NATIONAL ASSEMBLY
Law no.: 86/2015/QH13

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom - Happiness

LAW ON NETWORK INFORMATION SECURITY

Pursuant to the Constitution of the Socialist Republic of Vietnam;

The National Assembly hereby promulgates the Law on Information Security.

CHAPTER I
GENERAL PROVISIONS

Article 1. Scope

This law provides regulations on network information security activities, rights and duties of agencies, organizations and individuals in securing network information security; civil cryptography; technical standards and norms of network information security; business in information security; human development for network information security; state management of network information security;

Article 2. Subjects of application

This law shall apply to any Vietnamese agencies organization, individual; foreign organization and individual in Vietnam who directly involves in or is related to network information security activities in Vietnam.

Article 3. Definitions

In this Law, the following terms shall be construed as follows:

1. *Network information security* means the protection of network information and information systems against any illegal access, use, disclosure, interruption, amendment or sabotage in order to ensure the integrity, confidentiality and availability of information.

2. *Network* is the environment where information is supplied, transmitted, collected, processed, stored and exchanged via telecommunication networks and computer networks.

3. *Information system* means any assembly of hardware, software and database which is purposely set up for establishment, supply, communication, collection, handling, storage and exchange of network information.

4. *National important information system* means an information system that any of its sabotage will result in damage particularly serious to national defense and security.

5. *Information system owner* means an organization or individual who has the power to directly manage its/his/her own information system.

6. *Violation of network information security* means an act of illegal access to, use, disclosure, interruption, amendment or sabotage of information or information system.

7. *Information security incident* means a failure of information or an information system with consequent impacts on its confidentiality, integrity or availability.

8. *Information security risk* means a subjective or objective factor that potentially affects the status of network information security.

9. *Information security risk assessment* means detection, analysis and estimation of a damage or threat to information or information system.

10. *Information security risk management* means providing a set of measures to reduce network information security risks.

11. *Malicious software* (Malware) means a software that is able to cause any abnormal operation to an information system in part or in whole, or to illegally reproduce, change, or delete information stored in the information system.

12. *Malware filter system* means a combination of hardware and software connected to a network in order to detect, block, filter and reckon malware up.

13. *Electronic address* means an address in use for sending and receiving cyber information that can be an email address, telephone number, Internet address and other smiliar forms.

14. *Information conflict* means two or more local and foreign organizations taking measures of information technology or technique to damage an information system, a program or an information source.

15. *Personal information* means information associated with the identity of a specific person.

16. *Personal information owner* means the person identified by the personal information.

17. *Handling personal information* means performance of one or more operations to collect, edit, use, store, supply, share, and disperse personal information in the network for commercial purposes.

18. *Civil cryptography* means cryptographic techniques and encrypted products in use for confidentiality or authentication of the information which is beyond the domain of state secret.

19. *Network information security product* means any hardware or software product which is functioned to protect information and information system.

20. *Network information security service* means the service to protect information and information system.

Article 4. Principles of network information security

1. Organizations, individuals shall be responsible for ensuring network information security. Information security activities of organizations, individuals shall comply with regulations of laws, secure national security, state secrets, maintain political stability and promote economic and social developments.

2. Organizations, individuals taking part in online activities shall not violate network information security of other organizations, individuals.

3. Handling of information incidents shall ensure legitimate rights and benefits of individuals, organizations, without infringement upon the private and secret life of individuals, family secrets of individuals and private information of organizations.

4. Activities of network information security guarantee shall be performed frequently, continuously, and effectively.

Article 5. State policies on network information security

1. Promoting training and human resource development for network information security to meet demands for political stability, socio-economic developments, national defense, social order and safety.

2. Encouraging research and development, supporting export and market expansion for products and services, providing mechanism to support the application of network information security technique and engineering domestically produced or supplied; giving favorable conditions for importing advanced products and technologies that cannot be produced or supplied domestically.

3. Securing an environment of fair competition in provision network information security products and services; encouraging and creating conditions for organizations, individuals to invest, research and develop and supply network information security products and services.

4. Allocating resources to ensure network information security of state bodies and network security of information systems of national importance.

Article 6. International cooperation on network information security

1. International cooperation on network information security should abide by the principles as follows:

a) Respecting the independence, sovereignty and territorial integrity of countries without intervention in internal affairs of the others, for equality and mutual benefits;

b) Complying with Vietnam laws and international treaties to which the Socialist Republic of Vietnam is a state member.

2. Contents of international cooperation on network information security:

a) International cooperation on research and application of science, technique and engineering of network information security;

b) International cooperation in prevention and fighting against illegal acts in relation with network information security, and against the abuse of information network for terrorist acts;

c) Other international cooperation on network information security.

Article 7. Prohibited acts

1. Illegal prevention of network information transmission; intervention, access, damaging, deletion, change, reproduction and misleading of network information.

2. Illegal affecting, blocking the normal operation of an information system or legal access possibility of users to an information system.

3. Attack, illegal invalidation to disable the measures in place to protect network information security for an information system; attack, illegal appropriation of rights to control, and sabotage of an information system.

4. Sending spams, malware, establishing a fake or swindling information system.

5. Illegal collection, use, dissemination of or trading in personal information of others; exploitation of a weekness point of an information system to collect and exploit personal information.

6. Illegal access to the confident code and legally encoded information of agencies, organization, or individuals; disclosure of information of civil code products; use of and trading in civil code products of unclear origin.

Article 8. Treatment of network information security violation

Any person, who commits an act in violation of regulations set forth herein shall, depending on the nature and level of violation, be subject to disciplinary or administrative treatment or penal proceedings, and to payment for any damage, if any, under current laws.

