http://rulebook-jica.ekon.go.id/english/4902_PP_82_2012_e.html

REGULATION OF THE GOVERNMENT OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012

CONCERNING
ELECTRONIC SYSTEM AND TRANSACTION OPERATION

BY THE GRACE OF ALMIGHTY GOD
PRESIDENT OF THE REPUBLIC OF INDONESIA,

Elucidation

Considering:

that to implement provisions of Article 10 paragraph (2), Article 11 paragraph (2), Article 13 paragraph (6), Article 16 paragraph (2), Article 17 paragraph (3), Article 22 paragraph (2) and Article 24 paragraph (4) of Law Number 11 of 2008 concerning Electronic Information and Transaction, it is necessary to stipulate Government Regulation concerning Electronic System and Transaction Operation;

In view of:

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

2. Law Number 11 of 2008 concerning Electronic Information and Transaction (Statute Book of the Republic of Indonesia Number 58 of 2008, Supplement to Statute Book of the Republic of Indonesia Number 4843);

DECIDES:

To stipulate:

GOVERNMENT REGULATION CONCERNING ELECTRONIC SYSTEM AND TRANSACTION OPERATION.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Government Regulation what is referred as:

1. Electronic System is a series of devices and electronic procedures that serve to prepare, collect, process, analyze, store, display, publish, transmit, and/or distribute Electronic Information.

2. Electronic Transaction is a legal act that is conducted by the use of Computers, Computer networks, and/or other electronic media.

3. Electronic Agent is device of an Electronic System made to perform an action on a certain Electronic Information automatically that is organized by Person.

4. Electronic System Operator is any Person, state agency, Business Entity, and community that provide, manage, and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party's interest.

5. Sector Supervisory and Regulatory Agency is the agency that in charge for supervision of the implementation of sector task and issued a regulation to the sector such as the banking and transportation sectors.

6. Electronic information is one or a set of electronic data, including but not limited to text, sound, images, maps, plans, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, marks, numbers, access codes, symbols, or perforations treated with sense or be understood by people who are able to understand them.

7. Electronic Document is any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, Access Codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them..

8. Information Technology is a technique to collect, prepare, store, process, publish, analyze, and/or disseminate information.

9. Electronic System User is any Person, state administrators, Business Entities, and the community who use the goods, services, facilities, or the information provided by the Electronic Systems Operator.

10. Hardware is one or a series of tools that are linked in Electronic Systems.

11. Software is one or a set of computer programs, procedures, and/or documentation related with the operation of Electronic Systems.

12. Electronic System Capability Certification is a series of checking and testing process performed by an authorized and competent agency to ensure an Electronic System working properly.

13. Access is the activities to make interaction with the stand-alone or network Electronic Systems.

14. Electronic Transactions operation is a series of Electronic Transaction activities conducted by the Sender and Receiver by using the Electronic System.

15. Electronic Contract is an agreement of the parties created through the Electronic System.

16. Sender is the law subject that transmits Electronic Information and/or Electronic Document.

17. Receiver is law subject receiving Electronic Information and/or Electronic Document from Sender.

18. Electronic Certificate is a certificate which has electronic characteristics that contains Electronics Signatures and identities that shows the status of the law subject of the parties in Electronic Transaction issued by the electronic certification operator.

19. Electronic Signature is a signature that consists of Electronic Information attached to, associated, or linked with other Electronic Information that is used as a means of verification and authentication.

20. Signer is law subject that is associated or related with Electronic Signature.

21. Electronic Signature Operator is a legal entity that serves as a trusted party that facilitates the making of Electronic Signatures.

22. Supporting of Electronic Signature Services is a legal entity that serves as the supporting party for the implementation to use Electronic Signatures.

23. Electronic Signature Making Data is a personal code, biometrics code, cryptographic code, and/or the code generated from the conversion of a manual signature become Electronic Signature, including another code generated from the development of Information Technology.

24. Reliability Certification Agency is an independent agency established by a recognized, authorized, and supervised professional by the Government with the authority to audit and issue a Reliability Certificate in Electronic Transactions.

25. Reliability Certificate is a document states Business Entity whose operate Electronic Transactions already pass audit or test of the suitability from Reliability Certification Agency.

26. Business Entity is any individual or legal entity, whether in the form of legal entity or not, established and domiciled or conducting activities within the jurisdiction of the Republic of Indonesia, individually and collectively, through the agreement for the implementation of business activities in various fields of economics.

27. Personal Data is specific individual data are stored, treated, and keep on the truth and confidentiality is protected.

28. Domain Name is the internet address of state administrator, Person, Business Entity, and/or community, which can be used to communicate through the internet, in the form of code or arrangement of characters that is unique to indicate a specific location in the Internet.

29. Domain Name Registry is operator that has responsible for managing, operating, and maintenance of the Domain Name Electronic System Operation.

30. Domain Name Registrar is Person, Legal Entity, or a society that provides Domain Name registration services.

31. Domain Name User is Person, State Administrator Agency, Business Entity, or community who apply for registration to use the Domain Name to the Domain Name Registrar.

32. State Administrator Agency hereinafter called as Agency is legislative, executive, and judicial institution in center or regional level and other institution established by regulation.

33. Person is an individual, both Indonesian citizens, foreign citizens, or legal entity.

34. Business Entity is a individual company or partnership firm, whether in the form of legal entity or non legal entity.

