LAW 116
ON CYBERSECURITY
Dated 10 December 2025

CONTENTS

Chapter I 1

GENERAL PROVISIONS 1

Article 1 *Governing scope and applicable entities* 1

Article 3 *State policies on cybersecurity* 3

Article 4 *Principles of cybersecurity protection* 3

Article 5 *Measures for cybersecurity protection* 3

Article 6 *International cooperation on cybersecurity* 4

Article 7 *Conduct which is strictly prohibited* 5

Chapter II 6

PROTECTION OF CYBERSECURITY OF INFORMATION SYSTEMS 6

Article 8 *Classification of information system levels* 7

Article 9 *Information systems critical for national security* 7

Article 10 *Tasks and measures for protecting cybersecurity of information systems* 8

Article 11 *Responsibilities to protect cybersecurity of information systems critical for national security* 9

Article 12 *Inspection of cybersecurity of information systems of agencies and organizations not on the list of information systems critical for national security* 9

Chapter III 10

PREVENTION OF AND DEALING WITH AN INFRINGEMENT OF CYBERSECURITY 10

Article 13 *Information and acts of using information technology and electronic facilities to infringe national security and social order and safety in cyberspace* 10

Article 14 *Prevention of and dealing with information and acts of using IT or e-facilities to infringe upon national security, and social order and safety in cyberspace* 12

Article 15 *Prevention of and combatting cyberespionage; and protection of information classified as State secret, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace* 12

Article 16 *Prevention and combat of child abuse in cyberspace* 14

Article 17 *Prevention, discovery, stopping and dealing with malicious software* 14

Article 18 *Prevention of and combating cyberattacks* 15

Article 19 *Prevention of and combating cyberterrorism* 16

Article 20 *Prevention of and dealing with dangerous cybersecurity situations* 16

Article 21 *Fighting to protect cybersecurity* 17

Article 22 *Prevention of conflict of information in cyberspace* 18

Chapter IV 18

CYBERSECURITY PROTECTIVE ACTIVITIES 18

Article 23 *Implementation of cybersecurity protective activities in State agencies, political organizations and socio-political organizations at the central and local levels* 18

Article 24 *Protection of cybersecurity of national cyberspace infrastructure and international network gateways* 19

Article 25 *Guarantees relating to cyberinformation security* 19

Article 26 *Guarantees relating to data security* 20

CHAPTER V 20

STANDARDS AND TECHNICAL REULATIONS, CYBERSECURITY PRODUCTS AND SERVICES 20

Article 27 *Standards and technical regulations on cybersecurity* 20

Article 28 *Cybersecurity products and services* 21

Article 29 *Business of cybersecurity products and services* 21

CHAPTER VI 22

FORCES AND CONDITIONS FOR GUARANTEEING CYBERSECURITY 22

Article 30 *Cybersecurity protective forces* 22

Article 31 *Guarantees relating to cybersecurity protective human resources* 22

Article 32 *Selection, training and development of cybersecurity protective forces* 23

Article 33 *Education and retraining on cybersecurity knowledge and expertise* 23

Article 34 *Training on advanced cybersecurity knowledge and skills* 23

Article 35 *Dissemination of knowledge about cybersecurity* 23

Article 36 *Research and development of cybersecurity* 24

Article 37 *Improvement of self-autonomy regarding cybersecurity* 24

Article 38 *Funds for cybersecurity protective activities* 25

Chapter VII 25

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR CYBERSECURITY ..25

Article 39 *Responsibilities of State administration of cybersecurity* 25

Article 40 *Responsibilities of administrators of information systems in protection of cybersecurity* 27

Article 41 *Responsibilities of enterprises providing services in cyberspace* 27

Article 42 *Responsibilities of agencies, organizations and individuals using cyberspace* 28

Chapter VIII 28

IMPLEMENTING PROVISIONS 28

Article 43 *Amendments to a number of articles of relevant laws* 28

Article 44 *Effectiveness* 29

Article 45 *Transitional provisions* 30

NATIONAL ASSEMBLY

No. 116/2025/QH15

SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

LAW
ON
CYBERSECURITY

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

The National Assembly hereby promulgates the *Law on Cybersecurity*.

Chapter I

GENERAL PROVISIONS

Article 1 *Governing scope and applicable entities*

1. This Law regulates cybersecurity, protection of cybersecurity; and the rights, obligations and responsibilities of agencies, organizations and individuals involved.

2. This Law applies to:

   (a) Vietnamese agencies, organizations and individuals;

   (b) Foreign agencies, organizations and individuals in Vietnam and people of Vietnamese origin with unidentified nationality who currently live in Vietnam and have been issued with certificates of identity;

   (c) Foreign agencies, organizations and individuals directly participating or involved in protection of cybersecurity and business of cybersecurity products and services in Vietnam.