CHAPTER II

ASSURANCE OF NETWORK INFORMATION SECURITY

Section 1

NETWORK INFORMATION PROTECTION

Article 9. Classification of information

1. The organization with information in its possession shall classify it by confidentiality in order to take appropriate protection measures.

2. Information in the domain of state secret shall be classified and protected as set forth in regulations on protection of state secrets.

The organization using classified or unclassified information for activities in its field shall be responsible for establishing regulations and procedures to handle information, to determine the contents and methods to record permitted accesses to classified information.

Article 10. Administration of information sending

1. Sending network information shall ensure the requirements as follows:

a) not faking the sending source;

b) complying with regulations herein and relevant laws.

2. Organizations, individuals must not send commercial information to a recipient's electronic address without his/her prior consent, request, or when the recipient refuses it, except for the cases where the recipient is obliged to receive the information under current laws.

3. Telecommunications companies, enterprises providing telecommunications application services, and enterprises rendering information technology services that send information shall:

a) Comply with legal regulations on information storage, and protection of personal information and private information of organizations, individuals;

b) Take measures to stop and respond upon receipt of any notice from organizations, individuals of sending information in violation of legal regulations;

c) Make it available for recipients to have rights to refuse further receive information;

d) Provide technical and professional conditions necessary for competent state bodies to, upon request, perform duties of state administration of network information security.

Article 11. Prevention, detection, blocking and treatment of malware

1. Agencies, organizations, and individuals shall be responsible for prevention and blocking of malware as instructed or required by competent state bodies.

2. Owners of national important information systems shall deploy professional and technical systems to prevent, detect, block and handle malware in due time.

3. Organizations shall provide services of email, information transmission and storage shall have malware filtration systems in place during sending, receiving, and storing of information in their own systems and shall report to competent agencies as stipulated by laws.

4. Internet service providers shall take measures to manage, prevent, detect, and block the dispersal of malware and treatment thereof upon request of competent state bodies.

5. The Ministry of Information and Communications shall be in charge and cooperate with the Ministry of Defense, the Ministry of Public Security, relevant ministries, sectors for organizing to prevent, detect, block and handle malware that is causative of impacts in national defense and security.

Article 12. Assurance of telecommunications resources

1. Organizations, individuals using telecommunication resources shall:

a) Take managerial and technical measures to avoid information insecurity that is originated from their own frequencies, stocks of numbers, domain names and Internet addresses;

b) Provide, upon request, information relating to security of telecommunications resources and cooperate with competent agencies.

2. Internet service providers shall manage, cooperate and avoid of information insecurity that is originated from their own Internet resources and clients, provide sufficient information upon request of competent state bodies; cooperate for connection and routing in order to secure safe and stable operations of the Vietnam domain name server system.

3. The Ministry of Information and Communications shall be responsible for network information security for the Vietnam domain name servers.

Article 13. Response to network information security incidents

1. A response to network information security incidents means an activity to handle with and remedy any incidents causative of network information insecurity.

2. Any response to a network information security incident shall comply with the principles as follows:

a) Timely, speedy, accurate and effective;

b) Compliant with legal regulations on coordination of responses to network information security incidents;

c) Cooperative between local and foreign agencies, organizations and businesses.

3. Ministries and equivalents, agencies under the Government, People's Committees of provinces and cities subordinate to the Central Government, telecommunications companies, and owners of national important information systems shall establish or appoint specialized divisions in charge of responses to network information security incidents.

4. The Ministry of Information and Communications shall coordinate nationwide responses to network information security incidents and detail the coordination of responses to network information security incidents.

Article 14. Emergency response to secure national network information security

1. Emergency response to secure national network information security means urgent response in case of catastrophic circumstance or upon request of competent agencies in order to secure national network information security.

2. Emergency response to secure national network information security shall comply with the principles as follows:

a) Organization and implementation as decentralized;

b) Action in a rapid, strict and close coordinative manner;

c) Application of scientific and engineering measures to ensure effectiveness and feasibility.

3. The system of emergency responses to secure national network information security includes:

a) Emergency response plan to secure national network information security;

b) Emergency response plan for urgent responses to secure network information security of state bodies, political and social-political organizations;

c) Emergency response plan for urgent responses to secure network information security of localities;

d) Emergency response plan for urgent responses to secure network information security of telecommunications companies.

4. The responsibility of concerned parties for coordination to secure national network information security is as follows:

a) The Prime Minister makes decisions on the plans for emergency response to secure national network information security;

b) The Ministry of Information and Communications shall direct and coordinate to secure national network information security;

c) Ministries, sectors and local authorities shall coordinate and direct emergency responses to secure network information security at ministries, sectors and localities;

d) Telecommunications companies shall implement and coordinate with the Ministry of Information and Communications and relevant ministries, sectors and localities to secure national network information security.

Article 15. Responsibilities of organizations, individuals in network information security

1. Agencies, organizations, individuals involving in network information security activities shall cooperate with competent state bodies and other organizations, individuals in securing network information security.

2. Agencies, organizations, individuals using network services shall timely inform the service provider or response-specialized division on detection of any act of sabotage or network information security incident.

Section 2

PROTECTION OF PERSONAL INFORMATION

Article 16. Principles of personal information protection in network

1. Individuals using network services shall protect their own personal information and compliance with laws on supply of personal information.

2. Organizations, individuals handling personal information shall ensure network information security for the personal information they handle.

3. Organizations, individuals handling personal information shall build up and publicize their policies applicable to handling and protection of personal information of their own organizations, individuals.