35. Minister is the minister who held government affairs in the field of communication and informatics.

Article 2

This Government Regulation governing on the:

- a. Electronic System Operation;
- b. Electronic Agent operator;
- c. Electronic Transactions operation;
- d. Electronic Signature;
- e. electronic certification operation;
- f. Reliability Certification Agency; and
- g. Domain Name management.

CHAPTER II
ELECTRONIC SYSTEM OPERATION

Part One
General

Article 3

(1) The Electronic System Operation is implemented by Electronic Systems Operator.

(2) The Electronic System Operation as intended in paragraph (1) may be done to:

- a. public services; and
- b. non public services.

(3) The criteria of public service as intended in paragraph (2) a are referring to the provisions of regulation.

Article 4

Electronic System Operator as intended in Article 3 paragraph (1) include the regulation on the:

- a. registration;
- b. Hardware;
- c. Software;
- d. expert;
- e. management;
- f. security;
- g. Electronic System Capability Certification; and
- h. supervision.

Part Two
Registration

Article 5

(1) The Electronic System Operator for public services shall conduct registration.

(2) Electronic Systems Operator for non public services may conduct registration

(3) Obligation for the registration of Electronic System Operator for the public services as intended in paragraph (1) performed before starting Electronic Systems for public.

(4) The registration as intended in paragraphs (1) and (2) shall be submitted to the Minister.

(5) Further provisions on the procedure for registration as intended in paragraph (1) and paragraph (2) are governed by Ministerial Regulation.

Part Three
Hardware

Article 6

(1) Hardware is used by Electronic System Operator shall:

- a. fulfill the interconnectivity and compatibility aspects with the system used;
- b. obtain capability certificate from the Minister;
- c. have technical support, maintenance, and after sales services from the seller or provider;
- d. have supporting references from other users that Hardware is functioning according to specifications;
- e. have guaranteed availability of spare parts for at least 3 (three) years;
- f. have a guarantee of clarity on the new conditions; and
- g. have a guarantee of free from defect products.

(2) Electronic System Operator shall ensure technology neutrality and freedom of choice in the use of Hardware.

(3) The Minister shall determine the Hardware technical standards used by the Electronic System Operator.

(4) Further provisions on the Hardware technical standards as intended in paragraph (3) are governed by Ministerial Regulation.

Part Four
Software

Article 7

(1) Software used by Electronic System Operator for the public service shall:

- a. registered in the ministry that conduct of governmental affairs in the field of communication and informatics;
- b. guaranteed the safety and reliability of operation as appropriate; and
- c. in accordance with the provisions of the regulation.

(2) Further provisions on the requirements of the Software as intended in paragraph (1) are governed by Ministerial Regulation.

Article 8

(1) Providers who develop software created specifically for an Agency must submit the source code and documentation of the Software to the agency concerned.

(2) In case the delivery of the source code and documentation of the Software as intended in paragraph (1) may not be implemented, providers can submit source code and documentation of the Software to a trusted third party to store source code.

(3) Providers must ensure the acquisition and/or access to source code and documentation of the Software to a trusted third party as intended in paragraph (2).

Article 9

(1) Electronic System Operator shall ensure the confidentiality of the source code of the Software is used.

(2) The source code as intended in paragraph (1) can be inspected if necessary for investigation.

Part Five
Experts

Article 10

(1) The experts used by Electronic System Operator must have competence in the field of Electronic Systems or Information Technology.

(2) Experts as intended in paragraph (1) shall have a certificate of expertise.

Article 11

(1) The Electronic System Operation for strategic characteristics shall use Indonesian nationally experts.

(2) In case of that there is no Indonesian nationality expert, Electronic System Operator may use foreign expert.

(3) The provisions on the position of experts in the Electronic System Operation for strategic characteristics carried out in accordance with the provisions of the regulation.

(4) Further provisions on the competence of experts are governed by Ministerial Regulation.

Part Six
Electronic Systems Management

Article 12

(1) Electronic System Operator shall ensure:

- a. availability service level agreements;
- b. the availability of information security agreement of services of Information Technology are used, and
- c. information security and internal communication tools are organized.

(2) Electronic System Operator as intended in paragraph (1) shall ensure each component and integration of all operating Electronic Systems as they should.

Article 13

The Electronic System Operator shall apply risk management against damage or loss caused.

Article 14

(1) Electronic System Operator shall have a management policy, operations work procedures, and periodical audit mechanisms for Electronic Systems.

(2) Further provisions on management policy, operations work procedures, and audit mechanism as intended in paragraph (1) shall be governed by Ministerial Regulation.

Article 15

(1) Electronic System Operator shall:

- a. keep on secrecy, integrity, and availability of Personal Data are managed;
- b. ensure that the acquisition, use, and utilization of Personal Data based on approval from the owner of Personal Data, unless otherwise provided by regulations: and
- c. ensure the use or disclosure of the data based on approval from owner of such Personal Data, and in accordance with the purpose of being delivered to the owner of Personal Data on the data acquisition.

(2) If there is a failure in the protection of confidential Personal Data that are managed, Electronic System Operator shall notify in writing to the owner of those Personal Data.

(3) Further provisions on the guidelines for Personal Data protection in Electronic Systems as intended in paragraph (2) are governed by Ministerial Regulation.

Article 16

(1) The Electronic System Operator for public services is obligated to implement good management and accountability.

(2) Good management as intended in paragraph (1) at least meet the following requirements:

- a. availability of procedures or guidance in the Electronic System Operation that is documented and/or published by the language, information, or symbol that are understood by the parties related with the Electronic System Operation;
- b. sustainable mechanism to maintain new and clear of implementation guidelines procedure;
- c. there is institutional and completeness of support personnel for the operation of the Electronic Systems as appropriate;
- d. the implementation of the performance management to the operated Electronic System to ensure the Electronic Systems operating as they should; and
- e. there is plan to maintain the continuity of managed Electronic System Operation.

