NATIONAL ASSEMBLY OF VIETNAM	SOCIALIST REPUBLIC OF VIETNAM
-------	Independence - Freedom - Happiness

No. 116/2025/QH15	*Hanoi, December 10, 2025*

LAW

CYBERSECURITY

Pursuant to the Constitution of the Socialist Republic of Vietnam, amended by Resolution No. 203/2025/QH15;

The National Assembly of Vietnam hereby promulgates the Law on Cybersecurity.

Chapter I

GENERAL PROVISIONS

Article 1. Scope and regulated entities

1. This Law provides for cybersecurity and protection thereof, as well as the rights, obligations, and responsibilities of relevant agencies, organizations, and individuals.

2. This Law applies to:

a) Vietnamese agencies, organizations, and individuals;

b) Foreign agencies, organizations, and individuals in Vietnam, and persons of Vietnamese origin whose nationality has not yet been determined and who are residing in Vietnam and have been issued identity certificates;

c) Foreign agencies, organizations, and individuals that directly participate in or are involved in cybersecurity protection activities, or in the business of cybersecurity products and services in Vietnam.

Article 2. Interpretation of terms

For the purpose of this Law, the following terms shall be construed as follows:

1. *Cybersecurity* refers to the stability, security, and safety of cyberspace, the protection of information systems, and assurance that information, data, and activities in cyberspace do not harm national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals.

2. *Cyber information security* refers to the assurance of the integrity, confidentiality, and availability of information in cyberspace, preventing unauthorized and illegal access, use, disclosure, alteration, sabotage, or other acts that threaten or harm national security, as well as social order and safety.

3. *Data security* refers to the assurance of data quality and the processing and use of data in cyberspace for socio-economic development and national digital transformation, preventing unauthorized and illegal access, use, disclosure, alteration, sabotage, or other acts that threaten or harm national security, as well as social order and safety.

4. *Cybersecurity protection* refers to the prevention, detection, and handling of acts infringing upon cybersecurity.

5. *Cyberspace* refers to an environment formed by interconnected networks of information technology infrastructure, including telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, and databases; it is a space in which humans conduct social activities without limitation by space or time.

6. *National cyberspace* refers to the portion of cyberspace under the sovereignty, jurisdiction, and control of the Socialist Republic of Vietnam.

7. *Information system* refers to a set of hardware, software, and data established for the purposes of creating, providing, transmitting, collecting, processing, storing, and exchanging information in cyberspace.

8. *Information system administrator* refers to an agency, organization, or individual with direct management authority over an information system.

9. *Malicious software* refers to software capable of causing abnormal operation of part or all of an information system, or of illegally copying, modifying, or deleting information stored in an information system.

10. *Malicious hardware* refers to physical components intentionally designed or additionally attached beyond standard hardware components for the purpose of illegally collecting information or data, or interfering with, disrupting, paralyzing, or sabotaging computer systems or information systems.

11. *System log* refers to a collection of records that reflect time, users, activities, and system status, serving system management, monitoring, and confidentiality.

12. *Cybercrime* refers to acts that are dangerous to society, as prescribed in the Criminal Code, committed by individuals or organizations in cyberspace through the use of information technology or electronic equipment.

13. *Cyberattack* refers to acts carried out in cyberspace through the use of information technology or electronic equipment to appropriate information; disrupt, interrupt, or paralyze

operations; sabotage; or control telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic equipment.

14. *Cyberterrorism* refers to acts carried out in cyberspace through the use of information technology or electronic equipment with the aim of causing public panic or political instability.

15. *Cyber espionage* refers to acts carried out in cyberspace through the covert use of information technology or electronic equipment to infiltrate, appropriate, collect, or copy information classified as state secrets, or important data of agencies, organizations, or individuals, for the purpose of harming national security, as well as social order and safety.

16. *Cybersecurity threat* refers to a state of cyberspace in which signs emerge indicating threats to national security, causing serious harm to social order and safety, or to the lawful rights and interests of agencies, organizations, or individuals.

17. *Cybersecurity incident* refers to an unexpected event occurring in cyberspace that infringes upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, or individuals.

18. *Cybersecurity emergency* refers to a state or development in cyberspace upon elements of attack, intrusion, incitement, information leakage or loss, or other acts threatening to cause serious infringement upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, or individuals.

19. *Digital account* refers to information used for authentication, verification, and authorization of the use of applications and services in cyberspace.

20. *Civil cryptography* refers to cryptographic techniques and products used to secure or authenticate information that is not classified as a state secret, and to ensure information security for agencies, organizations, and individuals.

21. *Cybersecurity products* refer to hardware and software with functions that protect cybersecurity, cyber information security, data security, information, data, information systems, and information technology infrastructure.

22. *Cybersecurity services* refer to services provided to protect cybersecurity, cyber information security, data security, information, data, information systems, and information technology infrastructure.

23. *Cipher information system* refers to an information system that uses cipher cryptography to protect information classified as state secrets, serving professional cipher operations, directly managed and operated by cipher organizations.

Article 3. State policies on cybersecurity

1. To develop a healthy cyberspace that does not harm national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals.

2. To prioritize cybersecurity protection in the fields of national defense, security, cipher, socio-economic development, science, technology, and foreign affairs.

3. To prioritize the allocation of resources for building and developing specialized cybersecurity protection forces; to ensure high-quality human resources for cybersecurity protection; to enhance capacity for cybersecurity protection forces and for agencies, organizations, and individuals participating in cybersecurity protection; to prioritize investment in research and development of modern science and technology serving cybersecurity protection; and to adopt special mechanisms and incentive policies to mobilize, attract, train, and employ talents in the field of cybersecurity.

4. To promote linkages and investment in cybersecurity protection through public-private partnership modalities; to encourage and facilitate agencies, organizations, and individuals to participate in cybersecurity protection and in addressing cybersecurity threats; to research and develop technologies, products, services, and applications for cybersecurity protection; and to use cybersecurity products and services of Vietnam.

5. To expand international cybersecurity cooperation to enhance cybersecurity protection capacity; to prevent and combat cybercrime and transnational cybersecurity threats; and to acquire advanced technologies to enhance national cybersecurity self-reliance.

Article 4. Principles of cybersecurity protection

1. To comply with the Constitution and the law, and to ensure national security, sovereignty, and national interests in cyberspace.

2. To place cybersecurity protection under the leadership of the Communist Party of Vietnam (CPV) and the consistent management of the State; to mobilize the combined strength of the political system and the entire nation; and to promote the core role of specialized cybersecurity protection forces.

3. To closely combine cybersecurity protection with socio-economic development; to ensure human rights and citizens' rights; to protect personal data; and to facilitate agencies, organizations, and individuals to conduct lawful activities in cyberspace.

4. To apply measures to protect national cyberspace; to proactively prevent, detect, block, combat, and defeat all activities in cyberspace that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals; and to promptly and strictly handle violations of cybersecurity law.

5. To carry out cybersecurity protection activities on a regular and continuous basis for the national cyberspace infrastructure, and to proactively apply measures to protect national security information systems.

Article 5. Cybersecurity protection measures

1. Cybersecurity protection measures include:

a) Cybersecurity appraisal;

b) Assessment of cybersecurity conditions;

c) Cybersecurity inspection;

d) Cybersecurity supervision;

dd) Response to and remediation of cybersecurity incidents;

e) Cybersecurity protection operations;

g) Use of cryptography to protect network information;

h) Use of technical solutions to protect cyber information security, data security, and information systems; and to prevent information that violates the law;

i) Prevention and request for suspension or cessation of the provision of network information; termination or suspension of activities relating to the establishment, provision, and use of telecommunications networks and the Internet, as well as the manufacture and use of radio transmitting and receiving devices in accordance with law;

k) Request for removal or enforced removal of illegal information or false information and fake news in cyberspace that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals;

l) Collection of electronic data related to activities infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace;

m) Blocking or restriction of the operation of information systems; termination, suspension, or requests for cessation of operation of information systems; and revocation of domain names in accordance with the law;

n) Initiation of criminal proceedings, investigation, prosecution, and adjudication in accordance with the Criminal Procedure Code;

o) Other measures in accordance with the law on national security and the law on handling of administrative violations.

2. The Government of Vietnam shall elaborate on the contents, procedures, and authority to apply cybersecurity protection measures, except for the measures prescribed in Points n and o Clause 1 of this Article.

Article 6. International cybersecurity cooperation

1. International cybersecurity cooperation shall be conducted based on respect for independence, sovereignty, and territorial integrity; non-interference in each other's internal affairs; equality and mutual benefit; and in compliance with the Constitution and laws of Vietnam, and with international treaties to which the Socialist Republic of Vietnam is a signatory.

2. The contents of international cybersecurity cooperation include:

a) Sharing of information, data, and early warnings on cybersecurity threats, cybersecurity incidents, and cyberattacks affecting cybersecurity;

b) Development of legal frameworks, policies, and cooperation and coordination mechanisms for cybersecurity protection; negotiation, conclusion, and participation in the implementation of international treaties and international agreements on cybersecurity;

c) Training, consultancy, sharing of experience, and enhancement of professional and technical capacity in the field of cybersecurity;

d) Prevention and combat against cybercrime and crimes using high technology; cooperation in the investigation and handling of violations of law, cybercrime, and crimes using high technology;

dd) Research, development, and transfer of technologies, products, and technical solutions serving cybersecurity protection;

e) Organization of international conferences and seminars, and implementation of international cooperation programs and projects on cybersecurity;

g) Other international cooperation activities concerning cybersecurity.