4. Personal information protection shall adhere to regulations of this Law and specific regulations of relevant fields.

5. Handling of personal information for the purpose of national defense, security, social order and security or for non-commercial purposes shall observe other regulations of relevant laws.

Article 17. Collection and use of personal information

1. Organizations, individuals handling personal information shall:

a) Collect personal information only after obtaining the consent of information owner on the scope and purpose of the information collection and use;

b) Use collected personal information for any purpose different from the initial one only after obtaining the personal information owner's agreement.

c) Must not share, disperse the collected, accessed or controlled personal information to any third party, unless it is agreed by the personal information owner or requested by competent state bodies.

2. State bodies shall be responsible for the confidentiality and storage of personal information that they collect.

3. The personal information owner shall have rights to require any organization, individual handling personal information to provide his/her personal information that is collected and stored by the organization, individual.

Article 18. Updating, change and deletion of personal information

1. The personal information owner shall have rights to require organizations, individuals handling personal information to update, change, and delete his/her personal information that the handling organizations, individuals collect, store or to cease, if he/she previously agrees on, the supply of his/her personal information to a third party.

2. Upon receipt of a valid requirement of updating, change or deletion of personal information from the owner or a valid requirement of ceasing the supply of his/her personal information to a third party, organizations, individuals handling personal information shall:

a) Fulfill the requirement and notice the personal information owner thereof or provide the personal information owner with rights to access, update, change or delete his/her own personal information;

b) Take suitable measures to protect personal information; notice the personal information owner thereof in cases that it is not yet possible to fulfill the requirement due to technical or other factors.

3. Organizations, individuals handling personal information shall delete the stored personal information when the purpose of use is accomplished or the storage period expires and shall notice the personal information owner thereof, unless otherwise stipulated by laws.

Article 19. Protection of personal information security in network

1. Organizations, individuals handling personal information shall take appropriate managerial and technical measures to protect personal information that they collect and store; comply with technical standards and norms of network information security.

2. In cases of technical incidents or risks thereof, organizations, individuals handling personal information are required taking remedial, blocking measures as soon as possible.

Article 20. Obligations of state administration agencies in network personal information protection

1. Establishing online information channels to receive feedbacks and recommendations by organizations, individuals in relation with personal information security.

2. Periodically inspecting, examining organizations and companies handling personal information; inspecting without prior notice when needed.

Section 3

INFORMATION SYSTEM PROTECTION

Article 21. Classification in security of information systems

1. Security classification of an information system means determination of its network information security level in the increment order from 1 to 5 to take managerial and technical measures to protect it accordingly.

2. Information system shall be categorized into security levels as follows:

a) Level 1 is the level that when an information system is sabotage, it will damage legitimate rights and benefits of organizations, individuals, not public benefits, social order and safety, national defense or security;

b) Level 2 is the level that when an information system is sabotage, it will severely damage legitimate rights and benefits of organizations, individuals, damage public benefits, not social order and safety, national defense or security;

c) Level 3 is the level that when an information system is sabotage, it will severely damage production, public benefits, social order or damage safety, national defense or security;

d) Level 4 is the level that when an information system is sabotage, it will extremely damage public benefits, social order or damage safety, or severely damage national defense or security;

e) Level 5 is the level that when an information system is sabotage, it will extremely damage national defense or security;

3. The Government shall stipulate details of criteria, power, sequence and procedures to determine the security levels of information systems responsibilities for securing network information security at every level.

Article 22. Duties on information system protection

1. To determine security levels of information systems

2. To assess and manage security risks to information systems.

3. To urge, supervise and examine the protection of information systems.

4. To take measures to protect information systems.

5. To comply with the reporting regime.

6. To conduct public information for raising awareness about network information security.

Article 23. Measures to protect information systems

1. Issuing regulations on network information security in designing, construction, management, operation, use, and cancellation of information systems.

2. Applying technical measures in accordance with technical standards and norms of network information security to prevent, avoid of and remedy network information security incidents.

3. Inspecting and monitoring of the compliance with regulations and evaluation of effectiveness of managerial and technical measures in use.

4. Monitoring of information system security.

Article 24. Monitoring security of information system

1. Monitoring security of information system is action to select subjects, tools for monitoring, collecting and analyzing information status of the monitored subjects to identify the factors that might constitute impacts on the information system; to report and warn of any act of violation of network information security or any act that might cause any network information security incident to the information system; to analyze the crucial key factors that affect the network information security status; to recommend changes in technical measures.

2. Subjects to safety status monitoring include: firewall, access control, main information route, important server, device or terminal.

4. Telecommunications companies, information technology service providers and network information security service providers shall cooperate with information system owners in monitoring of information system safety upon request of competent state bodies.

Article 25. Responsibilities of information system owners

1. Information system owners shall protect information systems pursuant to regulations in Articles 22, 23 and 24 of this law.

2. Information systems owners using state budget shall perform according the responsibilities set forth in item 1 hereof and shall:

a) Have plans for network information protection that are appraised by competent state bodies when the information system is established, expanded or upgraded.

b) Appoint individual(s) or division(s) in charge of network information security.

Article 26. National important information systems

1. The establishment, expansion and upgrading of national important information system shall be subject to network information security auditing prior to operation and exploitation.

2. The Ministry of Information and Communications shall preside over and cooperate with the Ministry of Defense, the Ministry of Public Security and relevant ministries and sectors to prepare a list of national important information systems and submit for the Prime Minister to issue.

Article 27. Responsibilities for securing network information security for national important information systems

1. Owners of national important information systems shall:

a) Implement regulations set forth in Article 25.2 of this Law;

b) Periodically assess network information security risks. This shall be done by a specialized organization that is appointed by competent authorities;

c) Deploy standby solutions for information systems;

d) Make protective plans and maneuver plans for protecting national important information systems.