(3) In addition to the requirements as intended in paragraph (2), related Sector Supervisory and Regulatory Agency can determine other requirements are stipulated in regulation.

(4) Further provisions on the Electronic System management for public service are governed by Ministerial Regulation.

Article 17

(1) The Electronic System Operation for public service shall have a continuity plan of activities to solve with disruption or disaster according to the risk of impacts.

(2) Electronic System Operator for the public service is obligated to put the data center and disaster recovery center in Indonesian territory for the purpose of law enforcement, protection, and enforcement of national sovereignty to the data of its citizens.

(3) Further provisions on the obligation of placing the data center and disaster recovery center in Indonesian territory as intended in paragraph (2) shall be governed by related Sector Supervisory and Regulatory Agency in accordance with the provisions of regulation after coordination with the Minister.

Part Seven
Security of Electronic System Operation

Article 18

(1) The Electronic System Operator shall provide an audit trail record of all activities of the Electronic System Operation.

(2) Audit trail record as intended in paragraph (1) is used for purposes of monitoring, enforcement, dispute resolution, verification, testing, and other checking.

Article 19

Electronic System Operator shall secure the Electronic Systems components.

Article 20

(1) Electronic System Operator shall have and perform the procedures and structure for securing the Electronic Systems in avoiding disruption, failure, and loss.

(2) Electronic System Operator shall provide a security system that includes procedures and systems to prevent and solve the threats and attacks that cause disruption, failure, and loss.

(3) In case there is failure or disruption of system with seriously affected as a result of the actions of the other party to Electronic Systems, Electronic System Operator shall secure the data and immediately report at the first opportunity to the law enforcement officers or related Sector Supervisory and Regulatory Agency.

(4) Further provisions on the security system as intended in paragraph (2) are governed by Ministerial Regulation.

Article 21

Electronic System Operator shall redisplay Electronic Information and/or Electronic Documents completely in accordance with the format and retention period determined based on regulation.

Article 22

(1) Electronic System Operator shall maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of the Electronic Information and/or Electronic Document in accordance with the provisions of the regulation.

(2) The Electronic Systems Operation purpose for Electronic Information and/or Electronic Document that are transferable, Electronic Information and/or Electronic Document must be unique and describe the acquisition and ownership.

Article 23

The Electronic System Operator shall ensure the proper functioning of Electronic Systems as it should, by keep on the interoperability and compatibility with the previous Electronic Systems and/or the related Electronic System.

Article 24

(1) The Electronic System Operator shall conduct training to Electronic Systems to Users.

(2) Training as intended in paragraph (1) at least on the rights, obligations and responsibilities of all parties involved, and the procedures for filing a complaint.

Article 25

Electronic System Operator shall submit information to the Electronic System User for at least:

- a. Electronic System Operator identity;
- b. objects in the transaction;
- c. capability or safety of Electronic Systems;
- d. procedures to use of the device;
- e. terms of the contract;
- f. procedures to reach an agreement; and
- g. guarantee of the privacy and/or protection of Personal Data.

Article 26

(1) Electronic System Operator shall provide the features in accordance with the characteristics of the Electronic Systems are used.

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

- a. make corrections;
- b. cancel the order;
- c. give confirm or reconfirm;
- d. choose to continue or to stop carrying out the next activity;
- e. see the information are submitted in the form of contract or advertisement offers;
- f. check the status of success or failure of the transaction; and
- g. read the agreement before making a transaction.

Article 27

Electronic System Operator is obligated to protect its users and the public from harm caused by its operation of Electronic Systems.

Article 28

(1) Each person who works in the Electronic Systems Operation must secure and protect structure and infrastructures of Electronic Systems or information transmitted through the Electronic System.

(2) Electronic System Operator shall provide, teach, and train personnel in charge and responsible on the security and protection of structure and infrastructure of Electronic Systems.

Article 29

For the purposes of the criminal justice process, Electronic System Operator shall provide the information contained in Electronic Systems or information generated by the Electronic Systems on the legal request from investigators for certain crimes in accordance with the authority determined by regulation.

Part Eight
Electronic System Capability Certification

Article 30

(1) The Electronic System Operator for public services is obligate to have an Electronic Systems Capability Certificate.

(2) Electronic System Capability Certificate as intended in paragraph (1) is obtained through the process of Electronic System Capability Certification.

(3) The obligation as intended in paragraph (1) may be implemented on all components or some of the components in Electronic System in accordance with the characteristics of the protection needs and the strategic characteristic of the Electronic System Operation.

(4) Application of the provisions as intended in paragraphs (1) and (2) shall be determined by the Minister after coordination with the head of related Sector Supervisory and Regulatory Agency.

Article 31

(1) Electronic System Capability Certificate as intended in Article 30 is given by the Minister.

(2) Standard and/or technical requirements used in Electronic System Capability Certification process are determined by the Minister.

(3) Related Sector Supervisory and Regulatory Agency can determine other technical requirements in the framework of Electronic System Capability Certification in accordance with the needs of each sector.

Article 32

(1) The Minister may delegate the authority to grant the Electronic System Capability Certificate to certification agency recognized by the Minister.

(2) Granting Electronic System Capability Certificate as intended in paragraph (1) shall observe the standard and/or technical requirements specified by the Minister and related Sector Supervisory and Regulatory Agency.