3. Responsibilities for international cooperation in cybersecurity are prescribed as follows:

a) The Ministry of Public Security of Vietnam shall assume responsibility before the Government of Vietnam for taking charge of and cooperating in the implementation of international cybersecurity cooperation;

b) The Ministry of National Defense of Vietnam shall assume responsibility before the Government of Vietnam for implementing international cybersecurity cooperation within its management scope;

c) The Ministry of Foreign Affairs of Vietnam shall cooperate with the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam in international cooperation activities concerning cybersecurity;

d) Where international cybersecurity cooperation involves the responsibilities of multiple ministries or central authorities, the Prime Minister of Vietnam shall make the decision;

dd) International cooperation activities concerning cybersecurity conducted by other ministries, central authorities, or local authorities shall require written opinions of the Ministry of Public Security of Vietnam before implementation.

Article 7. Prohibited acts in cybersecurity

1. Posting or disseminating information with the following contents in cyberspace:

a) Propaganda against the State of the Socialist Republic of Vietnam, including: distorting and defaming the people's authority; inciting psychological warfare; provoking wars of aggression; sowing division and hatred among ethnic groups, religions, and peoples of countries; and insulting the nation, national flag, national emblem, national anthem, great figures, leaders, eminent persons, or national heroes;

b) Distortion of history; denial of revolutionary achievements; sabotage of the great national unity bloc; religion insult; gender discrimination; and racial discrimination;

c) Fabrication, slander, false information, infringement upon the dignity, honor, or reputation of others, or causing damage to the lawful rights and interests of other agencies, organizations, or individuals;

d) False information causing public panic; causing damage to socio-economic activities; obstructing the normal operation of state agencies or persons performing official duties; infringing upon the lawful rights and interests of other agencies, organizations, or individuals; fabricated or false information about products, goods, money, bonds, bills, government bonds, checks, and other security instruments; fabricated or false information in the fields of finance, banking, e-commerce, multi-level marketing business, and securities.

2. Committing the following acts in cyberspace:

a) Organizing, operating, colluding, inciting, bribing, deceiving, enticing, or training persons to oppose the State of the Socialist Republic of Vietnam;

b) Provoking, calling for, mobilizing, inciting, threatening, causing division, or conducting armed activities or using violence to oppose the people's authority; calling for, mobilizing, inciting, threatening, or enticing mass gatherings to cause disorder, oppose persons performing official duties, or obstruct the operations of agencies or organizations, thereby causing instability in security and order;

c) Appropriating, trading, seizing, or deliberately disclosing information classified as state secrets, work secrets, or business secrets; appropriating, trading, seizing, or deliberately disclosing personal secrets, family secrets, or private life information, thereby affecting the honor, reputation, dignity, or lawful rights and interests of agencies, organizations, or individuals; deliberately eavesdropping on, illegally recording audio or video of conversations in cyberspace; disclosing information on civil cryptography products or information on clients lawfully using civil cryptography products; using or trading civil cryptography products of unknown origin;

d) Engaging in prostitution-related activities, social evils, human trafficking, or human body part trading; disseminating obscene or depraved cultural products; provoking or promoting violence or depraved and deviant lifestyles; sabotaging national customs and traditions, social morality, or community health;

dd) Engaging in fraudulent appropriation of property; organizing gambling or gambling via the Internet; engaging in theft of international telecommunications charges on the Internet platform; disseminating, advertising, or trading goods and services prohibited by law; infringing on copyright and intellectual property rights in cyberspace;

e) Impersonating websites of agencies, organizations, or individuals; forging, circulating, stealing, trading, illegally collecting or exchanging credit card information, bank accounts, crypto assets, or digital assets of others; illegally issuing, providing, or using means of payment; forging documents of agencies or organizations;

g) Using artificial intelligence or new technologies to illegally impersonate another person's video, images, or voice; creating, posting, or disseminating information prescribed in Clause 1 of this Article;

h) Illegally collecting, using, disseminating, exchanging, transferring, or trading personal information or data of others;

i) Instructing, inciting, enticing, or provoking others to commit crimes or violations of law;

k) Committing other acts in cyberspace through the use of information technology or electronic equipment to violate national security, social order, and safety laws.

3. Carrying out cyberattacks, cyberterrorism, cyber espionage, cybercrime, or crimes using high technology; causing cybersecurity incidents; attacking, infiltrating, seizing control of, falsifying, disrupting, suspending, paralyzing, or sabotaging information systems.

4. Manufacturing or putting into use tools, equipment, or software, or committing acts that obstruct, disrupt, or disseminate spam emails, spam messages, spam calls, or harmful software that damage the operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, or electronic equipment.

5. Illegally infiltrating telecommunications networks, computer networks, information systems, information processing and control systems, databases, or electronic equipment of others.

6. Opposing or obstructing the operations of cybersecurity protection forces; illegally attacking or neutralizing cybersecurity protection measures.

7. Exploiting or abusing cybersecurity protection activities to infringe upon sovereignty, interests, national security, social order and safety, or the lawful rights and interests of agencies, organizations, or individuals, or to obtain illicit gains.

8. Committing other acts in violation of this Law.

Chapter II

CYBERSECURITY PROTECTION FOR INFORMATION SYSTEMS

Article 8. Classification of information system levels

1. Information systems shall be classified into 5 levels based on the extent of damage to national security, social order and safety, the lawful rights and interests of organizations and individuals, and public interests in the event of cybersecurity incidents or acts in violation of cybersecurity law, as follows:

a) Level 1, which may cause damage to the lawful rights and interests of organizations or individuals;

b) Level 2, which may cause serious damage to the lawful rights and interests of organizations or individuals, or cause damage to public interests;

c) Level 3, which may cause particularly serious damage to the lawful rights and interests of organizations or individuals; serious damage to public interests; damage or serious damage to social order and safety; or damage to national security;

d) Level 4, which may cause particularly serious damage to public interests or to social order and safety, or serious damage to national security;

dd) Level 5, which may cause particularly serious damage to national security.

2. The Government of Vietnam shall elaborate on the criteria for determining information system levels, and prescribe the authority and procedures for determining the level of information systems, as well as the measures, responsibilities, and obligations for ensuring cybersecurity corresponding to each information system level.

Article 9. National security information systems

1. National security information systems refer to information systems that play a strategic and particularly important role in politics, national defense, security, diplomacy, economy, and social activities, where cybersecurity incidents or violations of cybersecurity law may cause damage to national security or serious harm to social order and safety, and which fall within the list decided by the Prime Minister of Vietnam.

2. National security information systems include information systems in the following fields:

a) Military, security, diplomatic, and cipher information systems;

b) Information systems for storing and processing information classified as state secrets;

c) Information systems serving the storage and preservation of artifacts and documents of particularly important value;

d) Information systems serving the preservation of materials and substances that are particularly dangerous to humans and the environment;

dd) Information systems serving the preservation, fabrication, and management of other particularly important physical facilities related to national security;

e) Important information systems serving the operations of central agencies and organizations;

g) National information systems in the fields of energy, finance, banking, telecommunications, transport, agriculture, natural resources and environment, chemical, health, and culture;

h) Automatic control and supervision systems at important works related to national security and important national security objectives.

3. National security information systems shall be subject to cybersecurity appraisal and certification of eligibility for cybersecurity before being put into operation and use; shall undergo regular cybersecurity inspection and cybersecurity supervision during use; and shall promptly respond to and remedy cybersecurity incidents.

4. The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries, central authorities, agencies, organizations, and individuals in preparing and submitting to the Prime Minister of Vietnam for consideration and decision the list of national security information systems.

5. The Government of Vietnam shall elaborate on the criteria for identifying national security information systems.

Article 10. Tasks and measures for cybersecurity protection of information systems

1. Tasks for cybersecurity protection of information systems include:

a) Determining the cybersecurity level of information systems and national security information systems;

b) Assessing and managing cybersecurity risks of information systems;

c) Urging, supervising, and inspecting cybersecurity protection activities for information systems;

d) Organizing the implementation of cybersecurity protection measures for information systems;

dd) Implementing prescribed reporting regulations;

e) Organizing dissemination and raising awareness of cybersecurity.

2. Measures for cybersecurity protection of information systems include:

a) Promulgating regulations on the assurance of cybersecurity in the design, construction, management, operation, use, upgrading, and decommissioning of information systems;

b) Conducting cybersecurity appraisal of dossiers and designs of information systems;

c) Assessing cybersecurity conditions for information systems;

d) Applying management measures in accordance with standards and technical regulations on cybersecurity; researching and developing a national firewall system to prevent cybersecurity threats and remedy cybersecurity incidents;

dd) Organizing the implementation of storage and backup measures to protect cyber information security and the security of constituent components of information systems;

e) Inspecting and supervising compliance with regulations and assessing the effectiveness of applied management and technical measures;

g) Conducting cybersecurity supervision;

h) Responding to and remedying cybersecurity incidents affecting information systems.

3. Information system administrators of level-1 and level-2 information systems shall fully perform the tasks specified in Clause 1 of this Article and, based on actual needs and capacity, select and apply the measures specified in Clause 2 of this Article.

4. Information system administrators of level-3 and level-4 information systems not included in the list of national security information systems shall fully perform the tasks specified in Clause 1 of this Article; shall implement the measures specified in Points a, d, dd, e, g, and h of Clause 2 of this Article; and, based on actual needs and capacity, may select and apply the measures specified in Points b and c of Clause 2 of this Article.