2. The Ministry of Information and Communications shall:

a) Preside over and cooperate with owners of national important information systems, the Ministry of Public Security and relevant ministries and sectors to instruct, supervise, inspect and examine activities of network information security protection for national important information systems, except for the systems set forth in items 3 and 4 of this Article;

b) Require telecommunications companies, information technology companies to participate in technical consultancy, support and response to network information security incidents for information systems of national importance.

3. The Ministry of Public Security shall preside over, instruct, supervise, inspect and examine activities of network information security protection for national important information systems under its administration; cooperate with the Ministry of Information and Communications, relevant owners of national important information systems, ministries, sectors and People's Committees at various levels in safeguarding national important information systems upon request of competent agencies.

4. The Ministry of Defense shall preside over, instruct, supervise, inspect, and examine network information security protection activities for national important information systems under its administration.

5. The Government Information Security Commission shall preside and apply encoding solutions to national important information systems that belong to state bodies, political and social-political organizations; cooperate with owners of national important information systems in network information security monitoring under current laws.

Section 4

PREVENTION OF NETWORK INFORMATION CONFLICTS

Article 28. Responsibilities of organizations and individuals in prevention of network information conflicts

1. Organizations and individuals shall, within their duties and power:

a) Prevent sabotage information from their own information systems; cooperate to identify sources, drive back and remedy consequences of cyber attacks via information systems of local and foreign organizations and individuals.

b) Block any act of domestic or foreign organizations and individuals that is aimed at sabotage of the network integrity.

c) Eliminate the implementation of illegal acts by local and foreign organizations and individuals on the network that severely affects national defense and security, social order and security.

2. The Government shall provide details for prevention of network information conflicts.

Article 29. Prevention of network use for the purpose of terrorism

1. Measures to stop network use for the purpose of terrorism include:

a) Neutralization of the Internet source in use for the terrorist act;

b) Blocking the establishment and expansion of information exchange in relation to signals, factors, methods and usages of the Internet for the purpose of terrorism, targets and operations of cyber terrorism organizations;

c) Exchange of experiences and practices in controlling of Internet sources, chase and control of contents of websites having terrorist purposes;

2. The Government shall provide details of responsibilities for implementation and measures to stop network use for the purpose of terrorism.

CHAPTER III

CIVIL CRYPTOGRAPHY

Article 30. Civil code products and services

1. Civil cryptographic product means materials, technical equipment and cryptographic skills for protecting information that is out of the state secret domain.

2. Civil cryptographic service means service to protect the information on use of a civil cryptographic product; examination and evaluation of civil code products; consultancy for confidentiality and network information security using civil code products.

Article 31. Trading in civil encryption products

1. Companies trading in civil encryption products shall obtain business licenses for trading in cryptographic products or services in the list of cryptographic products or services.

2. A companies is granted a business license for trading in cryptographic products or services shall it meet the conditions as follows:

a) Having administrative, management and technical staff that meet skill requirements of information confidentiality and security;

b) Having equipment and facilities in line with the scale of trading in cryptographic products or services;

c) Having feasible technical and sales plans in compliance with regulations, technical standards and norms;

d) Having plans for network information confidentiality and security for the process of, management and supply of cryptographic products or services;

e) Having an appropriate business plan.

3. Cryptographic products shall be subject to examination and certification of meeting standards before circulation on the market.

4. Companies being granted Business licenses for trading in civil code products and services shall pay fees as stipulated by laws on fees and charges.

5. The Government shall issue the list of civil code products and services and details of this Article.

Article 32. Sequence, procedures to get business licenses for trading in civil cryptographic products and services

1. The applicant applying to get a business license for trading in civil cryptographic products and service shall submit the application to the Government Cipher Committee.

2. The application for obtaining a business license for trading in civil cryptographic products and service shall be established in two copies, including:

a) Request for business license for trading in civil cryptographic products;

b) Copy of the business registration certificate, investment registration certificate or equivalent;

c) Copy of diplomas or skill certificates on information confidentiality and security of the management, operation and technical staff;

d) Technical plan, including documentations of technical specification and parameters of products; technical norms of products; standards and quality of services; technical solutions and measures; plans for product maintenance and service;

đ) Plan of network information confidentiality and security during the process of management and supply of civil cryptographic products and services;

e) Business plan, including scope, subject matters of supply, scale of products, services and systems to serve clients and technical guarantees.

3. Within 30 days as of receipt of sufficient documents, the Government Cipher Committee shall examine and grant the business license for trading in civil cryptographic products and services; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

4. Business licenses for trading in civil cryptographic products and services shall be valid for 10 years.

Article 33. Amendment, reissue, suspension and withdrawal of business licenses for trading in civil cryptographic products and services

1. Amendment to a business license granted for a company for trading in civil cryptographic products and services shall be made in cases of any change in the name, legal representative of the company or any change or addition of civil cryptographic products and services.

The concerned company shall apply for amendment to the business license with the Government Cipher Committee. The application shall be established in two copies, including:

a) Request for business license amendment;

b) Copy of the business registration certificate, investment registration certificate or equivalent;

c) The granted business license for trading in civil cryptographic products and services;

d) Technical plan, network information confidentiality and security plan, business plan for the added products and services as specified in points d, đ and e, Clause 2, Article 32 of this Law, in case that the company requests to add civil cryptographic products and services, business sectors and fields;

Within 10 working days as of receipt of sufficient documents, the Government Cipher Committee shall examine, amend and reissue the business license for the company; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

2. In cases of loss or damage of the business license for trading in civil cryptographic products and services, the company shall make a request, specifying reasons, with Government Cipher Committee for re-grant the license. Within 05 working days as of receipt of the request, the Government Cipher Committee shall examine and re-grant the business license to the company.