(3) Further provisions on the procedure for Electronic System Capability Certification and certification agency are governed by Ministerial Regulation.

Part Nine
Supervision

Article 33

(1) The Minister has the authority to supervise the Electronic System operation.

(2) Supervision as intended in paragraph (1) includes monitoring, control, inspection, search, and security.

(3) The provisions of supervision on the Electronic Systems operation in certain sectors must be made by related Sector Supervisory and Regulatory Agency after coordination with the Minister.

CHAPTER III
ELECTRONIC AGENT OPERATOR

Part One
Electronics Agent

Article 34

(1) The Electronic System can hold its own electronic system or via the Electronic Agent Operator.

(2) Electronic Agent may in the form of:

- a. visual;
- b. audio;
- c. electronic data; and
- d. other forms.

Article 35

(1) Electronics Agent shall contain or submit information to protect the rights of users at least include information on:

- a. Electronic Agent operator identity;
- b. objects are in the transaction;
- c. eligibility or security of Electronic Agent;
- d. procedures to use the devices; and
- e. the phone number for the complaint.

(2) Electronic Agent shall contain or provide features in the framework to protect the rights of users in accordance with the characteristics of the Electronic Agent is used.

(3) Features as intended in paragraph (2) may include facilities to:

- a. make correction;
- b. cancel the order;
- c. confirm or reconfirm;
- d. choose to continue or to stop carrying out the next activity;
- e. see the information presented in the form of a contract offer or advertisement; and/or
- f. check the status of success or failure of the transaction.

Article 36

(1) Electronic Agent can be held for more than one interests of Electronic System Operator based on the agreement between the parties.

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

- a. rights and obligations;
- b. responsibility;
- c. complaint and dispute resolution mechanisms;
- d. period;
- e. costs;
- f. service coverage; and
- g. choice of law.

(3) In case of Electronic Agent is held for more than one benefits of Electronic System Operator, Electronic Agent operator must give equal treatment to the Electronic System Operator that uses the Electronic Agent.

(4) In case of Electronic Agent is held for the benefit of more than 1 (one) Electronic System Operators, Electronic Agent operator is pretended as a separate Electronic System Operator.

Part Two
Registration

Article 37

(1) The Electronic Agent operator shall make registration as Electronic Agent operator to the Minister.

(2) Electronic Agent operator Registration as intended in paragraph (1) that meets the requirements will be entered in the list of Electronic Agent operators by the Minister.

(3) Further provisions on the registration procedures and requirements as intended in paragraphs (1) and (2) are governed by Ministerial Regulation.

Part Three
Obligations

Article 38

(1) In Electronic Agent Operation, Electronic Agent operator must consider the principles of:

- a. prudence;
- b. security and integration of Information Technology system;
- c. securing control over the Electronic Transactions activities;

- d. cost effectiveness and efficiency; and
- e. customer protection accordance with the provisions of regulation.

(2) Electronic Agent operator shall have and execute standard operating procedures that meet the user's data security control principles and Electronic Transaction.

(3) The user's data security control principles and Electronic Transactions as intended in paragraph (2) including:

- a. confidentiality;
- b. integrity;
- c. availability;
- d. authenticity;
- e. authorization; and
- f. non-repudiation.

Article 39

(1) Electronic Agent operator shall:

- a. test identity authenticity and check authorization of Electronic System User who conducting Electronic Transactions;
- b. have and implement policies and procedures to take action if there is indication of data theft;
- c. ensure control over the authorization and access right to the system, database, and application of Electronic Transactions;
- d. develop and implement methods and procedures to protect and/or keep the integrity of the data, records, and related information of Electronic Transactions;
- e. have and implement standards and controls over the use and protection of the data if the service provider has access to the data;
- f. have a business continuity plan include an effective contingency plan to ensure the availability of systems and Electronic Transaction services sustainable; and
- g. have procedures for handling unexpected events that quickly and appropriately to mitigate the impact of an incident, fraud, and failure of Electronic Systems.

(2) Electronic Agent Operator shall prepare and establish procedures to ensure that the Electronic Transactions can not be repudiated by the consumer.

CHAPTER IV
IMPLEMENTATION OF ELECTRONIC TRANSACTIONS

Part One
Scope of Electronic Transactions operation

Article 40

(1) The Electronic Transactions can be made in the public or private scope.

(2) The Electronic Transactions in the public scope include:

- a. Electronic Transactions operation by agency or by another party that organizes public service as far as not excluded by the Law on Information and Electronic Transactions; and
- b. Electronic Transactions operation in other public scope are governed by regulation.

(3) The Electronic Transactions in the private scope includes Electronic Transactions:

- a. between Business Entities;
- b. between Business Entity with customer;
- c. between personals;
- d. between agencies; and
- e. between agency with Business Entity in accordance with the provisions of regulations.

(4) Electronic Transaction operation in the public or private scope as intended in paragraphs (2) and (3) by using the Electronic System for public services, is implemented in accordance with the provisions of this Government Regulation.

Part Two
Electronic Transactions Operation Requirements

Article 41

(1) The Electronic Transactions in the public or private scope by using Electronic System for the benefit of the public service shall use Reliability Certificate and/or Electronic Certificate.

(2) In case of using the Reliability Certificate, the Electronic Transactions operation in the public shall be certified by the Indonesian Reliability Certification Agency are already registered.

(3) In case of using Electronic Certificates, implementation of Electronic Transactions in the public scope must use Indonesian electronic certification service providers are already certified.