5. Information system administrators of information systems included in the list of national security information systems shall fully perform all tasks and measures specified in Clauses 1 and 2 of this Article.

6. The Government of Vietnam shall elaborate on Clauses 1 and 2 of this Article.

Article 11. Responsibilities for cybersecurity protection of national security information systems

1. Information system administrators of national security information systems shall have the following responsibilities:

a) Implement Clause 5 Article 10 of this Law;

b) When establishing, expanding, or upgrading national security information systems, conduct cybersecurity inspections before putting them into operation and utilization; conduct annual self-inspection of cybersecurity, assess cybersecurity conditions of national security information systems, and notify the inspection results in writing to the competent specialized cybersecurity protection forces before October each year;

c) Take charge and cooperate with the competent specialized cybersecurity protection forces in regularly conducting cybersecurity supervision; establishing self-warning mechanisms and receiving warnings of cybersecurity threats; proposing emergency response and remediation plans;

d) Develop plans for responding to and remedying cybersecurity incidents; implement response and remediation plans when cybersecurity incidents occur and promptly submit reports to the competent specialized cybersecurity protection forces;

dd) Cooperate with specialized cybersecurity protection forces in conducting ad hoc cybersecurity inspections.

2. The Ministry of Public Security of Vietnam shall have the following responsibilities for national security information systems, except for military information systems and cipher information systems under the Government Cipher Committee, in accordance with the law:

a) Conduct cybersecurity appraisal of national security information systems;

b) Assess and certify eligibility for cybersecurity of national security information systems;

c) Conduct ad hoc cybersecurity inspections of national security information systems;

d) Conduct cybersecurity supervision; issue warnings and cooperate with information system administrators in remedying and handling cybersecurity threats and cybersecurity incidents affecting national security information systems;

dd) Coordinate response and remediation activities for cybersecurity incidents occurring in national security information systems; notify information system administrators upon detecting cyberattacks or cybersecurity incidents;

e) Take charge and cooperate with the Government Cipher Committee in implementing measures to protect national security information systems that use cryptographic solutions and products provided by the Government Cipher Committee to protect state secrets.

3. The Ministry of National Defense of Vietnam shall conduct cybersecurity assessments, assess cybersecurity conditions, conduct ad hoc cybersecurity inspections, conduct cybersecurity supervision, and coordinate response and remediation activities for cybersecurity incidents affecting military information systems under its management.

4. The Government Cipher Committee shall organize the implementation of solutions using cipher cryptography to protect state secret information in national security information systems; conduct cybersecurity assessments, assess cybersecurity conditions, conduct ad hoc cybersecurity inspections, conduct cybersecurity supervision, and coordinate response and remediation activities for cybersecurity incidents affecting cipher information systems under the Government Cipher Committee.

Article 12. Cybersecurity inspection of information systems of agencies and organizations not included in list of national security information systems

1. Cybersecurity inspection of information systems of agencies and organizations not included in the list of national security information systems shall be conducted in the following cases:

a) Where there are acts specified in Clauses 12, 13, 14, and 15 of Article 2 of this Law;

b) Upon the request of the information system administrator.

2. Subjects of cybersecurity inspection include:

a) Hardware, software, and digital devices used in the information system;

b) Information stored, processed, and transmitted within the information system;

c) Measures to protect state secrets and prevent the disclosure or loss of state secrets through technical channels.

3. The information system administrator shall notify the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam upon detecting acts in violation of cybersecurity laws on information systems under its management.

4. The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall conduct cybersecurity inspections of information systems of agencies and

organizations in the cases specified in Clause 1 of this Article. The results of cybersecurity inspections shall be kept confidential in accordance with the law.

5. The Government of Vietnam shall stipulate the procedures for cybersecurity inspection as prescribed in this Article.

Chapter III

PREVENTION AND HANDLING OF ACTS INFRINGING ON CYBERSECURITY

Article 13. Information and acts using information technology and electronic equipment infringing on national security, social order and safety in cyberspace

1. Information containing content propagandizing against the State of the Socialist Republic of Vietnam, provoking riots, undermining security, or disturbing public order includes:

a) Propagandizing information and materials that distort, smear, or defame the people's authority;

b) Conducting psychological warfare; provoking wars of aggression; sowing division and hatred among ethnic groups, religions, and peoples of different countries;

c) Insulting the nation, the national flag, national emblem, national anthem, great figures, leaders, eminent persons, or national heroes;

d) Calling for, mobilizing, inciting, threatening, or causing division; carrying out armed activities or using violence to oppose the people's authority;

dd) Calling for, mobilizing, inciting, threatening, or enticing mass gatherings to cause disorder, oppose persons performing official duties, or obstruct the normal operations of agencies and organizations, thereby causing instability in security and order;

e) Providing distorted or inaccurate information regarding national borders or the national sovereignty of Vietnam; posting or transmitting distorted, inaccurate, or incomplete images of maps of Vietnam, or misrepresenting the national sovereignty of Vietnam.

2. Information containing content sabotaging solidarity policies and socio-economic policies of the Socialist Republic of Vietnam includes:

a) Causing conflicts or divisions among social strata; between the people and the people's authority; or between the people and the people's armed forces or socio-political organizations;

b) Provoking hatred, discrimination, division, or ethnic separatism; infringing upon the right to equality within the community of ethnic groups in Vietnam;

c) Provoking conflicts or divisions between religious believers and non-believers, among followers of different religions, or between religious followers and the people's authority, the people's armed forces, or socio-political organizations;

d) Sabotaging or obstructing the implementation of international solidarity policies;

dd) Propagandizing content causing direct or indirect harm to the State's lawful rights and interests in political, economic, or social fields, or to its international reputation;

e) Calling for or provoking acts to sabotage the implementation of socio-economic policies or to obstruct policy enforcement;

g) Calling for or provoking sabotage of the physical and technical facilities of the Socialist Republic of Vietnam.

3. Information containing content infringing on the lawful rights and interests of organizations and individuals includes:

a) Spreading distorted, fabricated, or false information affecting the reputation or normal operations of organizations;

b) Calling for, mobilizing, or inciting boycotts of products, services, goods, brands, or trademarks of organizations or enterprises, causing physical damage or reputational harm to such organizations or enterprises;

c) Impersonating or forging information or images; counterfeiting products, goods labels, or brands of organizations or enterprises by using technological utilities, thereby affecting their reputation;

d) Insulting the honor, reputation, or dignity of others;

dd) Distorting facts, thereby affecting the honor, reputation, or dignity of others;

e) Fabricating or disseminating information known to be false, causing harm to the lawful rights and interests of others;

g) Fabricating accusations that others have committed crimes and reporting them to competent authorities;

h) Impersonating or forging information, images, or voices of individuals, thereby affecting their reputation, honor, or dignity.

4. Acts committed in cyberspace by using information technology and electronic equipment that infringe on national security and social order and safety include:

a) Posting or disseminating information in cyberspace containing content specified in Clauses 1, 2, and 3 of this Article;

b) Committing acts specified in Clause 1 of Article 15 of this Law;

c) Appropriating property; organizing gambling or gambling via the Internet; stealing international telecommunications charges via the Internet; infringing on copyright and intellectual property rights in cyberspace;

d) Impersonating websites of agencies, organizations, or individuals; forging, circulating, stealing, trading, or illegally collecting and exchanging other persons' credit card information or bank accounts; illegally issuing, providing, or using means of payment; forging seals, documents, or other papers of agencies or organizations;

dd) Disseminating, advertising, or illegally trading weapons, explosives, combat gear, or fireworks; narcotics, narcotic precursors, additive substances, or psychotropic substances; endangered, precious, and rare wildlife and other goods and services on the prohibited list in accordance with the law; brokering prostitution; disseminating pornographic materials; sexually abusing children; committing sexual harassment;

e) Establishing, providing services for, or supporting the operation, business, transactions, trading, or online marketing for illegal trading floors, websites, or applications in cyberspace, including e-commerce platforms, websites, applications for selling goods or providing e-commerce services; commodity index-based trading floors; digital asset trading floors; or multilevel marketing activities;

g) Using false identities or forged documents or dossiers, or illegally using other persons' information to establish enterprises or to set up or register bank accounts, securities accounts, insurance accounts, tax accounts, or other digital accounts; illegally collecting, storing, exchanging, trading, gifting, or disclosing data or information relating to bank accounts, bank cards, e-wallet accounts, securities accounts, insurance accounts, tax accounts, and other types of digital accounts;

h) Advertising or trading counterfeit goods, smuggled goods, goods of unclear origin, goods circulating domestically subject to emergency measures, or expired goods;

i) Instructing others to commit acts in violation of the law;

k) Committing other acts in cyberspace through the use of information technology or electronic equipment that violate national security, social order, and safety laws.

Article 14. Prevention and processing/handling of information and acts using information technology and electronic equipment that infringe on national security and social order and safety in cyberspace

1. Information system administrators, and domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace shall implement management and technical measures to prevent, detect, block, and remove information containing the content specified in Clauses 1, 2, and 3 of Article 13 of this Law on information systems under their management or upon request of the specialized cybersecurity protection forces.

2. The specialized cybersecurity protection forces and competent authorities shall apply the measures specified in Clause 1 of Article 5 of this Law to process information in cyberspace containing the content specified in Clauses 1, 2, and 3 of Article 13 of this Law, and to combat and prevent acts of using information technology and electronic equipment that infringe on national security and social order and safety in cyberspace.

3. Domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace, and information system administrators shall cooperate with the specialized cybersecurity protection forces in processing information in cyberspace containing the content specified in Clauses 1, 2, and 3 of Article 13 of this Law, and in preventing and combating acts of using information technology and electronic equipment that infringe on national security and social order and safety in cyberspace.

4. Organizations and individuals that draft, post, or disseminate information in cyberspace containing the content specified in Clauses 1, 2, and 3 of Article 13 of this Law shall remove such information upon request of the specialized cybersecurity protection forces and bear responsibility in accordance with the law.

5. The Government of Vietnam shall elaborate on this Article.

Article 5. Prevention and combat against cyber espionage; protection of information classified as state secrets, work secrets, business secrets, personal secrets, family secrets, and private life in cyberspace

1. Acts of cyber espionage; infringement on state secrets, work secrets, business secrets, personal secrets, family secrets, and private life in cyberspace include:

a) Appropriating, trading, seizing, or deliberately disclosing information classified as state secrets, work secrets, or business secrets; appropriating, trading, seizing, or deliberately disclosing personal secrets, family secrets, and private life, thereby affecting the honor, reputation, dignity, and lawful rights and interests of agencies, organizations, or individuals;

b) Deliberately deleting, damaging, losing, or altering information classified as state secrets, work secrets, business secrets, personal secrets, family secrets, or private life that is transmitted or stored in cyberspace;

c) Deliberately altering, abolishing, or disabling technical measures that are established and applied to protect information classified as state secrets, work secrets, business secrets, personal secrets, family secrets, or private life;

d) Uploading to cyberspace information classified as state secrets, work secrets, business secrets, personal secrets, family secrets, or private life in violation of the law;

dd) Deliberately eavesdropping on, audio-recording, or video-recording conversations illegally;

e) Other acts that deliberately infringe on state secrets, work secrets, business secrets, personal secrets, family secrets, or private life.

2. Information system administrators shall have the following responsibilities:

a) Conduct cybersecurity inspections to detect and remove malicious software and malicious hardware, remedy weaknesses and security vulnerabilities; detect, prevent, and handle illegal infiltration activities or other risks threatening cybersecurity;

b) Implement management and technical measures to prevent, detect, and block acts of cyber espionage and acts infringing on state secrets, work secrets, business secrets, personal secrets, family secrets, and private life on information systems, and promptly remove information related to such acts;

c) Cooperate with and comply with requests of the specialized cybersecurity protection forces regarding the prevention and combat against cyber espionage and protection of information classified as state secrets, work secrets, business secrets, personal secrets, family secrets, and private life on information systems.

3. Agencies and organizations that draft and store information and documents classified as state secrets shall be responsible for protecting state secrets that are drafted, stored on computers or other devices, or exchanged in cyberspace in accordance with the law on protection of state secrets.

4. The Ministry of Public Security of Vietnam shall have the following responsibilities, except for the cases specified in Clauses 5 and 6 of this Article:

a) Conduct cybersecurity inspections of national security information systems to detect and remove malicious software and malicious hardware, remedy weaknesses and security vulnerabilities; detect, prevent, and handle illegal infiltration activities;

b) Conduct cybersecurity inspections of devices, products, communication information services, digital devices, and electronic devices before they are put into use in national security information systems;

c) Conduct cybersecurity supervision of national security information systems to detect and handle illegal collection of information classified as state secrets;

d) Detect and handle acts of illegally posting, storing, or exchanging information and documents containing state secrets in cyberspace;

dd) Participate in the research and production of products for storing and transmitting information and documents containing state secrets in accordance with the law, and products for encrypting information in cyberspace in line with assigned functions and tasks;

e) Conduct inspections and examinations of the protection of state secrets in cyberspace by state agencies and of cybersecurity protection by administrators of national security information systems;

g) Organize training sessions and drills to raise awareness and knowledge of the protection of state secrets in cyberspace, prevention of cyberattacks, and protection of cybersecurity for cybersecurity protection forces as specified in Clause 1 of Article 30 of this Law.

5. The Ministry of National Defense of Vietnam shall implement the contents specified in Clause 4 of this Article for military information systems.

6. The Government Cipher Committee shall implement the contents specified in Clause 4 of this Article for cipher information systems under the Government Cipher Committee, and organize the implementation of specific laws regarding the use of cryptography to protect information classified as state secrets that is stored or exchanged in cyberspace.

Article 16. Prevention and combat against child abuse in cyberspace

1. Children shall have the right to access information, participate in social activities, engage in recreation and entertainment, have their personal secrets and private life protected, and enjoy other rights in cyberspace in accordance with the law.

2. Where children use value-added services in cyberspace, their parents or legal guardians, in accordance with civil law, shall register accounts using the parents' or guardians' information and shall be responsible for supervising and managing the content that children access, post, and share on such service platforms.

3. Information system administrators and enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace shall have the following responsibilities:

a) Control information content on information systems or services provided by the enterprise so as not to cause harm to children, abuse children, or infringe on children's rights;

b) Prevent the sharing of and remove information containing content that harms or abuses children or infringes on children's rights;

c) Develop and implement technical systems to support the prevention of content on child abuse in cyberspace;

d) Cooperate with agencies, organizations, and enterprises in preventing sources that disseminate information on child abuse in cyberspace;

dd) Promptly notify and cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam in handling.

4. Agencies, organizations, and individuals participating in activities in cyberspace shall cooperate with competent authorities in ensuring children's rights in cyberspace and preventing and combating child abuse in cyberspace.

5. Agencies, organizations, parents, guardians, teachers, child caregivers, and other relevant individuals shall ensure children's rights and protect them when participating in activities in cyberspace in accordance with the law on children and this Law.

6. The specialized cybersecurity protection forces and competent authorities shall apply measures to prevent, detect, block, and strictly handle acts of using cyberspace to cause harm to children, abuse children, or infringe on children's rights.

Article 17. Prevention, detection, blocking, and handling of malicious software

1. Agencies, organizations, and individuals shall proactively prevent, detect, and block malicious software and comply with the guidelines and requirements of competent state authorities.

2. Administrators of national security information systems shall implement technical systems to prevent, detect, block, and promptly handle malicious software.

3. Organizations and enterprises that provide email, information transmission, and information storage services shall have malicious software filtering systems in place during the process of sending, receiving, and storing information on their systems, and submit reports to competent state authorities in accordance with the law.

4. Internet service providers shall implement management measures to prevent, detect, and block the dissemination of malicious software and shall handle such matters in accordance with requests of competent state authorities.

5. The Ministry of Public Security of Vietnam shall take charge and cooperate with the Ministry of National Defense of Vietnam and relevant ministries and central authorities in organizing the prevention, detection, blocking, and handling of malicious software harming national security.

Article 18. Prevention and combat against cyberattacks

1. Cyberattacks and acts related to cyberattacks include:

a) Disseminating malicious computer programs that harm telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic equipment;

b) Obstructing, disrupting, paralyzing, interrupting, suspending operations, or illegally blocking the transmission of data in cyberspace;

c) Infiltrating, damaging, or appropriating data stored or transmitted via telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic equipment;

d) Infiltrating, creating, or exploiting weaknesses, security vulnerabilities, and system services to appropriate information or obtain illicit gains;

dd) Producing, trading, exchanging, or gifting tools, devices, or software with functions that harm telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic equipment for illegal purposes;

e) Other acts that adversely affect the normal operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic equipment.

2. Information system administrators shall apply technical measures to prevent and block the acts specified in Points a, b, c, d, and e Clause 1 of this Article to information systems under their management.

3. When a cyberattack infringes on or threatens to infringe on sovereignty, interests, or national security, or causes serious harm to social order and safety, the specialized cybersecurity protection forces shall take charge and cooperate with information system administrators and relevant organizations and individuals, in applying measures to identify the origin of the cyberattack and collect evidence; request enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace to filter and block information to prevent and eliminate cyberattacks, and to fully and promptly provide relevant information and documents.

4. Responsibilities for the prevention and combat against cyberattacks are prescribed as follows:

a) The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries, central authorities, and local authorities in preventing, detecting, and handling the acts specified in Clause 1 of this Article that infringe on or threaten to infringe on sovereignty, interests, or national security, or cause serious harm to social order and safety nationwide, except for the cases specified in Points b and c of this Clause;

b) The Ministry of National Defense of Vietnam shall take charge and cooperate with relevant ministries and central authorities in preventing, detecting, and handling the acts specified in Clause 1 of this Article for military information systems;

c) The Government Cipher Committee shall take charge and cooperate with relevant ministries and central authorities in preventing, detecting, and handling the acts specified in Clause 1 of this Article for cipher information systems under the Government Cipher Committee.

Article 19. Prevention and combat against cyberterrorism

1. Competent state authorities shall apply measures in accordance with this Law and the law on the prevention and combat against terrorism to handle cyberterrorism.

2. Information system administrators shall regularly review and inspect the information systems under their management to eliminate cybersecurity threats related to cyberterrorism.

3. Upon detecting signs or acts of cyberterrorism, agencies, organizations, and individuals shall promptly report them to the cybersecurity protection forces. Receiving agencies shall be responsible for fully receiving reports on cyberterrorism and promptly notifying the specialized cybersecurity protection forces.

4. The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries and central authorities in implementing the prevention and combat against cyberterrorism, applying measures to neutralize sources of cyberterrorism, handling cyberterrorism, and minimizing consequences for information systems to the lowest possible extent, except for the cases specified in Clauses 5 and 6 of this Article.