3. The company, which has not violated any regulations of laws on trading in civil cryptographic products and services, shall have its business license for trading in civil cryptographic products and services renewed once with the renewal period of at most 01 year. The request for renewing the license shall be submited to the Government Cipher Committee at least 60 days before the expiry date of the license. The application for renewing the license shall be established in two copies, including:

a) Request for renewing the license;

b) Valid business license for trading in civil cryptographic products and services;

c) Report on the company's operations in the latest 02 years.

Within 20 days as of receipt of sufficient documents, the Government Cipher Committee shall examine and make decision on renewal and re-grant of the license to the company; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

4. A company shall be suspended from trading in civil cryptographic products and services for at most 06 months in the cases as follows:

a) Providing a product or service which fails to comply with the contents of the License;

b) Failing to meet one of the conditions set forth in Article 31.2 of this Law;

c) Other cases as stipulated by laws.

5. A company shall have its license for trading civil cryptographic products and services revoked in the cases as follows:

a) It fails to provide the service within 01 year as of the grant date of the License without legitimate reason;

b) The license expired;

c) It fails to remedy the problems mentioned in Clause 4 of this Article after the suspension period expires.

Article 34. Importation and exportation of civil cryptographic products

1. In importation and exportation of civil cryptographic products in the list of civil cryptographic products to be imported and exported under permits, the company shall hold a permit for importation and exportation of civil cryptographic products that is granted by competent state bodies.

2. A company shall be granted a permit for importation and exportation of civil cryptographic products if it meets the conditions as follows:

a) It holds a business license for trading in civil cryptographic products;

b) The civil cryptographic product to be imported is certified and announced of norm conformity as set forth in Article 39 hereof;

c) The subject and purpose of using the civil cryptographic product do not cause damages to national defense, security and social discipline and safety.

3. The application for obtaining a permit for importation and exportation of civil cryptographic products shall include:

a) Request for the permit for importation and exportation of civil cryptographic products;

b) Copy of the business license for trading in civil cryptographic products and services;

c) Copy of the norm conformity certificate on the imported civil cryptographic product.

4. Within 10 working days as of receipt of sufficient documents, the Government Cipher Committee shall examine and grant the company a permit for importation and exportation of civil cryptographic product; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

5. The Government shall issue the list of civil cryptographic products to be imported and exported under permits and detailed regulations on this Article.

Article 35. Responsibilities of companies trading in civil cryptographic products and services

1. Management of documents and materials relating to technical and engineering solutions of products.

2. Making, storing and keeping secret of client information such as name, type, quantity, and purpose of use of civil cryptographic products and services.

3. Annually reporting to the Government Cipher Committee on their business, importation and exportation of civil cryptographic products and services and a summary of client information before 31 December every year.

4. Taking measures to ensure security and safety during transport and storage of civil cryptographic products.

5. Refusing to provide civil cryptographic products and services when detecting of the relevant organization, individual’s violation of laws on use of civil cryptographic products and services, or violation of agreed undertakings on use of the product or service provided by the company.

6. Suspending or ceasing the provision of civil cryptographic products and services in order to ensure national defense and security, social discipline and order upon request of competent state bodies.

7. Cooperating, giving conditions for competent state bodies to take professional measures when required.

Article 36. Responsibility of organizations, individuals using civil cryptographic products and services

1. Complying with regulations undertaken with the provider of civil cryptographic products regarding the use management of cryptographic keys, transfer, repair, maintenance, abandonment and destruction of civil cryptography products, and other relevant contents.

2. Providing necessary information relating to cryptographic keys for competent state bodies upon request.

3. Cooperating, giving conditions for competent state bodies to take measures to prevent crimes of stealing information or cryptographic keys and using civil cryptographic products for illegal purposes.

4. Organizations, individuals using a civil cryptographic product which is provided by a provider not licensed for trading in civil cryptographic products shall declare it with the Government Cipher Committee, except for diplomatic agencies, foreign consulates and representative agencies of inter-governmental organizations in Vietnam.

CHAPTER V

STANDARDS AND NORMS ON NETWORK INFORMATION SECURITY

Article 37. Standards and norms of network information security

1. Network information security standards include international standards, regional standards, foreign standards, national standards and manufacturer standards on information systems, hardware, software, and systems for management and safe operation of network information which are announced and recognized for application in Vietnam.

2. Technical regulations of network information security include national and local norms on information systems, hardware, software products, and information systems, procedures of management and operation of network information security that are established, issued and applied in Vietnam.

Article 38. Management of Standards and norms of network information security

1. Certification of network information security norms conformity means certifying that hardware, software products, information systems, management systems for network information security conform to technical norms of network information security.

2. Publication of network information security norms conformity means an organization or company announces the conformity of hardware, software products, information systems, management systems for network information security with technical norms of network information security.

3. Certification of network information security standard conformity means certifying that hardware, software products, information systems, management systems for network information security conform to standards of network information security.

4. Publication of network information security standard conformity means an organization or company announces the conformity of hardware, software products,

information systems, management systems for network information security with standards of network information security.

5. The Ministry of Science and Technology shall preside over, coordinate relevant agencies to appraise and promulgate national standards of network information security under current laws on standards and norms.

6. The Ministry of Information and Communications shall:

a) Draft the national standards of network information security, excepting national standards mentioned in Clause 7 of this Article;

b) Issue the norms of network information security, excepting national standards mentioned in Clause 7 of this Article; and stipulate network information security regulation conformity assessment;

c) Administer the quality of network security products and services, except for civil cryptographic products and services;

d) Register, appoint and manage operations of the organization in charge of certification of network information security conformity; except for the organization in charge of conformity certification for civil cryptographic products and services.