Article 42

(1) The Electronic Transactions in the private scope can use Reliability Certificate and/or Electronic Certificate.

(2) In case of using the Certificate of Reliability, the Electronic Transactions operation in the private scope can be certified by the Indonesian Reliability Certification Agencies are already registered.

(3) In case of using Electronic Certificates, implementation of Electronic Transactions in the private scope may use Indonesian electronic certification service providers are already registered.

Article 43

(1) The Electronic Transactions in the territory of the Republic of Indonesia shall:

- a. pay attention to the aspect of security, reliability, and efficiency;
- b. perform transactions data storage in domestically;
- c. utilizing national gate, if in its implementation involves more than one Electronic System Operators; and
- d. utilize domestic Electronic Systems network.

(2) In case of a national gate and Electronic Systems network as intended in paragraphs (1) c and d can not be implemented yet, the Electronic Transactions operation may use other means or facility from overseas after obtaining the approval from the related Sector Supervisory and Regulatory Agency.

(3) In compliance with paragraph (1), the parties to the Electronic Transaction must pay attention to regulation from related Sector Supervisory and Regulatory Agency.

Article 44

(1) The sender must ensure that Electronic Information is transmitted properly and not interfere.

(2) Further provisions on the Electronic Information sending are stipulated in the Ministerial Regulation.

Article 45

(1) If necessary, certain institutions may hold the Electronic Transactions that are special.

(2) The provisions of the Electronic Transactions that are special are regulated by related Sector Supervisory and Regulatory Agency.

Part Three
Electronic Transaction Requirements

Article 46

(1) Electronic Transactions undertaken by the parties give legal effect to the parties.

(2) The Electronic Transactions undertaken by the parties shall pay attention to:

- a. good faith;
- b. the prudence principle;
- c. transparency;
- d. accountability; and
- e. reasonableness.

Article 47

(1) Electronic Transactions can be done under the Contract Electronics or other contractual forms as a form of agreement made by the parties.

(2) Electronic Contract is valid if:

- a. there is an agreement of the parties;
- b. performed by a competent legal subject or authorized representative in accordance with the provisions of regulations;
- c. there are certain things; and
- d. transaction object must not conflict with the laws, morality and public order.

Article 48

(1) Electronic Contract and other contractual forms as intended in Article 47 paragraph (1) addressed to the residents of Indonesia must be made in Indonesian language.

(2) Electronic contracts are made with a standard clause should be in accordance with the provisions of the standard clause are stipulated by the regulation.

(3) Electronic Contract shall at least contain:

- a. identity data of the parties;
- b. objects and specifications;
- c. requirements of the Electronic Transactions;
- d. prices and costs;
- e. procedures in case of cancellation by the parties;
- f. provision which entitles the injured party to be able to return the goods and/or request a replacement product if there is a hidden defect; and
- g. Electronic Transaction completion legal options.

Article 49

(1) Any Business Entity offering products through the Electronic System must provide complete and accurate information relating to the contract terms, manufacturers, and products offered.

(2) Business Entity is required to provide clear information on the contract offer or advertisement.

(3) Business Entity shall give a deadline to the consumer to return the goods delivered if not in accordance with the agreement or there is a hidden defect.

(4) Business Entity is required to submit information on the goods have been shipped.

(5) Business Entity can not make burden to consumers on the obligation to pay the goods delivered without a contract basis.

Article 50

(1) Electronic Transaction occurs when the parties reach agreement.

(2) The agreement as intended in paragraph (1) occurs at the time of bidding transactions sent by the sender has been accepted and approved by the recipient.

(3) The agreement as intended in paragraph (2) can be done by:

- a. actions receipt indicating approval, or
- b. act of acceptance and/or use of the object by Electronic Systems User.

Article 51

(1) In the implementation of the Electronic Transaction, Parties shall ensure:

- a. provision of data and information are correct; and
- b. availability of facilities and services, as well as complaints settlement.

(2) In the Electronic Transactions operation, the parties shall determine the equilibrium choice of law on the implementation of Electronic Transactions.

CHAPTER V
ELECTRONIC SIGNATURE

Part One
General

Article 52

(1) Electronic Signature serves as an authentication and verification of:

- a. Signer identity; and
- b. the integrity and authenticity of Electronic Information.

(2) Electronic Signature in Electronic Transaction constitute approval Signer on Electronic Information and/or Electronic Document signed by the Electronic Signatures.

(3) In case of misuse of Electronic Signatures as intended in paragraph (2) by other parties who are not ligible, proof of abuse by the Electronic Signature is by Electronic System Operator.

Article 53

(1) Electronic Signature used in Electronic Transactions can be generated through a variety of procedures signing.

(2) Electronic Signatures as intended in paragraph (1) has valid force of law and the legal consequences if:

- a. Electronic Signature Creation Data relate only to Signer;
- b. Electronic Signature Creation Data during the signing process just to be in power Signer;
- c. any changes to the Electronic Signatures occurring after the time of the signing can be known;
- d. any changes to the Electronic Information associated with the Electronic Signature after signing time can be known;
- e. there is a certain way that is used to identify who is signer; and
- f. there is a certain way to indicate that the Signer has granted approval to the relevant Electronic Information.

(3) The provisions as intended in paragraph (2) d shall be applied if all Electronic Signatures are used to ensure the integrity of Electronic Information.

Part Two
Type of Electronic Signature

Article 54

(1) Electronic Signatures include:

- a. Electronic Signatures certified; and
- b. Electronic Signatures are not certified.