5. The Ministry of National Defense of Vietnam shall take charge and cooperate with relevant ministries and central authorities in implementing the prevention and combat against cyberterrorism, applying measures to neutralize sources of cyberterrorism, handling cyberterrorism, and minimizing consequences for military information systems to the lowest possible extent.

6. The Government Cipher Committee shall take charge and cooperate with relevant ministries and central authorities in implementing the prevention and combat against cyberterrorism, applying measures to neutralize sources of cyberterrorism, handling cyberterrorism, and minimizing consequences for cipher information systems under the Government Cipher Committee to the lowest possible extent.

Article 20. Prevention and handling of cybersecurity emergencies

1. Cybersecurity emergencies include:

a) The emergence of provoking information in cyberspace that poses a risk of riots, security disruption, or terrorism;

b) Attacks against national security information systems;

c) Large-scale, high-intensity attacks against multiple information systems;

d) Cyberattacks aimed at destroying works of critical importance to national security

dd) Cyberattacks that seriously infringe on sovereignty, interests, or national security, or cause exceptionally serious harm to social order and safety, and to the lawful rights and interests of agencies, organizations, and individuals.

2. Responsibilities for the prevention of cybersecurity emergencies are prescribed as follows:

a) Specialized cybersecurity protection forces shall cooperate with administrators of national security information systems in implementing technical and professional solutions to prevent, detect, and handle cybersecurity emergencies;

b) Telecommunications, Internet, and information technology enterprises, enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace, and relevant agencies, organizations, and individuals shall cooperate with the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam in the prevention, detection, and handling of cybersecurity emergencies.

3. Measures to handle cybersecurity emergencies include:

a) Immediately implementing cybersecurity emergency prevention and response plans to prevent, eliminate, or mitigate damage caused by cybersecurity emergencies;

b) Notifying relevant agencies, organizations, and individuals;

c) Collecting relevant information; continuously monitoring and supervising cybersecurity emergencies;

d) Analyzing and assessing information; forecasting the possibility, scope of impact, and extent of damage caused by cybersecurity emergencies;

dd) Suspending the provision of network information services in specific areas or disconnecting international network gateways;

e) Arranging forces and equipment to prevent and eliminate cybersecurity emergencies;

g) Other measures in accordance with the Law on National Security.

4. The handling of cybersecurity emergencies is prescribed as follows:

a) Upon detecting a cybersecurity emergency, agencies, organizations, and individuals shall promptly notify the specialized cybersecurity protection forces and immediately apply the measures specified in Points a and b Clause 3 of this Article;

b) The Prime Minister of Vietnam shall consider, decide, or authorize the Minister of Public Security of Vietnam to consider, decide, and handle cybersecurity emergencies nationwide, within specific provinces, or with respect to a specific objective.

The Prime Minister of Vietnam shall consider, decide, or authorize the Minister of National Defense of Vietnam to consider, decide, and handle cybersecurity emergencies with respect to military information systems and cipher information systems under the Government Cipher Committee;

c) The specialized cybersecurity protection forces shall take charge and cooperate with relevant agencies, organizations, and individuals in applying the measures specified in Clause 3 of this Article to handle cybersecurity emergencies;

d) Relevant agencies, organizations, and individuals shall cooperate with the specialized cybersecurity protection forces in implementing measures to prevent and handle cybersecurity emergencies.

Article 21. Cybersecurity protection operations

1. Cybersecurity protection operations refer to organized activities carried out by specialized cybersecurity protection forces in cyberspace to protect national security and ensure social order and safety.

2. Cybersecurity protection operations include the following contents:

a) Supervising online information and preventing, combating, and handling organizations and individuals that use cyberspace to infringe on national security and social order and safety;

b) Applying technical solutions to block information in violation of the law;

c) Preventing cyberattacks and protecting the stable operation of national security information systems;

d) Paralyzing or restricting the use of cyberspace for activities that harm national security or cause exceptionally serious damage to social order and safety;

dd) Proactively conducting offensive operations to neutralize targets in cyberspace to protect national security and ensure social order and safety.

3. The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries and central authorities in conducting cybersecurity protection operations; the Ministry of National Defense of Vietnam shall take charge and cooperate with relevant ministries and central authorities in conducting cybersecurity protection operations with respect to military information systems.

Article 22. Prevention of information conflicts in cyberspace

1. Information conflict refers to the use by two or more domestic or foreign organizations of technological and information-technical measures that cause damage to information or information systems in cyberspace, thereby affecting national security and social order and safety.

2. Prevention of information conflicts in cyberspace refers to the implementation of technological and technical measures to supervise, detect, warn, identify sources, block and

filter, remove, counter, guide public opinion, remedy consequences, impose penalties, and apply other measures to eliminate information conflicts in cyberspace.

3. Within the scope of their functions and entitlements, organizations and individuals shall have the following responsibilities:

a) Prevent information conflicts in cyberspace originating from their own information systems; cooperate in identifying sources, repelling attacks, and remedying consequences of cyberattacks carried out through the information systems of domestic and foreign organizations and individuals;

b) Prevent activities of domestic and foreign organizations and individuals aimed at creating information conflicts in cyberspace;

c) Eliminate the organization or execution of the posting or dissemination of information in cyberspace that seriously affects national defense, national security, and social order and safety by domestic and foreign organizations and individuals.

4. The Government of Vietnam shall elaborate on this Article.

Chapter IV

CYBERSECURITY PROTECTION ACTIVITIES

Article 23. Implementation of cybersecurity protection activities in state agencies, political organizations, and socio-political organizations at central and local levels

1. The contents of the implementation of cybersecurity protection activities include:

a) Developing and improving regulations on the use of internal computer networks and computer networks connected to the Internet; plans for ensuring cybersecurity for information systems; and plans for responding to and remedying cybersecurity incidents;

b) Applying and implementing plans, measures, and technologies for cybersecurity protection for information systems and for information and documents that are stored, drafted, and transmitted on information systems within the scope of management;

c) Organizing training and advanced training courses on cybersecurity knowledge for cadres, civil servants, public employees, and employees; enhancing cybersecurity protection capacity for cybersecurity protection forces;

d) Ensuring cybersecurity in the provision of public services in cyberspace; in the provision, exchange, and collection of information with agencies, organizations, and individuals; in internal information sharing and information sharing with other agencies; and in other activities in accordance with the Government of Vietnam’s regulations;

dd) Investing in and building physical facilities suitable for the conditions required to implement cybersecurity protection activities for information systems;

e) Conducting cybersecurity inspections of information systems; preventing and combating violations of cybersecurity laws; and responding to and remedying cybersecurity incidents.

2. Heads of relevant agencies and organizations shall be responsible for implementing cybersecurity protection activities within their management jurisdiction.

Article 24. Cybersecurity protection for national cyberspace infrastructure and international network gateways

1. Cybersecurity protection for national cyberspace infrastructure and international network gateways shall ensure a close combination between cybersecurity protection requirements and socio-economic development requirements; international network gateways located within the territory of Vietnam shall be encouraged; organizations and individuals shall be encouraged to participate in investment in the development of national cyberspace infrastructure.

2. Agencies, organizations, and individuals that manage and operate national cyberspace infrastructure and international network gateways shall have the following responsibilities:

a) Protect cybersecurity within their management scope; be subject to management, inspection, and examination by competent state authorities; and comply with cybersecurity protection requirements imposed by competent state authorities;

b) Facilitate and implement necessary technical and professional measures to enable competent state authorities to perform cybersecurity protection tasks upon request.

Article 25. Assurance of cyber information security

1. Websites, web portals, or specialized pages on social networks of agencies, organizations, and individuals shall not provide, post, or transmit information with contents specified in Clauses 1, 2, and 3 of Article 13 and Clause 1 of Article 15 of this Law, or other information that infringes on national security.

2. Domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam shall have the following responsibilities:

a) Verify information when users register digital accounts; ensure the security of users' information and accounts; and provide user information for the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam no later than 24 hours from the time a request is made by written document, email, telephone, or another verified form of communication for verification, investigation, and handling of violations of cybersecurity laws; in emergency cases threatening national security or human life, information shall be provided no later than 3 hours;

b) Prevent the sharing of information; delete information; and remove services or applications with contents in violation of this Law no later than 24 hours from the time a request is made by the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam; and retain system logs for verification, investigation, and handling of violations of cybersecurity laws for the period prescribed by law; in emergency cases threatening national security, requests to block or remove information shall be complied with no later than 6 hours;

c) Refrain from providing or ceasing the provision of services on telecommunications networks, the Internet, and value-added services for organizations and individuals that post information in cyberspace with contents specified in Clauses 1, 2, and 3 of Article 13 and Clauses 1 and 2 of Article 14 of this Law, upon the request of the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam;

d) Store personal information of service users and data generated by service users, including account names, service usage time, service fee payment information, IP addresses, and other related data, for the period prescribed by law after users terminate service use.

3. Domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam that collect, utilize, analyze, and process personal data, data on relationships of service users, and data generated by service users in Vietnam shall apply data protection measures in accordance with the law and store such data in Vietnam for the period prescribed by the Government of Vietnam.

Foreign enterprises specified in this Clause shall establish a branch or representative office in Vietnam.

4. The Government of Vietnam shall elaborate on Clauses 2 and 3 of this Article.

Article 26. Assurance of data security

1. Assurance of data security refers to an overall set of technical, organizational, and legal measures to protect data and prevent and combat acts of infringement on data security.