7. The Government Cipher Committee shall assist the Minister of Defense to draft the national standards applicable to civil cryptographic products and services, submit same for competent agencies to promulgate and instruct for implementation; prepare and submit same for the Minister of Defense to promulgate the national norms of civil cryptographic products and services, appoint and manage operations of the organization in charge of conformity certification for civil cryptographic products and services; manage the quality of civil cryptographic products and services.

8. Provincial People's Committees shall establish, issue and instruct for implementation of local norms of network information security; manage the quality of civil cryptographic products and services in their administration areas.

Article 39. Assessment of network information security conformity to standards and norms

1. Assessment of conformity to standards and norms of network information security shall be performed for the cases as follows:

a/ Regulation conformity certification or announcement shall be conducted and regulation conformity stamps shall be used before an organization or individual markets network information security products;

b/ To serve the state management of network information security.

2. Assessment of conformity to standards and norms of network information security for national important information systems and for state management of network information security shall be performed by the conformity assessment organization appointed by the Minister of Information and Communications.

3. Assessment of conformity to standards and norms of civil cryptographic products and services shall be performed by the conformity assessment organization appointed by the Minister of Defense.

4. The mutual recognition of assessment results regarding conformity to standards and norms of network information security between Vietnam and a country or territory and

between the conformity certification organization of Vietnam and those of other nations and territories shall observe legal regulations on standards and technical norms.

CHAPTER VI

NETWORK INFORMATION SECURITY BUSINESS

Section 1

GRANT OF LICENSE FOR BUSINESS IN NETWORK INFORMATION SECURITY PRODUCTS AND SERVICES

Article 40. Business in network information security

1. Business in network information security shall be conditional. Business in network information security includes business in network information security products and business in network information security services.

2. Businesses in network information security products and services set forth in Article 41 herein shall obtain licenses for business in network information security products and service that are granted by competent state bodies. The term of a license for business in network information security products and services shall be valid for 10 years.

3. Trading in network information security products and services shall comply with this Law and others relevant laws.

The conditions applicable to business, procedures of granting business license for trading in civil cryptographic products and services, importation and exportation of civil cryptographic products and services, responsibilities of companies trading in civil cryptographic products and services and the use of civil cryptographic products and services shall observe regulations in Chapter III of this Law.

Conditions and the order and procedures for grant of licenses for provision of digital signature certification services must comply with the law on electronic transactions.

Article 41. Network information security products and services

1. Information security services include:

a) Information security test and assessment;

b) Information confidentiality without civil cryptography;

c) Civil cryptographic services

d) Digital signature services;

đ) Network information security consultancy;

e) Network information security monitoring;

g) Network information security incident response serices;

h) Date recovery services;

i) Cyber attack prevention services.

k) Others

2. Information security products include:

a) Civil cryptographic products;

b) Products for testing and assessing network information security;

c) Products for monitoring network information security;

d) Products against attacks or hacking;

đ) Others.

3. The Government shall provide details of the list of network information security products and services mentioned at Point k, Clause 1, and Point dd, Clause 2, of this Article.

Article 42. Conditions for granting business license for trading in network information security products and services

1. Companies shall be granted business licenses for trading in network information security products and services, except those mentioned at Points a, b, c and d, Clause 1, and Point a, Clause 2, Article 41 of this Law, when fully meeting the following conditions:

a) Conformity to the strategy and planning for national network information security development;

b) Having equipment and facilities in line with the scale of providing network information security products and services;

c) Having managerial, operational and technical staff meeting skill requirements of information security;

d) Having appropriate business plans.

2. Companies shall be granted business licenses for rending network information security examination and assessment should they meet all the conditions as follows:

a) Conditions specified in Clause 1 of this Article;

b) Establishment and legal operation in Vietnam, excepting foreign-invested companies;

c) Company's legal representatives, and the managerial, operational and technical staff being Vietnamese citizens permanently residing in Vietnam;

d) Having technical plans that meet technical standards and norms;

đ) Having plans for client information confidentiality in the process of rendering services

e) Managerial, operational and technical staff having diplomas or skill certificates on information security examination and assessment.

3. Companies shall be granted business licenses for rending information confidentiality services without use of civil cryptographic should they meet all the conditions as follows:

a) Conditions specified at Points a, b, c, d and dd, Clause 2 of this Article;;

b) Managerial, operational and technical staff having diplomas or skill certificates on information confidentiality.

4. The Government shall provide details of this Article.

Article 43. Application for permits to trading network information security products and services

1. The company, which requests a permit to trading network information security products and services, shall file its application for the permit with the Ministry of Information and Communications.

2. The application for the permit to trading network information security products and services shall be established in five copies, including:

a) Request for the permit to trading network information security products and services, specifying the type of network information security products and services to be traded;

b) Copy of business registration certificate, investment registration certificate or equivalent;

c) Explanation of technical equipment and facilities to ensure the conformity with legal requirements;

d) Business plan, including the scope, subjects to render products and services, standards, and the quality of products and services;

đ) Copies of diplomas or skill certificates on information security of the managerial, operational and technical staff.

3. In addition to the papers and documents mentioned in Clause 2 of this Article, the application for the permit to trading information security examination and assessment services or information confidentiality services without use of civil cryptographics shall include:

a) Police record sheets of the legal representative and the managerial, operational and technical staff;

b) Technical plan;

c) Plan for client information confidentiality in the process of rendering services.