Article 2 *Interpretation of terms*

In this Law, the following terms are construed as follows:

1. *Cybersecurity* means the stability, security and safety of cyberspace; protection of information systems and assurance that information, data and activities in cyberspace will not cause harm to [infringe][1] national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals.

2. *Cyberinformation security* means the assurance of the integrity, confidentiality, and availability of information in cyberspace, and avoidance of unauthorized access, use, disclosure and modification, sabotage or other acts which threaten or cause harm to national security, social order and safety.

3. *Data security* means the assurance of data quality and the activities of processing and using data in cyberspace for the purposes of socio-economic development, national digital transformation, and avoidance of unauthorized access, use, disclosure, and modification, sabotage or other acts which threaten or cause harm to national security, social order and safety.

4. *Cybersecurity protection* means the prevention, detection, avoidance of and dealing with acts which infringe cybersecurity.

5. *Cyberspace* means the environment which is formed by the connected network of information technology [IT] infrastructure comprising telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases; and where [being the environment in which] people perform social acts without being limited by space and time.

[1] Allens footnote: Square brackets contain translator's comments only.

6. *National cyberspace* means part of cyberspace under the sovereignty, jurisdiction and control of the State of the Socialist Republic of Vietnam.

7. *Information system* means a collection of hardware, software and data established for the purposes of creation, provision, transmission, collection, processing, storage and exchange of information in cyberspace.

8. *Information system administrator* means an agency, organization or individual having the authority to directly manage an information system.

9. *Malware* means software which is capable of causing abnormal activities to part or all of an information system or illegally copying, modifying and deleting information stored in the information system.

10. *Malicious hardware* means physical parts intentionally designed or added to the components of standard hardware in order to illegally collect information or data or interfere with, stall, paralyse or destroy computer systems and information systems.

11. *System log* means a collection of records reflecting time, users, activities, and status of a system for serving the management, supervision and security of the system.

12. *Cybercrime* means activities which endanger the society as prescribed in the Criminal Code and which are performed by individuals or organizations in cyberspace by using IT or e-facilities.

13. *Cyberattack* means an act conducted in cyberspace by using IT or e-facilities to appropriate information, disrupt, interrupt and/or paralyse operations of, and destroy or control telecom network systems, the Internet, computer networks, information systems, information processing and control systems, and databases or e-facilities.

14. *Cyberterrorism* means an act conducted in cyberspace by using IT or e-facilities to cause public panic or political turmoil.

15. *Cyberespionage* means an act conducted in cyberspace by using IT or e-facilities for secret infiltration to appropriate, collect, and/or copy information within the category of State secrets, or important data of agencies, organizations and individuals for the purpose of causing harm to national security and social order and safety.

16. *Cybersecurity threat* means a condition in cyberspace which presents indications of a threat to infringe national security, and/or to cause serious harm to social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

17. *Cybersecurity incident [or breakdown]* means any unusual occurrence in cyberspace which infringes upon national security, social order and safety and/or the lawful rights and interests of agencies, organizations and individuals.

18. *Dangerous cybersecurity situation* means a condition or development in cyberspace when there is any factor of attack, infiltration, incitement, divulgence, or loss of information or other act which threatens to seriously infringe national security, social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

19. *Digital account* means information used to verify, authenticate and/or delegate authority to use applications and services in cyberspace.

20. *Civil cryptography* means cryptographic techniques and products used to keep confidential or authenticate information not within the category of State secrets in order to ensure information security for agencies, organizations and individuals.

21. *Cybersecurity products* means hardware and software having the function of protecting cybersecurity, cyberinformation security, data security, information, data, information systems, and information technology infrastructure.

22. *Cybersecurity services* means services provided to protect cybersecurity, cyberinformation security,

data security, information, data, information systems, and information technology infrastructure.

23. *Cipher information system* means the information system using cipher cryptography to protect information within the category of State secrets to serve cipher operations directly managed and operated by a cipher organization.

Article 3 *State policies on cybersecurity*

1. Building a healthy cyberspace which does not cause harm to national security, social order and safety or to the lawful rights and interests of agencies, organizations and individuals.

2. Prioritizing protection of network security in the sectors of national defence, security, cipher, socio-economic development, science, technology and foreign affairs.

3. Prioritizing arrangement of resources to build and develop a specialized force responsible for the protection of cybersecurity [Cybersecurity Task Force or CTF][2], and ensuring high quality human resources servicing cybersecurity protection; upgrading the capacity of cybersecurity protective forces and of other organizations and individuals participating in the protection of cybersecurity; prioritizing investment in the activities of research and development of modern science and technology for purposes of protecting cybersecurity; and having special mechanisms and preferential policies to mobilize, attract, train and use talents in the sector of cybersecurity.