2. The contents of data security assurance include:

a) Developing policies and establishing procedures for data security assurance;

b) Applying measures, standards, and technical regulations in accordance with the law on cybersecurity;

c) Using cipher cryptography and civil cryptography to ensure data security;

d) Implementing strict personnel control mechanisms for those directly involved in data processing;

dd) Conducting periodic inspections and risk assessments to detect, prevent, and promptly address threats to data security;

e) Inspecting and assessing cross-border data transfers; conditions for ensuring data security in national security information systems, databases, data centers, and data storage systems;

g) Other contents as prescribed by law.

3. The Government of Vietnam shall elaborate on Clause 2 of this Article and stipulate the responsibilities for ensuring data security.

Chapter V

STANDARDS, TECHNICAL REGULATIONS, PRODUCTS, AND SERVICES CONCERNING CYBERSECURITY

Article 27. Standards and technical regulations on cybersecurity

1. Standards and technical regulations on cybersecurity shall apply to information systems, hardware, software, cybersecurity management and operation systems, cybersecurity products and services, information technology, and network-connected devices.

2. Certification of conformity with technical regulations on cybersecurity, declaration of conformity with technical regulations on cybersecurity, certification of conformity with cybersecurity standards, and declaration of conformity with cybersecurity standards shall be carried out in accordance with the law on standards and technical regulations.

3. Assessment of conformity with standards and technical regulations on cybersecurity serving national security information systems and state management activities concerning cybersecurity shall be conducted by conformity assessment organizations designated by the Minister of Public Security of Vietnam.

4. The Ministry of Public Security of Vietnam shall have the following responsibilities:

a) Develop draft national standards on cybersecurity;

b) Manage the quality of cybersecurity products and services, except for civil cryptographic products and services;

c) Register, designate, and manage the activities of cybersecurity conformity assessment organizations, except for the cases prescribed in Clause 6 of this Article.

5. The Minister of Public Security of Vietnam shall promulgate national technical regulations on cybersecurity.

6. The Ministry of National Defense of Vietnam shall register, designate, and manage the activities of cybersecurity conformity assessment organizations in the military field.

The Government Cipher Committee shall assist the Minister of National Defense of Vietnam in managing the quality of civil cryptographic products and services, as well as registering, designating, and managing the activities of cybersecurity conformity assessment organizations for civil cryptographic products and services.

Article 28. Cybersecurity products and services

1. Cybersecurity products include:

a) Civil cryptographic products;

b) Cybersecurity inspection and assessment products;

c) Cybersecurity supervision products;

d) Products for preventing cyberattacks and infiltrations;

dd) Other cybersecurity products.

2. Cybersecurity services include:

a) Cybersecurity inspection and assessment services;

b) Information security services not using civil cryptography;

c) Civil cryptography services;

d) Cybersecurity consulting services;

dd) Cybersecurity supervision services;

e) Cybersecurity incident response services;

g) Data recovery services;

h) Cyberattack prevention and response services;

i) Other cybersecurity services.

3. The Government of Vietnam shall elaborate on this Article.

Article 29. Business operations involving cybersecurity products and services

1. Enterprises engaged in the business of cybersecurity products and services shall obtain a cybersecurity product and service business license.

2. Enterprises engaged in the business of cybersecurity products and services shall have the following responsibilities:

a) Ensure compliance with the cybersecurity product and service business license, and compliance with the law on cybersecurity and other relevant laws;

b) Ensure that the quality of cybersecurity products and services conforms with the declared applicable standards and corresponding technical regulations in accordance with the law on product and goods quality and the law on standards and technical regulations before circulation on the market;

c) Establish, store, and safeguard clients' information; manage records and documents on technical solutions and technologies of products and service provision activities in accordance with the law;

d) Refuse to provide cybersecurity products and services upon detecting that organizations or individuals violate the law on the use of cybersecurity products and services or breach commitments agreed upon regarding the use of products and services provided by the enterprise;

dd) Cooperate with, facilitate, and comply with requests of the specialized cybersecurity protection forces in implementing cybersecurity protection measures.

3. The Government of Vietnam shall stipulate the issuance, suspension, and revocation of cybersecurity product and service business licenses, the import and export of cybersecurity products, and business activities involving cybersecurity products and services.

Chapter VI

FORCES AND CONDITIONS FOR ENSURING CYBERSECURITY

Article 30. Cybersecurity protection forces

1. Cybersecurity protection forces include:

a) Specialized cybersecurity protection forces arranged within the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam;

b) Cybersecurity protection forces arranged within ministries, central authorities, provincial People's Committees, and agencies or organizations directly managing national security information systems;

c) Organizations and individuals mobilized to participate in cybersecurity protection.

2. The Government shall elaborate on Clause 1 of this Article and stipulate the cooperation among cybersecurity protection forces.

Article 31. Assurance of human resources for cybersecurity protection

1. The State shall train and develop human resources for cybersecurity protection in sufficient quantity and quality to meet the capacity requirements for protecting national cybersecurity.

2. Specialized cybersecurity protection forces shall be given priority in personnel arrangement according to job position and title standards, and be subject to special mechanisms for recruitment, selection, utilization, training, advanced training, treatment, and talent attraction as prescribed by the Government of Vietnam.

3. Information system administrators of national security information systems shall have the following responsibilities:

a) Arrange appropriate units or specialized personnel in accordance with the protection level of the system;

b) Ensure that personnel performing cybersecurity tasks meet professional and technical standards;

c) Regularly provide advanced training courses and update skills for personnel involved in the operation, supervision, incident response, and handling of network incidents.

Article 32. Recruitment, training, and development of cybersecurity protection forces

1. Vietnamese citizens who meet standards of moral integrity, health, qualifications, and knowledge of cybersecurity and information technology, and who have aspirations, may be recruited into cybersecurity protection forces.

2. Priority shall be given to training and developing high-quality cybersecurity forces, as well as identifying young talent in cybersecurity and information technology, to guide their education, recruitment, attraction, and utilization in the cybersecurity field.

3. Priority shall be given to developing cybersecurity training institutions that meet international standards, encouraging linkage, and creating cooperation opportunities in cybersecurity between the public and private sectors, domestically and internationally.

Article 33. Education and advanced training in cybersecurity

1. Cybersecurity education and advanced training contents shall be incorporated into national defense and security education subjects in schools and into national defense and security knowledge training programs in accordance with the Law on National Defense and Security Education.

2. The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries and central authorities in organizing professional cybersecurity training for cybersecurity protection forces and for civil servants, public employees, and employees participating in cybersecurity protection.

The Ministry of National Defense of Vietnam and the Government Cipher Committee shall organize professional cybersecurity training for entities under their management.

Article 34. Training in in-depth cybersecurity knowledge and skills

1. Cybersecurity protection forces specified in Points a and b Clause 1 Article 30 of this Law shall meet the requirements for in-depth cybersecurity knowledge and skills.

2. Individuals directly administering and operating information systems at levels 3, 4, and 5 within agencies, organizations, and state-owned enterprises shall receive in-depth cybersecurity knowledge and skills training and be granted certification, except for those already trained in cybersecurity as a specialized discipline.

3. The Ministry of Public Security of Vietnam shall take charge and cooperate with relevant ministries and central authorities in organizing in-depth cybersecurity knowledge and skills training, except for the cases prescribed in Clause 4 of this Article.

4. The Ministry of National Defense of Vietnam and the Government Cipher Committee shall organize in-depth cybersecurity knowledge and skills training for entities under their management.

5. The Government of Vietnam shall stipulate standards for in-depth cybersecurity knowledge and skills, programs, contents, and certification of in-depth cybersecurity knowledge and skills training.

Article 35. Universalization of cybersecurity knowledge

1. The State shall adopt policies to universalize cybersecurity knowledge nationwide, encourage state agencies to cooperate with private organizations and individuals in implementing education and awareness-raising programs on cybersecurity, and prioritize the universalization and guidance for children, the elderly, and persons with cognitive difficulties to enhance their capacity to protect their lawful rights and interests in cyberspace.

2. Ministries, central authorities, agencies, and organizations shall develop and implement activities to universalize cybersecurity knowledge for cadres, civil servants, public employees, and employees under their management.

3. Provincial People’s Committees shall develop and implement activities to universalize knowledge and raise awareness of cybersecurity for agencies, organizations, and individuals within their areas.

Article 36. Research and development of cybersecurity

1. Research and development of cybersecurity shall include:

a) Development of software systems and equipment for cybersecurity protection;

b) Methods for appraising software and equipment for cybersecurity protection to ensure standard compliance and to limit weaknesses, security vulnerabilities, and malicious software;

c) Methods for inspecting hardware and software provided to ensure that they perform their intended functions;

d) Methods for protecting state secrets, work secrets, business secrets, personal secrets, family secrets, and private life, and ensuring security during the transmission of information in cyberspace;

dd) Identification of the origin of information transmitted in cyberspace;

e) Cybersecurity threat resolution;

g) Development of cyber ranges and cybersecurity testing environments;

h) Technical initiatives to enhance cybersecurity awareness and skills;

i) Cybersecurity forecasting;

k) Research of practice and development of cybersecurity theory.

2. Relevant agencies, organizations, and individuals shall have the right to conduct cybersecurity research and development.

Article 37. Enhancement of cybersecurity self-reliance capacity

1. The State shall encourage and facilitate agencies, organizations, and individuals to enhance their cybersecurity self-reliance capacity and to improve their capacity in the production, inspection, assessment, and certification of digital devices, network services, and network applications.