Article 44: Application examination and grant of permits for trading in network information security products and services

1. Within 40 days as of receipt of sufficient documents, the Ministry of Information and Communications shall preside over and coordinate relevant ministries and sectors to examine and grant permits for trading network information security products and services, except for trading in the products and services mentioned at Points c and d, Clause 1, and Point a, Clause 2, Article 41 of this Law; any rejection shall be noticed in writing, specifying the reasons thereof.

2. A permit for trading in network information security products and services shall have the main contents as follows:

a) Company's name, transaction name in Vietnamese and foreign language(s) (if any); address of its main office in Vietnam;

b) Name of the legal representative;

c) Number, grant date, and expiry date of the permit;

d) Network information security products and services permitted for trading.

3. The company, which is granted a permit for trading in network information services and products, shall pay fees under laws on fees and charges.

Article 45. Amendment, renewal, suspension, withdrawal and re-grant of business licenses for trading in network information security products and services

1. Amendment to a business license granted for a company for trading in network information security products and services shall be made in cases of any change in the name, legal representative of the company or any change or addition of network information security products and services rendered by itself.

The concerned company shall apply for amendment to the license with the Ministry of Information and Communications. The application shall be established in two copies, including: the request for business amendment, a report detailing the contents to be amended and other relevant documents.

Within 10 working days as of receipt of sufficient documents, the Ministry of Information and Communications shall examine, amend and re-grant the license for the company; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

2. In cases of loss or damage of the license for trading in network information security products and services, the company shall make a request, specifying reasons, with the Ministry of Information and Communications for re-grant the license. Within 05 working days as of receipt of the request, the Ministry of Information and Communications shall examine and re-grant the license to the company.

3. The company, which has not violated any regulations of laws on trading in network information security products and services, shall have its license for trading in network information security products and services renewed once with the renewal period of at most 01 year. The request for renewing the license shall be filed with the Ministry of Information and Communications at least 60 days before the expiry date of the license. The application for renewing the license shall be established in two copies, including:

a) Request for renewing the license;

b) Valid license for trading in network information security products and services;

c) Report on the company's operations in the latest 02 years.

Within 20 days as of receipt of sufficient documents, the Ministry of Information and Communications shall examine and make decision on renewal and re-grant of the license to the company; any rejection shall be noticed in writing, clearly giving out the reasons thereof.

4. A company shall be suspended from trading in network information security products and services for at most 06 months in the cases as follows:

a) Rendering a service which fails to comply with the contents of the License;

b) Failing to meet one of the conditions set forth in Article 42 hereof;

c) Other cases as stipulated by laws.

5. A company shall have its business license for trading civil cryptographic products and services withdrawing in the cases as follows:

a) It fails to render the service within 01 year as of the grant date of the License without legitimate reason;

b) The license expired;

c) It fails to remedy the reasons set forth in item 4 of this Clause when the period of suspension is over.

Article 46. Responsibilities of companies trading in network information security products and services

1. Management of documents and materials relating to technical and engineering solutions of products.

2. Making, storing and keeping secret of client information.

3. Annually reporting to the Ministry of Information and Communications on their business, importation and exportation of network information security products and services before 31 December.

4. Refusing to provide network information security products and services when detecting of the relevant organization, individual's violation of laws on use of network information security products and services, or violation of agreed undertakings on use of the product or service provided by the company.

5. Suspending or ceasing the provision of network information security products and services in order to secure national defense and security, social discipline and order upon request of competent state bodies.

6. Cooperating, giving conditions for competent state bodies to take professional measures when required.

Section 2

ADMINISTRATION OF IMPORTATION OF NETWORK INFORMATION SECURITY PRODUCTS

Article 47. Principles of administration of importation of network information security products

1. The administration of importation of network information security products shall comply with regulations of this Law, regulations of relevant laws.

2. The importation by an agency, organization, or individual who enjoys diplomatic preferences and exemptions shall be governed by laws on customs, preference and exemption applicable to representatives for diplomatic bodies, consulates and international organizations in Vietnam.

3. In cases that Vietnam has not technical norms of network information security equivalent to the imported network information security product, the international agreements and treaties to which the Socialist Republic of Vietnam is a member state shall apply.

Article 48. Network information security products subject to import permit

1. On importing a network information security product specified in the list of network information security products to be imported according to permits as specified by the Government, the importer shall obtain the permit to import network information security product that is issued by competent state bodies.

2. Organizations, companies importing network information security products shall execute the procedures of certification and announcement of norm conformity before importation under regulations of Article 39 hereof.

3. An organization, company shall be granted a permit to import network information security products should it meets all the conditions as follows:

a) It holds a business license for trading in network information security products;

b) The network information security product is certified and announced as conformable to technical norms as set forth in Article 39 hereof;

c) The subject and purpose of use of the network information security product does not damage to national defense and security, social order and safety.

4. The Ministry of Information and Communications shall provide details of the sequence, procedures and application for permits to import network information security products according to permits.

CHAPTER VI

HUMAN RESOURCE DEVELOPMENT FOR NETWORK INFORMATION SECURITY

Article 49. Training and education of network information security skills

1. Information system owners shall provide training and education of knowledge and skills for managers and technicians in network information security.

2. Officers in charge of network information security shall be provided with conditions for working appropriately with their skills, and with priority to receive training in network information security skills.

3. The state encourages organizations and individuals to invest, co-invest and join with other organizations to invest to build up university education facilities, vocational training facilities for human resource training in the field of network information security.

4. The Ministry of Home Affairs shall preside over and cooperate with the Ministry of Information and Communications and relevant ministries and sectors to make plans and organize for training in and improvement of knowledge and skills of network information security for public officers and employees.