(2) Electronic Signatures certified as intended in paragraph (1) a shall meet the following requirements:

- a. made by using electronic certification service providers; and
- b. evidenced by the Electronic Certificate.

(3) Electronic Signatures are not certified as intended in paragraph (1) b made without the use of electronic certification service providers.

Part Three
Electronic Signature Creation Data

Article 55

(1) Electronic Signature Creation Data shall be uniquely refers only to Signer and can be used to identify Signer.

(2) Electronic Signature Creation Data as intended in paragraph (1) may be made by the Electronic Signatures Operator or Supporting Electronic Signature Service.

(3) Electronic Signature Creation Data as intended in paragraphs (1) and (2) shall comply with the following provisions:

- a. the whole process of making Electronic Signature Creation Data security and confidentiality guaranteed by the Electronic Signatures Operator or the Electronic Signatures Supporting Services;

- b. if using cryptographic codes, Electronic Signature Creation Data must not be easily seen from the Electronic Signature verification data through a specific calculation, within a certain time, and with a reasonable;
- c. Electronic Signature Creation Data stored in an electronic medium that is in the possession of Signer; and
- d. data related to the Signer mandatory or stored in a data storage facility, which uses a reliable system owned by Electronic Signature Operator or Electronic Signature Support Service that can detect the changes and meet the following requirements:
- 1. only person authorized to enter new data, change, exchange, or replace data;
- 2. Signer identity information can be checked for authenticity; and
- 3. Other technical changes which violate security requirements can be detected or recognized by the operator.

(4) Signer must maintain confidentiality and be responsible for Electronic Signature Creation Data.

Part Four
Signing Process

Article 56

(1) In the process of signing it should be conducted mechanism to ensure the Electronic Signature Creation Data:

- a. still valid, not canceled, or withdrawn;
- b. not reported missing;
- c. reported no over handle to an unauthorized person; and
- d. is in the proxy of Signer.

(2) Prior to the signing, Electronic Information to be signed must be known and understood by Signer.

(3) Approval Signer on Electronic Information to be signed by the Electronic Signatures must use affirmations mechanism and/or other mechanisms that show the intent and purpose to Signer related with Electronic Transactions.

(4) The methods and techniques used to make the Electronic Signature must include at least:

- a. Electronic Signature Creation Data;
- b. Electronic Signature creation time; and
- c. Electronic Information to be signed.

(5) Changes in Electronic Signature and/or Electronic Information, signed after the signature time shall be known, detected, or identified with a certain method or a certain way.

Article 57

(1) The Electronic Signature and/or Electronic Signature Supporting Services shall be responsible for the use of Electronic Signature Creation Data or Electronic Signature maker tools.

(2) Electronic Signature Operator and Electronic Signature Supporting Services shall use the Electronic Signatures maker tools which apply cryptographic techniques in the process of sending and storage of Electronic Signatures.

Part Five
Electronic Signature Identification, Authentication and Verification

Article 58

(1) Prior to use Electronic Signatures, Electronic Signatures Operator shall ensure identification of Signer by:

- a. Signer sends identity to the Electronic Signatures Operator;
- b. Signer registers to the Electronic Signatures Operator or Supporting Services; and
- c. If necessary, the Electronic Signature Operator may delegate signer data confidential identity to the other Electronic Signature Operator or Electronic Signature Supporting Service with the approval Signer.

(2) The mechanism used by the Electronic Signatures Operator for identity verification of Signer electronically is required to apply a combination of at least 2 (two) factors of authentication.

(3) The verification process of Electronic Information is signed can be done to check Electronic Signature Creation Data to track any changes in the data that was signed.

CHAPTER VI
ELECTRONIC CERTIFICATION OPERATION

One
Electronic Certificate

Article 59

(1) The Electronic System for public services must have an Electronic Certificate.

(2) Electronic System Operator for non public service must have an Electronic Certificate.

(3) Electronic System Operator and Users other than as intended in paragraphs (1) and (2) may have a Electronic Certificate issued by the electronic certification operator.

(4) To have an Electronic Certificate, Electronic System Operator and Users must apply to the electronic certification operator.

(5) Further provisions on the procedure to have the Electronic Certificate are governed by Ministerial Regulation.

Part Two
Electronic Certification Operator

Article 60

Electronic certification operator has the authority to:

- a. examination of prospective owners and/or holders of Certificates Electronics;
- b. Electronic Certificate issuance;
- c. Electronic Certificate extension period;
- d. Electronic Certificate blocking and revocation;
- e. Electronic Certificate validation; and
- f. active and frozen Electronic Certificates list makers.

Article 61

(1) Electronic certification operator that operating in Indonesia must obtain recognition from the Minister.

(2) Recognition as intended in paragraph (1) consists of levels:

- a. registered;

- b. certified; or
- c. has parent.

Article 62

(1) Recognition of the registered status as intended in Article 61 paragraph (2) a can be given by the Minister after the electronic certification operator fulfill registration process requirements are determined in the Ministerial Regulation.

(2) Recognition of the certified status as intended in Article 61 paragraph (2) b is given by the Minister after the electronic certification operator is registered and acquire the status of a accredited electronic certification operator from the accredited electronic certification operator certification agency.

(3) Recognition of the has parent status as intended in Article 61 paragraph (2) c is given by the Minister after the electronic certification operator obtain certified status and obtain a certificate as has parent electronic certification operator.

(4) Further provisions on the granting recognition as electronic certification operator are governed in Ministerial Regulation.

Article 63

(1) To obtain recognition on the electronic certification operation shall be subject to administration fee.

