y will forward such transaction to Bank X, through the network provider.

Letter d

Self-explanatory.

Article 37

Paragraph (1)

Letter a

Information on the identity of the Electronic Agent provider shall at least contain a logo or name indicating the identity.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Letter h

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 38

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

"equal treatment" shall include the application of the same tariffs, facilities, requirements and procedures.

Paragraph (4)

Self-explanatory.

Article 39

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

“confidentiality" shall be in accordance with the legal concept of confidentiality of information and communication electronically.

Letter b

“integrity" shall be in accordance with the legal concept of integrity of Electronic Information.

Letter c

"availability" shall be in accordance with the legal concept of the availability of Electronic Information.

Letter d

"authenticity" shall be in accordance with the legal concept of authenticity (authentication) which includes the originality of the contents of Electronic Information.

Letter e

"authorization" shall be in accordance with the legal concept of authorization based on the scope of duties and functions of an organization and management.

Letter f

“Non-repudiation" shall be in accordance with the legal concept of non-repudiation.

Article 40

Paragraph (1)

Letter a

In testing the authenticity of identity and examining the authorization of Electronic System User, it is necessary to take the following matters into consideration:

1. written policy and procedures to ensure the ability to test the authentication of identity and examining the authorization of Electronic System User;
2. method for authenticity test; and
3. combination of at least 2 (two) factor authentication namely “what you know” (PIN/password), “what you have (magnetic card with a chip, token, digital signature), “what you are” or “biometric” (retina and fingerprint).

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Protection of the confidentiality of Personal Data Users of Electronic Systems shall also be fulfilled in the event that the provider uses the services of other parties (outsourcing).

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Procedures for handling unforeseen events shall also be fulfilled in the event that the provider uses the services of another party (outsourcing).

Paragraph (2)

In formulating and determining procedures to ensure the Electronic Transaction, so that it is unable to be repudiated by consumers, it shall consider:

a. Electronic Transaction system was designed to reduce the unintended transactions by the authorized user;
b. the entire identity of the party who conducts the transaction has been tested its authenticity or validity; and
c. financial transaction data is protected from possible changes and any changes which be detected.

Article 41

Self-explanatory.

Article 42

Self-explanatory.

Article 43

Self-explanatory.

Article 44

Paragraph (1)

This provision is intended to protect Electronic System Users from sending disturbing Electronic Information (spam).

Common forms of spam are e-mail spam, instant message spam, Usenet newsgroup spam, Web search-engine spam, blog spam, news spam on mobile phones, and Internet forum spam.

Paragraph (2)

Self-explanatory.

Article 45

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

"reasonable" is referred to the element of propriety which applies in accordance with the developing habits or business practices that develop.

Article 46

Paragraph (1)

Electronic Transactions can include several forms or variants, including:

a. the agreement is not conducted electronically, but the contractual relationship is completed electronically;

b. the agreement is conducted electronically, and the contractual relationship is completed electronically; and

c. the agreement is conducted electronically, and the contractual relationship is not settled electronically.

Paragraph (2)

Self-explanatory.

Article 47

Paragraph (1)

Self-explanatory.

Paragraph (2)

“laws and regulations” is referred to among others Law on Consumer Protection.

Paragraph (3)

Self-explanatory.

Article 48

Paragraph (1)

“complete and correct information" shall include:

a. the information which contains the identity and status of legal subjects and their competencies, both as producers, suppliers, organizers, and intermediaries;

b. Other information which explains certain things which become a legal condition of the agreement and explains the offered goods and/or services, such as the name, address, and description of the goods/services.

"contract" shall include agreement or cooperation.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 49

Paragraph (1)

Self-explanatory.

Paragraph (2)

Electronic Transaction occurs when an agreement between the parties which may take the form of checking data, identity, Personal Identification Number (PIN) or a password.

Paragraph (3)

Letter a

"retrieval action which states an approval" is among others by clicking agreement electronically by Electronic System User.

Letter b

Self-explanatory.

Article 50

Paragraph (1)

Self-explanatory.