Article 50. Certificates and diplomas of network information security training

1. Higher education institutions, vocational training entities, within their duties and powers, shall grant certificates and diplomas of network information security training.

2. The Ministry of Education and Training shall preside over and cooperate with the Ministry of Information and Communications and relevant ministries and sectors to recognize of university graduate certificates of network information security granted by foreign organizations.

3. The Ministry of Labor, War Invalids and Social Affairs shall preside over and cooperate with the Ministry of Information and Communications and relevant ministries and sectors to recognize vocational training certificates of network information security skills granted by foreign organizations.

CHAPTER VIII

STATE MANAGEMENT OF NETWORK INFORMATION SECURITY

Article 51. Contents of state management of network information security

1. Preparation of strategies, planning, plans for and policies on network information security; preparing and directing for implementation of national programs of network information security.

2. Issue and implementation of legal instruments on network information security; establishment and publication of national standards, issuance of technical norms of network information security.

3. State management of civil cryptography.

4. Managing of the assessment and announcement of conformity to network information security standards and norms;

5. Managing of information system security monitoring;

6. Appraisal of network information security in information system design file.

7. Education and dissemination of laws on network information security.

8. Managing of trading activities in network information security products and services.

9. Organization for scientific and engineering research and application of network information security; developing human resources for network information security; training officers in charge of network information security.

10. Examination, inspection and settling claims, denouncements and treatment of legal breaches in relation with network information security.

11. International cooperation on network information security.

Article 52. State management responsibilities for network information security

1. The Government shall consistently hold the state management of network information security.

2. The Ministry of Information and Communications shall be responsible before the Government for state management of network information security with the duties and powers as follows:

a) Issuing or establishing, escalating for competent authorities to issue legal instruments, strategies, planning, plans for, national standards and technical norms of network information security;

b) Appraising network information security in information system design files;

c) Managing the monitoring of information system safety nationwide, excepting the information systems set forth in points 3c and 5b of this Article;

d) Managing the assessment network information security;

đ) Granting licenses for trading in network information security products and services, permits to import information security products, except for civil cryptographic products and services;

e) Performing scientific and engineering research and application in network information security activities; training, improving knowledge and skills, developing human resources;

g) Managing and performing international cooperation on network information security;

h) Examining, inspecting and settling claims, denouncements and treating legal breaches in relation with network information security;

i) Presiding over, cooperating with relevant ministries, sectors, provincial People's Committees and companies to ensure network information security;

k) Educating, disseminating laws on network information security.

l) Annually reporting to the Government about network information security.

4. The Ministry of Defense shall have the duties and powers as follows:

a) Issuing or establish and escalating for competent authorities to issue legal instruments, strategies, planning, plans for, technical standards and norms of network information security in the field under its administration;

b) Examining, inspecting and settling claims, denouncements and treating legal breaches in activities to ensure network information security in the field under its administration;

c) Managing the safety monitoring of information systems under its administration.

3. The Government Cipher Committee shall assist the Minister of Defense for implementing state management of civil cryptography, with the duties as follows:

a) Establishing and escalating for competent state bodies to issue legal instruments on administration of civil cryptography;

b) Presiding over and cooperating with relevant ministries and sectors to establish and escalate for competent state bodies to issue national standards, technical norms applicable to civil cryptographic products and services;

c) Managing business activities and use of civil cryptography; administering the quality of civil cryptographic products and services; administering the assessment and announcement of standard and norm conformity in relation with civil cryptographic products and services;

d) Establishing and escalating for competent authorities to issue the list of civil cryptographic products and services and the list of civil cryptographic products and services to be imported or exported according to permits.

đ) Granting business licenses for trading in civil cryptographic products and services, permits to import or export civil cryptographic products;

e) Examining, inspecting and settling claims, denouncements and treating violation of laws in business activities and use of civil cryptography.

g) Performing international cooperation on civil cryptography.

5. The Ministry of Public Security shall have the duties and powers as follows:

a) Presiding over and cooperating with relevant ministries and sectors to establish and escalate for competent authorities to issue, or issuing as mandated and guiding for implementation of legal instruments in state secret protection, against cyber criminals and network use to violate national security, social order and security;

b) Managing the safety monitoring of information systems under its administration;

c) Organizing, steering, deploying actions against crimes, organizing for investigation of cyber crimes and other violations in the field of network information security;

d) Cooperating with the Ministry of Information and Communications and relevant ministries and sectors to inspect, examine and treat violations of laws on network information security as mandated.

6. The Ministry of Home Affairs shall organize for training and education of knowledge and skills in network information security for public officers and employees.

7. The Ministry Education and Training shall organize for training, disseminating knowledge of network information security in university education establishments.

8. The Ministry of Labor, War Invalids and Social Affairs shall organize for training and disseminating knowledge of network information security in the vocational training establishments.

9. The Ministry of Finance shall instruct and allocate budgets to perform network information security duties as stipulated.

10. Ministries and equivalents, within their power and duties, shall cooperate with the Ministry of Information and Communications in state management of network information security.

11. Provincial People's Committees, within their power and duties, shall perform local state management of information.

CHAPTER VIII

IMPLEMENTATION PROVISION

Article 53. Validity

This Law shall come into force as of 01 July 2016.

Article 58. Stipulation of details

The Government and competent state bodies shall stipulate details of articles and provisions as mandated under this Law.

This Law was passed by the 11th National Assembly of the Socialist Republic of Vietnam in the 10th session on 19 November 2015.

CHAIRMAN OF THE NATIONAL ASSEMBLY

Nguyen Sinh Hung

(Signed)

(Signed and sealed)