(2) Each revenue on administrative costs as intended in paragraph (1) is a non-tax state revenue.

Part Three
Supervision

Article 64

(1) Monitoring on the electronic certification operation is implemented by the Ministry.

(2) Supervision as intended in paragraph (1) including:

- a. recognition; and
- b. operation of the master electronic certification operation facility for has parent electronic certification operator.

CHAPTER VII
RELIABILITY CERTIFICATION AGENCIES

Article 65

(1) Business Entities who operate Electronic Transaction can be certified by the Reliability Certification Agency.

(2) Reliability Certification Agencies consists of:

- a. Indonesian Reliability Certification Agencies; and
- b. foreign Reliability Certification Agencies.

(3) Indonesian Reliability Certification Agencies as intended in paragraph (2) a shall be domiciled in Indonesia.

(4) Reliability Certification Agencies as intended in paragraph (2) must be registered in the list of Reliability Certification Agencies issued by the Minister.

Article 66

(1) Reliability Certification Agency can issue Reliability Certificate through Reliability Certification process.

(2) Reliability certification as intended in paragraph (1) include an examination of the complete and correct information from Business Entity and its electronic system to obtain Reliability Certificate.

(3) a complete and correct information as intended in paragraph (2) includes information that:

- a. contains the identity of the subject of the law;
- b. load status and competence of the subject of the law;
- c. explain certain things that are required validity of the agreement; and
- d. describes the goods and/or services offered.

Article 67

(1) Reliability Certificate aims to protect consumers in Electronic Transactions.

(2) Reliability Certificate as intended in paragraph (1) is an assurance that the Business Entities have met the criteria set by the Reliability Certification Agency.

(3) Business Entities have met the criteria as intended in paragraph (2) has the right to use Reliability Certificate on the page, and/or other Electronic Systems.

Article 68

(1) Reliability Certificate issued by the Reliability Certification Agency includes categories of:

- a. safeguards against identity;
- b. securing the exchange of data;
- c. safeguard against vulnerabilities;
- d. ranking of consumers; and
- e. safeguard on the confidentiality of personal data.

(2) Further provisions on the procedure for determining the category of Reliability Certificate as intended in paragraph (1) are governed in the Ministerial Regulation.

Article 69

(1) Reliability Certification Agency is established by professionals.

(2) The Professionals who establish Reliability Certification Agency as intended in paragraph (1) at least includes professions of:

- a. Information Technology consultant,
- b. Information Technology auditors; and
- c. legal consultant in the Information Technology field.

(3) Professionals can participate in the establishment of Reliability Certification Agency as intended in paragraph (2) includes professions of:

- a. accountants;
- b. management consultant in information technology;

- c. appraisal;
- d. notary; and
- e. profession within the Information Technology scope established by Ministerial Decree.

(4) Professional as intended in paragraphs (2) and (3) must have a professional certificate and/or a professional license in accordance with the provisions of the regulation.

(5) Further provisions on the requirements and procedures for the registration within the Information Technology scope as intended in paragraph (3) e are stipulated in the Ministerial Regulation.

Article 70

(1) In case of any license of professional who establish Reliability Certification Agency is revoked in accordance with the provisions of regulations, the relevant Reliability Certification Agency must replace professional license revoked with other professionals in the same field within 90 (ninety) days period.

(2) In case of the period as intended in paragraph (1) has been exceeded and Reliability Certification Agency not replace professional, the Minister issued a Reliability Certification Agency from Reliability Certification Agencies list.

Article 71

Supervision of Reliability Certification Agency is implemented by the Minister.

Article 72

(1) To obtain recognition for Reliability Certification Agency subject to administration cost.

(2) Any revenue on administrative cost as intended in paragraph (1) is a non tax state revenue.

CHAPTER VIII
DOMAIN NAME OPERATION

Article 73

(1) Domain Name Operation is conducted by Domain Name Operator.

(2) Domain Name consists of:

- a. Generic high level Domain Name;
- b. Indonesian high level Domain Name;
- c. Indonesian second level Domain name; and
- d. derivative level Indonesian Domain Name.

(3) Domain Name Operator as intended in paragraph (1) shall consist of:

- a. Domain name registry; and
- b. Domain Name Registrar.

Article 74

(1) Domain Name Operator as intended in Article 73 paragraph (3) may be convened by the Government and/or the community.

(2) Communities as intended in paragraph (1) must be incorporated in Indonesia.

(3) Domain Name Operator is determined by the Minister.

Article 75

(1) Domain Name Registry as intended in Article 73 paragraph (3) a conduct operation of generic high level and Indonesian high level Domain Name operation.

(2) Domain Name Registry can provide generic high level and Indonesia high level Domain name registration authority to Domain Name Registrar.

(3) Domain Name Registry has functions to:

- a. provide input to the plan of arrangement of Domain Name to the Minister;
- b. monitoring the Domain Name Registrar; and
- c. Domain name dispute resolution.

Article 76

(1) Domain Name Registrar as intended in Article 73 paragraph (3) b implement the second level and derivative level Domain Names.

(2) Domain Name Registrar consists of Domain Name Registrar Agencies and other than Domain Name Registrar Agencies.

(3) Domain Name Registrar Agencies can make second level Domain name and derivative level Domain Name registration for the need of Agencies.

(4) Domain Name Registrar Agencies as intended in paragraph (3) carried out by the Minister.

(5) Domain Name Registrar other than Agencies shall make the second level Domain Name for commercial and non-commercial users.

(6) Domain Name Registrar other than Agencies shall be registered by the Ministry.