4. Promoting affiliation and investment in the public private partnership form in the protection of cybersecurity; encouraging and facilitating agencies, organizations and individuals to participate in protecting cybersecurity and to deal with cybersecurity threats; researching and developing technology, products, services and applications for the purpose of protecting cybersecurity; and using cybersecurity products and services of Vietnam.

5. Expanding international cooperation on cybersecurity to enhance the ability to protect cybersecurity; preventing and combating cybercrime and threats of cross-border cybersecurity; and receiving modern technology in order to improve the capacity of self-autonomy of national cybersecurity.

Article 4 *Principles of cybersecurity protection*

1. Compliance with the Constitution and law; ensuring national security, sovereignty and interest in cyberspace.

2. Leadership by the Vietnamese Communist Party; and uniform administration by the State; mobilization of the combined strength of the political system and the entire nation; and development of the key role of the Cybersecurity Task Force.

3. Close association between the protection of cybersecurity and socio-economic development, ensuring human rights and civil rights, protecting personal data, and facilitating [all] agencies, organizations and individuals to conduct lawful activities in cyberspace.

4. Application of measures to protect national cyberspace; proactive prevention, detection, ending, fighting and defeating all acts in cyberspace to infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals; and promptly and strictly dealing with breaches of the law on cybersecurity.

5. Implementing cybersecurity protective activities regularly and continuously for the national cyberspace infrastructure; proactively applying measures to protect information systems critical for national security.

Article 5 *Measures for cybersecurity protection*

1. The measures for protecting cybersecurity comprise:

[2] Allens footnote: The literal translation is "specialized protective force" but for ease of reference Cybersecurity Task Force or CTF is used throughout

(a) Evaluation of cybersecurity;

(b) Assessment of cybersecurity conditions;

(c) Inspections [audits] of cybersecurity;

(d) Supervision of cybersecurity;

(dd) Response to and remedying any cybersecurity incident;

(e) Fighting [working hard] to protect cybersecurity;

(g) Using cryptography to protect cyberinformation;

(h) Using technical solutions to protect cyberinformation security, data security, information systems, and preventing information in breach of law;

(i) Stopping or requiring the temporary suspension or suspension of cyberinformation; suspension or temporary suspension of the acts of establishment, supply and use of telecom networks or the Internet, manufacturing and using radio transmitters and receivers in accordance with law;

(k) Requiring the deletion, access to delete unlawful or false information or fake news in cyberspace which infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals;

(l) Collecting electronic data relevant to acts of infringing national security, social order and safety or the lawful rights and interests of agencies, organizations and individuals in cyberspace;

(m) Freezing or restricting the operation of information systems; suspending, temporarily suspending or requiring the cessation of operation of information systems or withdrawing domain names in accordance with law;

(n) Laying charges and conducting investigations, prosecutions and trials in accordance with the Criminal Procedure Code;

(o) Other measures stipulated in the law on national security and the law on dealing with administrative offences.

2. The Government shall provide detailed regulations on the contents, sequence and procedures and authority for applying measures to protect cybersecurity, except for those prescribed in sub-clauses (n) and (o) of clause 1 above.

Article 6 *International cooperation on cybersecurity*

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

2. The contents of international cooperation on cybersecurity comprise:

(a) Sharing of information and data and early warning of any threats, incidents, and cyberattacks affecting cybersecurity;

(b) Formulation of legal framework, policies and mechanisms for cooperation and coordination in the protection of cybersecurity; negotiation, execution and participation in the implementation of international treaties or agreements on cybersecurity;

(c) Training, consultancy, and sharing of experience and enhancing professional and technical capacity in the sector of cybersecurity;

(d) Preventing and combating cybercrime, crimes using high technology; coordination in investigation of and dealing with breaches of law, cybercrime and crimes using high technology;

(dd) Research, development and transfer of technology, products, and technical solutions serving the protection of cybersecurity;

(e) Organizing international seminars and conferences and implementing programs and projects on international cooperation on cybersecurity;

(g) Undertaking other activities of international cooperation on cybersecurity.

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

(a) The Ministry of Public Security is responsible before the Government to preside over coordination in conducting international cooperation on cybersecurity;

(b) The Ministry of National Defence is responsible before the Government to conduct international cooperation on cybersecurity within the managerial scope of such ministry;

(c) The Ministry of Foreign Affairs is responsible to coordinate with the Ministry of Public Security and the Ministry of National Defence in conducting international cooperation on cybersecurity;

(d) The Prime Minister of the Government shall make a decision in a case where international cooperation on cybersecurity falls within the responsibility of a number of ministries and branches [line ministries];

(dd) Any other Ministry, line ministry or locality [wishing to] undertake activities of international cooperation on cybersecurity must first obtain a written opinion from the Ministry of Public Security prior to undertaking same.