2. The Government of Vietnam shall implement the following measures to enhance cybersecurity self-reliance capacity for agencies, organizations, and individuals:

a) Direct the development of policies, strategies, and development planning for the cybersecurity industry; standards and technical regulations for hardware and software products, to proactively eliminate cybersecurity risks from the product formation stage;

b) Promote technology transfer, research, mastery, and development of technologies, products, and services of the cybersecurity industry;

c) Promote the application of new and advanced technologies related to cybersecurity;

d) Organize training, development, and optimization of the use of high-quality cybersecurity human resources;

dd) Strengthen the business environment, improve competitive conditions, and support enterprises in researching and producing products, services, and applications for cybersecurity protection.

3. Investment activities and mobilization of resources for the development of cybersecurity industry infrastructure shall include:

a) Investment activities in the construction of cybersecurity industrial infrastructure shall be classified as sectors and professions entitled to special investment incentives and eligible for incentives and support in accordance with the law on investment, tax law, land law, and other relevant laws;

b) The State shall prioritize the allocation of state budget capital for investment in the construction of cybersecurity industry infrastructure, including: research, design, production, and testing facilities for cybersecurity products and services; national key laboratories for cybersecurity; facilities for measurement, testing, and assessment of cybersecurity products and services; big data centers; centralized cybersecurity industrial parks; and cybersecurity industrial complexes;

c) Cybersecurity industry infrastructure invested in by the State as prescribed in Point b of this Clause refers to a type of infrastructure asset and shall be managed, utilized, and operated in accordance with the law on management and use of public property;

d) Organizations and enterprises shall be permitted to import technological lines, devices, machinery, and tools serving training, research, and development activities for cybersecurity products and services;

dd) Agencies, organizations, and state-owned enterprises shall prioritize the use of domestically produced cybersecurity products and services.

4. The Ministry of Public Security of Vietnam shall advise and assist the Government of Vietnam in the construction and development of cybersecurity industry infrastructure to enhance cybersecurity self-reliance capacity.

Article 38. Funding for cybersecurity protection

1. Agencies, organizations, state-owned enterprises, political organizations, socio-political organizations, and public service providers funded by the state budget shall allocate funding for

cybersecurity protection within their annual expenditure estimates for tasks related to digital transformation and the application of information technology. They shall also allocate at least 15% of the total funding for programs, schemes, and investment projects on digital transformation and the application of information technology for cybersecurity protection.

2. Agencies, organizations, and units not specified in Clause 1 of this Article shall ensure funding for cybersecurity protection for their agencies, organizations, and units.

Chapter VII

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS, AND INDIVIDUALS FOR CYBERSECURITY

Article 39. Responsibilities for state management of cybersecurity

1. The Government of Vietnam shall carry out consistent state management of cybersecurity.

2. The Ministry of Public Security of Vietnam shall act as the focal agency assisting the Government of Vietnam in carrying out state management of cybersecurity and assume responsibility before the Government of Vietnam for performing the following cybersecurity state management tasks, except for the contents specified in Clauses 3 and 4 of this Article:

a) Promulgating or requesting competent state authorities to promulgate legislative documents on cybersecurity;

b) Developing and proposing strategies, guidelines, policies, and plans for cybersecurity protection; researching, constructing, developing, and using security cryptography to protect data security within the scope of management of the Ministry of Public Security of Vietnam;

c) Cooperating with relevant agencies in conducting dissemination activities and refuting information containing content opposing the Socialist Republic of Vietnam as prescribed in Clause 1 Article 13 of this Law;

d) Requesting enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace, as well as information system administrators, to remove information containing content in violation of cybersecurity laws from services and information systems directly managed by such enterprises, agencies, or organizations;

dd) Preventing and combating activities using cyberspace to infringe on sovereignty, interests, national security, social order and safety, and preventing and combating cybercrime;

e) Ensuring information security in cyberspace and data security; developing mechanisms for IP address identification management; authenticating digital account registration information; providing warnings and sharing information on cybersecurity incidents and cybersecurity threats;

g) Advising and proposing that the Government of Vietnam and the Prime Minister of Vietnam consider deciding the assignment of and cooperation in the implementation of cybersecurity protection measures and the prevention and handling of cybersecurity infringements in cases where state management contents fall under the responsibility of multiple ministries or central authorities;

h) Mobilizing experts, scientists, specialized cadres, and requisitioning systems, equipment, and devices in emergencies to protect national security and ensure social order and safety in cyberspace;

i) Organizing cyberattack prevention drills and cybersecurity incident response and remediation drills for national security information systems;

k) Inspecting, examining, and settling complaints and denunciations, and handling violations of cybersecurity laws.

3. The Ministry of National Defense of Vietnam shall assume responsibility before the Government of Vietnam for carrying out state management of cybersecurity within its scope of management, including:

a) Promulgating or requesting competent state authorities to promulgate legislative documents on cybersecurity within its scope of management;

b) Developing and proposing strategies, guidelines, policies, and plans for cybersecurity protection within its scope of management;

c) Preventing and combating activities using cyberspace to infringe on national security within its scope of management;

d) Cooperating with the Ministry of Public Security of Vietnam in organizing cyberattack prevention drills and cybersecurity incident response and remediation drills for national security information systems, and implementing cybersecurity protection activities;

dd) Inspecting, examining, and settling complaints and denunciations, and handling violations of cybersecurity laws within its scope of management.

4. The Government Cipher Committee shall assist the Minister of National Defense of Vietnam in carrying out state management of civil cryptography and cybersecurity within its scope of management in accordance with the law.

5. Ministries, ministerial agencies, and governmental agencies shall, within their respective scope of functions, tasks, and entitlements, carry out cybersecurity protection activities and cooperate with the Ministry of Public Security of Vietnam in state management of cybersecurity.

6. Provincial People's Committees shall carry out cybersecurity protection activities in their areas and cooperate with the Ministry of Public Security of Vietnam in state management of cybersecurity.

Article 40. Responsibilities of information system administrators in cybersecurity protection

1. Information system administrators shall have the following responsibilities:

a) Implement cybersecurity protection for information systems in accordance with this Law;

b) Connect cybersecurity supervision systems and centralized malicious software prevention systems to the National Cybersecurity Center of the Ministry of Public Security of Vietnam or the Cybersecurity Centers of provinces and cities to support cybersecurity supervision;

c) Report cybersecurity incidents to the specialized agencies of the Ministry of Public Security of Vietnam or the Ministry of National Defense of Vietnam.

2. Administrators of information systems funded by the state budget shall, in addition to the responsibilities specified in Clause 1 of this Article, have the following responsibilities:

a) Develop cybersecurity protection plans that are subject to cybersecurity appraisal by competent state authorities when establishing, expanding, or upgrading information systems;

b) Designate specific individuals or units to take charge of cybersecurity.

Article 41. Responsibilities of enterprises providing services in cyberspace

1. Comply with cybersecurity laws.

2. Warn users of potential cybersecurity risks arising from the use of services provided in cyberspace, provide guidelines on preventive measures, and develop emergency response plans to ensure cybersecurity to address vulnerabilities, risks, and cybersecurity incidents proactively.

3. Upon the occurrence of a cybersecurity incident, immediately implement emergency response plans to ensure cybersecurity and promptly report the incident to the specialized cybersecurity protection forces in accordance with this Law.

4. Apply measures and technical solutions to ensure cybersecurity in data processing activities, including personal data processing, in accordance with this Law, data laws, personal data protection laws, and other relevant laws.

5. Assume responsibility for identifying the IP addresses of organizations and individuals using Internet services, and provide the specialized cybersecurity protection forces with IP address identification information for the implementation of cybersecurity protection measures.

6. Cooperate in accordance with the guidelines of the specialized cybersecurity protection forces under the Ministry of Public Security of Vietnam in establishing connection systems, connecting technical transmission lines, transmitting data, and meeting other necessary conditions for implementing cybersecurity protection measures and solutions upon request to serve the investigation, verification, and handling of violations of cybersecurity laws.

7. Enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam shall comply with this Article and Clauses 2 and 3 of Article 25 of this Law.

Article 42. Responsibilities of agencies, organizations, and individuals using cyberspace

1. Comply with cybersecurity laws.

2. Safeguard information related to the registration, opening, management, and use of their digital accounts. Where digital accounts are used to commit violations of law, depending on the nature and severity of the violations, digital account holders or users shall be subject to disciplinary actions, administrative penalties, or criminal prosecution; where damage is caused to State interests or the lawful rights and interests of organizations or individuals, compensation shall be paid in accordance with the law.

3. Promptly provide competent authorities and cybersecurity protection forces with information related to cybersecurity protection, cybersecurity threats, and acts infringing on cybersecurity.

4. Comply with requests and guidelines from competent authorities in cybersecurity protection; assist and facilitate agencies, organizations, and responsible persons in carrying out cybersecurity protection measures.

Chapter VIII

IMPLEMENTATION

Article 43. Amendments and supplements to certain articles of relevant laws

1. Replacement of several phrases and annulment of certain clauses of the Law on Archives No. 33/2024/QH15:

a) The phrase “an toàn thông tin” (information safety) in Point b Clause 1 Article 35, the phrase “an toàn thông tin mạng” (cyber information safety) in Point b Clause 2 Article 36, and the phrase “an toàn, an ninh thông tin” (information safety and security) in Clause 3 Article 60 is replaced with the phrase “an ninh mạng” (cybersecurity);

b) Clause 4 Article 58 is annulled.