Paragraph (2)

"equal manner" is referred to considering the interest of both parties fairly.

Article 51

Paragraph (1)

The obligation by using Electronic Certificate shall apply upon the SSL Encryption.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Ownership of an Electronic Certificate Ownership is an effort to improve the security of Electronic System organization in addition to other security measures.

The ownership of an Electronic Certificate serves to support the security of the organization of the Electronic System which includes, among others, confidentiality, authenticity, integrity, and non-repudiation.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Regulation of the Minister shall consist among others the regulation on procedures for the submission of electronic certification application which is submitted through Electronic Certification Provider or registration authority which is appointed by the Electronic Certification Provider.

Article 52

Letter a

"examination" is referred to an examination of the physical presence of the prospective certificate holder, which may be conducted electronically online if the inspection uses biometrics.

Letter b

Digital Signature is approval on Electronic Information and/or Electronic Document which is conducted by an individual or an individual who represents a Business Entity or an Agency.

Article 53

Paragraph (1)

Letter a

“Indonesian Electronic Certification Provider” is referred to the Electronic Certification Provider which obtains certification, so that supervision may be conducted on its implementation and to be a differentiator that the Indonesian Electronic Certification Provider may be a trusted third party which guarantees the authenticity of electronic identity.

Letter b

Self-explanatory.

Paragraph (2)

“one parent principle" is referred to as the Indonesian Electronic Certification Provider shall stance to the parent Electronic Certification Operator which is organized by the Minister and the certificate is signed by using the certificate of the parent Electronic Certification Provider.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

"registered" does not mean registering as an Indonesian Business Entity but registering its company as a foreign Electronic Certification Provider to the Minister.

Paragraph (6)

Self-explanatory.

Article 54

Self-explanatory.

Article 55

Self-explanatory.

Article 56

Self-explanatory.

Article 57

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

An electronic seal is a Digital Signature which is used by a Business Entity or Agency to guarantee the originality and integrity of Electronic Information and/or Electronic Document.

Letter b

Electronic timer is a binding marker between time and date with Electronic Information and/or Electronic Documents by using reliable methods.

Letter c

Registered electronic delivery service is a service which provides delivery of Electronic Information and/or Electronic Documents and provides evidence in relation to the delivery of Electronic Information and/or Electronic Documents and protects Electronic Information and/or Electronic Documents which is sent from the risk of loss, theft, damage or unauthorized alteration.

Letter d

Website Authentication is a service which identifies the website owner and links the website to the Person or Business Entity which receives the Electronic Certificate of the website by using a reliable method.

Letter e

Preservation of Digital Signature and/or electronic seal is a service which guarantees the legal force of Digital Signature and electronic seal in an Electronic Information and/or Electronic Document still able to be validated even though the Electronic Certificate validity period has expired.

Article 58

Paragraph (1)

If the Indonesian Electronic Certification Provider cooperates with another Electronic System Provider in the organization of part of its infrastructure or services, therefore the remaining loss or negligence shall remain the responsibility of the Indonesian Electronic Certification Service Provider.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 59

Self-explanatory.

Article 60

Paragraph (1)

Digital Signatures shall function as the manual signature in terms of representing the identity of a Signer.

In authenticating, the manual signature may be conducted through verification or examination of the Digital Signature specimen from the Signer.

In Digital Signature, the Digital Signature Producing Data acts as a specimen of Digital Signature from the Signer.

Digital Signature shall be able to be used by competent experts to conduct examination and verification that Electronic Information which is signed with the Digital Signature does not change after being signed.

Paragraph (2)

The legal implications of the use of certified or non-certified Digital Signatures shall affect the strength of the evidentiary value.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 61

Paragraph (1)

"unique" is referred to that any code which is used or functioned as the Digital Signature Producing Data shall only refer to one legal subject or an entity which represents one identity.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Letter a

The Digital Signature Producing Data which is generated with cryptographic techniques generally have a probability-based mathematical correlation with Digital Signature verification data. Therefore the selection of the cryptographic code which will be used shall consider the adequacy of the level of difficulty which is encountered and the resources which shall be prepared by the party who tries to forge the Digital Signature Producing Data.