Article 77

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

(2) The registered domain name as intended in paragraph (1) shall meet the following requirements:

a. accordance with the provisions of regulations;

b. decency prevailing in the society; and

c. good faith.

(3) Domain name registry and Domain Name Registrar are authorized to:

- a. reject Domain Name registration in case of Domain Name does not meet the requirements as intended in paragraph (2);
- b. temporarily disable use of the Domain Name, or
- c. remove Domain Name in case of Domain Name user violates any provision of this Government Regulation.

Article 78

(1) Domain name registry and Domain Name Registrar must hold Domain Name operation accountable.

(2) In case of Domain Name Registry or Registrar Domain Name intends to terminate its operation, Domain Name Registry or Registrar Domain Name must submit the entire Domain Name operation to the Minister no later than 3 (three) months before.

Article 79

(1) Domain name indicates Agencies can only be registered and/or used by the agency concerned.

(2) Agencies must use the Domain Name in accordance with the name of the government agency concerned.

Article 80

(1) Domain name registry and Domain Name Registrar receive Domain Name registration from the Domain Name Users.

(2) Domain Name Users as intended in paragraph (1) are responsible for the registration of the Domain Name.

Article 81

(1) Domain Name Registry and/or Domain Name Registrar are entitled to revenue by charging registration fees and/or use of the Domain Name from Domain Name Users.

(2) In case of Domain Name Registry and Domain Name Registrar as intended in paragraph (1) are Domain Name operator other than Agencies, Domain Name Registry and Domain Name Registrar shall deposit part of the revenues of the registration and use of the Domain Name that is calculated from the percentage of revenue to the state.

(3) Revenue as intended in paragraph (1) and revenue as intended in paragraph (2) are non-tax state revenues.

Article 82

Supervision on the Domain Name Operation is undertaken by the Minister.

Article 83

Provisions on the requirements and procedures for determining Domain Name Operator are governed in Ministerial Regulation.

CHAPTER IX
ADMINISTRATIVE SANCTIONS

Article 84

(1) Violation of Article 7, paragraph (1), Article 8 paragraph (1) and paragraph (3), Article 12 paragraph (1) and paragraph (2), Article 13, Article 14 paragraph (1), Article 15 paragraph (1), Article 16 paragraph (1), Article 17 paragraph (1), Article 18 paragraph (1), Article 21, Article 22 paragraph (1), Article 27, Article 29, Article 30 paragraph (1), Article 37 paragraph (1), Article 39 paragraph (1), Article 58 paragraph (1) and paragraph (2), Article 59 paragraph (1), and Article 78 paragraph (1) subject to administrative sanctions.

(2) The administrative sanctions as intended in paragraph (1) may be:

- a. written warning;
- b. administrative fee;
- c. temporary suspension; and/or
- d. removed from the list as intended in Article 5 paragraph (4), Article 37 paragraph (2), Article 62 paragraph (1), and Article 65 paragraph (4).

(3) The administrative sanction given by the Minister or head of related Sector Supervisory and Regulatory Agency is in accordance with the provisions of the regulation.

(4) The imposition of sanctions by the head of related Sector Supervisory and Regulatory Agency as intended in paragraph (3) shall conducted after coordination with the Minister.

(5) The imposition of administrative sanctions as intended in paragraphs (2) and (3) do not eliminate criminal and civil liability.

Article 85

Further provisions on the procedure for the imposition of administrative sanctions and filing an objection to the imposition of administrative sanctions are stipulated in the Ministerial Regulation.

CHAPTER X
TRANSITIONAL PROVISIONS

Article 86

(1) When this Ministerial Regulation comes into force, Electronic System Operator for the public services that has been in operation before the this Ministerial Regulation comes into force, shall apply to the Minister within a period of one (1) year since this Ministerial Regulation comes into force.

(2) Electronic System Operator as intended in paragraph (1) is not conduct the registration subject to administrative penalties for each year of delay.

Article 87

At the time this government regulation come into force, the Electronic System Operator has been operating before the enactment of this Government Regulation, shall conform with this Government Regulation within a maximum period of 5 (five) years from this Ministerial Regulation comes into force.

Article 88

When this Ministerial Regulation comes into force, the electronic certification operator and Reliability Certification Agency that have been operating in Indonesia before the this Ministerial Regulation comes into force, shall conform with the provisions of this Ministerial Regulation within a maximum period of 3 (three) years from this Ministerial Regulation comes into force.

Article 89

At the time this Regulation came into force:

- a. Electronic System Capability Certification issued by the domestic agencies in accordance with the provisions regulation, remain in effect until the enactment of Ministerial Regulation on the Electronic System Capability Certification; and
- b. Electronic System Capability Certification issued by foreign institutions that meet the accreditation in the country concerned, remains in effect until the enactment of Ministerial Regulation on the Electronic System Capability Certification.

CHAPTER XI
CLOSING PROVISION

Article 90

This Government Regulation shall come into force on the date of promulgation.

For public cognizance, this Government Regulation shall be promulgated by placing it in the State Gazette of the Republic of Indonesia.

Stipulated in Jakarta
on October 12, 2012
THE PRESIDENT OF THE REPUBLIC OF INDONESIA,
signed,
DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta
on October 15, 2012
MINISTER OF LEGAL AND HUMAN RIGHTS OF REPUBLIC OF INDONESIA
signed,
AMIR SYAMSUDIN

STATUTE BOOK OF THE REPUBLIC OF INDONESIA NUMBER 189 OF 2012