2. Replacement and annulment of several phrases of the Law on Protection of Consumer Rights No. 19/2023/QH15:

a) The phrase “an toàn thông tin” (information safety) is replaced with the phrase “an ninh thông tin” (information security) in Point d Clause 1 Article 16; the phrase “an toàn, an ninh thông tin” (information safety and security) is replaced with the phrase “an ninh mạng” (cybersecurity) in Clause 1 Article 15, the title of Article 19, and Clauses 1 and 3 of Article 19;

b) The phrase “an toàn thông tin mạng,”(cyber information safety) in Clause 3 Article 19 is annulled.

3. Replacement of several phrases of the Law on Fees and Charges No. 97/2015/QH13, amended by Law No. 90/2017/QH14, Law No. 23/2018/QH14, Law No. 72/2020/QH14, Law No. 16/2023/QH15, Law No. 20/2023/QH15, Law No. 24/2023/QH15, Law No. 33/2024/QH15, Law No. 35/2024/QH15, Law No. 47/2024/QH15, Law No. 60/2024/QH15, Law No. 74/2025/QH15, Law No. 89/2025/QH15, Law No. 94/2025/QH15, Law No. 95/2025/QH15, and Law No. 118/2025/QH15:

a) The phrase “an toàn thông tin” (information safety) in Subsection 10 Section VI of Part A and Subsection 16 Section III of Part B of Appendix No. 1 – List of fees and charges, is replaced with the phrase “an ninh mạng” (cybersecurity);

b) The phrase “an toàn thông tin mạng” (cyber information safety) in Subsection 11 Section VI of Part A of Appendix No. 1 – List of fees and charges, is replaced with the phrase “an ninh mạng” (cybersecurity);

4. Replacement and annulment of several phrases of the Law on Digital Technology Industry No. 71/2025/QH15:

a) The phrase “an toàn thông tin” (information safety) in Point a Clause 1 Article 25 is replaced with the phrase “an ninh mạng” (cybersecurity);

b) The phrase “an toàn thông tin mạng,” (cyber information safety) in Article 10 is annulled.

5. Replacement and annulment of several phrases of the Law on Data No. 60/2024/QH15:

a) The phrase “an toàn, an ninh dữ liệu” (data safety and security) in Clause 4 Article 25 is replaced with the phrase “an ninh dữ liệu” (data security);

b) The phrase “an ninh, an toàn thông tin” (information safety and security) in Clause 2 Article 33 is replaced with the phrase “an ninh mạng” (cybersecurity);

c) The phrase “, an toàn thông tin”(information safety) in Clause 4 Article 25 is annulled;

d) The phrase “an toàn thông tin mạng,”(cyber information safety) in Clause 4 Article 39 is annulled;

dd) The phrase “pháp luật về an toàn thông tin mạng,”(cyber information safety laws) in Clause 4 Article 43 is annulled.

6. Replacement and annulment of several phrases of the Law on Cultural Heritage No. 45/2024/QH15, amended by Law No. 84/2025/QH15:

a) The phrase “an toàn thông tin mạng” (cyber information safety) in Clause 4 Article 59 is replaced with the phrase “an ninh mạng” (cybersecurity);

b) The phrase “an toàn thông tin mạng,”(cyber information safety) in Point c Clause 2 Article 86 is annulled;

7. Replacement and annulment of several phrases of the Law on Telecommunications No. 24/2023/QH15, amended by Law No. 47/2024/QH15:

a) The phrase “an toàn thông tin mạng” (cyber information safety) in Clause 8 Article 5 is replaced with the phrase “an ninh thông tin” (information security);

b) The phrase “, an toàn thông tin mạng” (cyber information safety) in the title of Article 5 and Clause 1 Article 5 and Point c Clause 2 Article 38 is annulled;

c) The phrase “an toàn thông tin mạng” (cyber information safety) in Clause 2 Article 21 and Point b Clause 2 Article 29 is annulled.

8. Replacement and annulment of several phrases of the Law on Electronic Transactions No. 20/2023/QH15, amended by Law No. 60/2024/QH15:

b) The phrase “an toàn thông tin mạng” (cyber information safety) in the title of Article 5 is annulled;

b) The phrase “pháp luật về an toàn thông tin mạng,”(cyber information safety laws) in Clause 1 Article 5 is annulled;

c) The phrase “an toàn thông tin mạng” (cyber information safety) in Point c Clause 1 Article 20, Clause 2 Article 21, Point c Clause 1 Article 29, Clause 6 Article 30, Clause 4 Article 44, Point a Clause 4 Article 46, and Point c Clause 1 Article 47 is replaced with the phrase “an ninh mạng” (cybersecurity);

d) The phrase “an toàn thông tin mạng” (cyber information safety) in Point d Clause 1 Article 42 and Point a Clause 1 Article 47 is annulled.

9. The phrase “an toàn thông tin mạng” (cyber information safety) in Point b Clause 2 Article 12 of the Law on Corporate Income Tax No. 67/2025/QH15; Clause 1 Article 169 of the Law on Land No. 31/2024/QH15, amended by Law No. 43/2024/QH15, Law No. 47/2024/QH15, Law No. 58/2024/QH15, Law No. 71/2025/QH15, Law No. 84/2025/QH15, Law No. 93/2025/QH15, and Law No. 95/2025/QH15., is replaced with the phrase “an ninh mạng” (cybersecurity).

10. The phrase “an ninh, an toàn thông tin” (information safety and security) in Point a Clause 3 Article 7 of the Law on Water Resources No. 28/2023/QH15, amended by Law No. 84/2025/QH15, is replaced with the phrase “an ninh mạng” (cybersecurity).

11. The phrase “an toàn thông tin mạng;” (cyber information safety) in Point dd Clause 1 Article 24 of the Law on Handling of Administrative Violations No. 15/2012/QH13, amended by Law No. 54/2014/QH13, Law No. 18/2017/QH14, Law No. 67/2020/QH14, Law No. 09/2022/QH15, Law No. 11/2022/QH15, Law No. Luật56/2024/QH15, and Law No. 88/2025/QH15, is annulled.

12. The phrase “an toàn thông tin mạng,” (cyber information safety) in Clause 6 Article 16 of the Law on People’s Public Security Force No. 37/2018/QH14, amended by Law No. 21/2023/QH15, Law No. 30/2023/QH15, Law No. 38/2024/QH15, Law No. 52/2024/QH15, and Law No. 86/2025/QH15; in Clause 1 Article 66 of the Law on Election of Deputies to the National Assembly and People’s Councils No. 85/2015/QH13, amended by Law No. 83/2025/QH15, is annulled.

13. The phrase “, an toàn thông tin” (information safety) in Clause 3 Article 136 of the Law on Organization of People’s Courts No. 34/2024/QH15, amended by Law No. 81/2025/QH15; Clause 1 Article 26 of the Law on Electricity No. 61/2024/QH15, amended by Law No. 94/2025/QH15, is annulled.

14. The phrase “an toàn thông tin,” (information safety) in Clause 8 Article 29 and the phrase “an toàn thông tin và” (information safety and) in Clauses 2 and 7 Article 29 of the Law on Chemicals No. 69/2025/QH15 are annulled.

15. The phrase “an toàn thông tin,” (information safety) in Clause 3 Article 51 and Clauses 1 and 5 Article 52 of the Law on Bidding No. 22/2023/QH15, amended by Law No. 57/2024/QH15 and Law No. 90/2025/QH15; Point e Clause 1 Article 23 of the Law on Civil Defense No. 18/2023/QH15, amended by Law No. 98/2025/QH15, is annulled.

16. The phrase “, pháp luật về bảo đảm an toàn thông tin” (information safety assurance laws) in Clause 4 Article 7 of the Law on Atomic Energy No. 94/2025/QH15 is annulled.

17. Clause 3 Article 49 of the Law on Libraries No. 46/2019/QH14 is annulled.

Article 44. Entry into force

1. This Law comes into force as of July 1, 2026.

2. The Law on Cybersecurity No. 86/2015/QH13, amended by Law No. 35/2018/QH14, and the Law on Cybersecurity No. 24/2018/QH14 shall cease to have effect from the effective date of this Law.

Article 45. Transitional provisions

1. Information systems whose levels have been determined under the Law on Cybersecurity No. 86/2015/QH13, amended by Law No. 35/2018/QH14, shall continue to maintain the determined levels from the effective date of this Law; within 12 months from the effective date of this Law, such systems shall ensure compliance with the conditions, standards, and cybersecurity protection measures corresponding to their respective levels as prescribed by this Law.

2. Licenses to engage in the business of cyber information security products and services and civil cryptography prescribed by the Law on Cybersecurity No. 86/2015/QH13, amended by Law No. 35/2018/QH14, that have been issued before the effective date of this Law, shall remain valid until the expiry date stated in such licenses.

3. Products, services, solutions, and technical equipment used for ensuring cyber information security in accordance with the Law on Cyber Information Security No. 86/2015/QH13, amended by Law No. 35/2018/QH14, that have been put into use before the effective date of this Law, shall continue to be used; within 12 months from the effective date of this Law, they must satisfy the cybersecurity conditions prescribed by this Law.

This Law is approved by the 15th National Assembly of the Socialist Republic of Vietnam during its 10th meeting session on December 10, 2025.

PRESIDENT OF THE NATIONAL ASSEMBLY

Tran Thanh Man