Letter b

"electronic media" are facilities, means, or device which is used to collect, store, process, and/or disseminate Electronic Information which is used temporarily or permanently.

Letter c

"data related to the Signer" is referred to all data which may be used to identify the identity of the Signer such as name, address, place and date of birth, as well as the specimen signature code, manual.

"Trusted system" is referred to a system which follows procedures for the utilization of Digital Signatures which ensure the authenticity and integrity of Electronic Information. This can be seen by considering several factors, including:

1. finance and resources;
2. the quality of Hardware and Software Device;
3. certificate and application procedures and data retention;
4. availability of the Digital Signature Producing Data; and
5. audit by an independent institution.

Letter d

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 62

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Examples of these provisions are as follows:

a. Changes to the Digital Signature after the time of signing shall result in the Electronic Information being attached to it does not function properly, damaged, or unable to be displayed if the Digital Signature is attached and/or related to the signed Electronic Information. The technique of attaching and linking an Digital Signature to signed Electronic Information may lead to the occurrence of new Electronic Information or Electronic Documents which:

   1. seen as an inseparable whole; or
   2. appear separate and signed Electronic Information may be read by laypeople while Digital Signatures in the form of codes and/or images.

b. Changes to Digital Signatures after the time of Signing shall result in some or all Electronic Information being invalid if the Digital Signature is logically associated with the signed Electronic Information.

   Changes which occur to the signed Electronic Information shall cause a discrepancy between the Digital Signature and the relevant Electronic Information which may be clearly seen through verification mechanisms.

Article 63

Self-explanatory.

Article 64

Paragraph (1)

Self-explanatory.

Paragraph (2)

Authentication factors which may be chosen to be combined may be divided into 3 (three) types, namely:

a. something which is owned individually (what you have) such as an ATM card or smart card;

b. something which is known individually (what you know) for example PIN/password or

cryptographic key; and

c. something which is characteristic of an individual (what you are), for example, voice patterns, handwriting dynamics, or fingerprints.

Paragraph (3)

Self-explanatory.

Article 65

Self-explanatory.

Article 66

Self-explanatory.

Article 67

Self-explanatory.

Article 68

Self-explanatory.

Article 69

Self-explanatory.

Article 70

Self-explanatory.

Article 71

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Self-explanatory.

Letter b

"address" shall at least explain the city of residence of the person or Business Entity operating.

Letter c

Self-explanatory.

Letter d

Self-explanatory.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 72

Self-explanatory.

Article 73

Paragraph (1)

Self-explanatory.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Letter a

Information Technology Consultants shall include the information security professions.

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Paragraph (5)

Self-explanatory.

Paragraph (6)

Self-explanatory.

Article 74

Self-explanatory.

Article 75

Self-explanatory.

Article 76

Paragraph (1)

Letter a

Identity registration is a Reliability Certificate, which its reliability guarantee is limited to the identity of the Businesses is correct.

Validation which is conducted by the Reliability Certification Body shall only apply to the identity of Businesses which shall at least contain the name of the legal subject, legal subject status, address or domicile, telephone number, e-mail address, business permit, and Taxpayer Identification Number (NPWP) if it is not already registered in the Electronically Integrated Business Licensing/Online Single Submission.

The Reliability Certification Agency which issues this Reliability Certificate shall provide search certainty that the identity of the businesses is correct.

Letter b

Electronic System Security is a Reliability Certificate which guarantees its reliability providing certainty that the process of delivering or exchanging data through the Perpetrator website.

The business is protected by using security technology for data exchange processes such as SSL/secure socket layer protocol.

This Reliability Certificate guarantees that there is a security system in the process of data exchange which has been proven.

Security against vulnerability (vulnerability seal) is a Reliability Certificate whose guarantee of reliability is to provide certainty that there is an information security management system which is implemented by the Businesses by referring to certain Electronic System security standards based on laws and regulations.

Letter c

The privacy policy is a Reliability Certificate which its reliability guarantee is providing certainty that Personal Data of the consumer is protected its confidentiality properly.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Article 77

Self-explanatory.

Article 78

Self-explanatory.

Article 79

Paragraph (1)

Self-explanatory.

Paragraph (2)

Letter a

“high-level generic Domain Name” is high-level Domain Name which shall consist of three characters or more in the hierarchy of domain naming system other than country code Top Level Domain. For example ".nusantara" or ".java".

Letter b

“high-level Indonesian Domain Name” is the high-level domain in the hierarchy of domain naming system which indicates Indonesia code (.id) in accordance with the list of country code in ISO 3166-1 which is used and acknowledged by the Internet Assigned Numbers Authority (IANA).

Letter c

Example of second-level Indonesian Domain Name is co.id, go.id, ac.id, or.id, or mil.id.

Letter d

Example of derivative-level Indonesian Domain Name is kominfo.go.id

Paragraph (3)

Letter a

Included in the scope of the understanding of the Domain Name Registry is the function and role of the ccTLD manager.

Letter b

Self-explanatory.

Article 80

Self-explanatory.

Article 81

Self-explanatory.

Article 82

Self-explanatory.

Article 83

Self-explanatory.

Article 84

Self-explanatory.

Article 85

Self-explanatory.

Article 86

Self-explanatory.

Article 87

Self-explanatory.

Article 88

Self-explanatory.

Article 89

Self-explanatory.

Article 90

Self-explanatory.

Article 91

Self-explanatory.

Article 92

Letter a

"The national Electronic System gateway" shall include the Indonesian National Single Window (INSW) and electronically integrated business licensing services (online single submission).

Letter b

Self-explanatory.

Letter c

Self-explanatory.

Letter d

The implementation of an integrated data center and national disaster recovery center is aimed for general applications and strategic Electronic Data.

Letter e

Self-explanatory.

Letter f

Self-explanatory.

Letter g

Self-explanatory.

Article 93

Self-explanatory.

Article 94

Self-explanatory.

Article 95

Self-explanatory.

Article 96

Letter a

"violating laws and regulations" shall include Electronic Information and/or Electronic Document which contain elements of pornography, gambling, slander and/or defamation, fraud, hatred of ethnicity, religion, race, and intergroup (SARA) , violence and/or child abuse, violations of intellectual property, violations of trade in goods and services through electronic systems, terrorism and/or radicalism, separatism and/or prohibited dangerous organizations, violations of information security, violations of consumer protection, violations in health, violations of supervision medicine and food.

Letter b

"disturbing the public and disturbing public order" shall include information and/or falsified facts.

Letter c

Self-explanatory.

Article 97

Self-explanatory.

Article 98

Paragraph (1)

"termination of Access" shall include blocking Access, closing an account, and/or removing content.

Paragraph (2)

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Article 99

Paragraph (1)

"Agency or institution which has strategic Electronic Data" is referred to agency or institution which has vital information infrastructure in the determined sector.

Paragraph (2)

Self-explanatory.

Paragraph (3)

The connection to certain data centers for data security shall be implemented in the context of incidents which must be reported to the body whose duties and responsibilities are concerned with the cybersecurity sector.

Paragraph (4)

Self-explanatory.

Article 100

Paragraph (1)

The imposition of sanctions in this provision is only intended for parties who conduct administrative violations, whereas those concerning moral or civil violations are not subject to administrative sanctions.

Paragraph (2)

Letter a

Self-explanatory.

Letter b

Self-explanatory.

Letter c

"temporary termination" is referred to a termination of some or all components or services in the relevant Electronic System for a certain period of time.

Letter d

"termination of Access" shall include blocking Access, closing an account, and/or removing content.

Letter e

Self-explanatory.

Paragraph (3)

Self-explanatory.

Paragraph (4)

Self-explanatory.

Paragraph (5)

Self-explanatory.

Article 101

Self-explanatory.

Article 102

Self-explanatory.

Article 103

Self-explanatory.

Article 104

Self-explanatory.

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 6400