Article 7 *Conduct which is strictly prohibited*

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

(a) Propaganda against the Socialist Republic of Vietnam comprises: distortion or defamation of the people's administrative authorities; psychological warfare, inciting an invasive war, causing division or hatred between [Vietnamese] ethnic groups, religions and people of all countries; insulting the [Vietnamese] people, the national flag, national emblem, national anthem, great men, leaders, famous people or national heroes;

(b) Distorting history, denying revolutionary achievements, destroying the national solidarity block, conducting offences against religion, gender discrimination or racist acts;

(c) Invented, slanderous or untruthful information infringing the honour, reputation or dignity of other people or causing damage to the lawful rights and interests of other agencies, organizations and individuals;

(d) Untruthful information causing confusion amongst the people, causing loss and damage to socio-economic activities, causing difficulties for the normal activities of State agencies or people performing their public duties [or] infringing the lawful rights and interests of other agencies, organizations and individuals; invented or untruthful information about products, goods, money, bonds, bills, Government bonds, cheques and other valuable papers; invented or untruthful information in the sectors of finance, banking, e-commerce, multi-level trading and securities.

2. Conducting the following acts in cyberspace:

(a) Organizing the activities of colluding, instigating, bribing, tricking, manipulating, training or drilling people to oppose the State of the Socialist Republic of Vietnam;

(b) Inciting, calling for, persuading, instigating, threatening or causing division, conducting armed activities or using violence to oppose the people's administrative authorities; calling for, persuading, instigating, threatening, or embroiling a mass/crowd of people to disrupt or oppose people [officials] conducting their official duties, or obstructing the activities of agencies or organizations causing instability to security and order;

(c) Appropriating, buying or selling, seizing, and/or intentionally disclosing information classified as State secret, work secrets, or business secrets; appropriating, buying or selling, seizing, and/or intentionally disclosing personal secrets, family secrets and private life [adversely] impacting on the honour, reputation, dignity and lawful rights and interests of agencies, organizations and individuals; intentionally eavesdropping, illegally recording in sound or images of conversations in cyberspace; disclosing information about civil cryptographic products, or information about customers legally using civil cryptographic products; or using or trading civil cryptographic products of unknown origin;

(d) Activities being prostitution, social evils or human or human body part trafficking; propagandizing cultural products which are lewd or depraved; inciting or promoting violence, depraved or deviant lifestyle, destroying the fine traditions and customs of the people, social ethics or health of the community;

(dd) Defrauding to appropriate assets; organizing gambling, gambling via the Internet; stealing international telecom charges on the Internet; disseminating, advertising or purchasing and selling goods or services on the list of those prohibited by law; and breaching copyright and intellectual property in cyberspace;

(e) Falsifying websites of agencies, organizations or individuals; forging, circulating, stealing, buying or selling, collecting or exchanging illegally credit card information, bank accounts, encrypted assets, or digital assets of other people; illegally issuing, providing or using payment means; falsifying papers of agencies or organizations;

(g) Using artificial intelligence or new technology to falsify videos, images or voice of other people contrary to law; creating, posting or distributing the information prescribed in clause 1 above;

(h) Illegally collecting, using, distributing, exchanging, transferring or trading personal information or data of another person;

(i) Guiding, inciting, enticing or activating other people to commit crime or conduct an act in breach of law;

(k) Conducting other acts in cyberspace by using IT or e-facilities to breach the law on national security, social order and safety.

3. Conducting a cyberattack, cyberterrorism, cyberespionage, cybercrime or crime using high technology; causing a cybersecurity incident, attacking, infringing, or hijacking the control of, or distorting, interrupting, stalling, paralyzing or destroying an information system.

4. Producing or putting into use tools, facilities, software or committing an act obstructing, disrupting the operation of a telecom network, the Internet, computer network, information systems, information processing and control systems or e-facilities; or distributing spam emails, spam text messages, spam calls, or informatics programs which harm same.

5. Illegally infiltrating a telecom network, computer network, information system, information processing and control system, database or e-facility of another person.

6. Opposing or obstructing the activities of cybersecurity protective forces; illegally attacking, disabling, or rendering ineffective any cybersecurity protective measures.

7. Abusing or misusing cybersecurity protective activities in order to infringe national sovereignty, interests or security, social order and safety or the lawful rights and interests of agencies, organizations and individuals, or for personal profit.

8. Other conduct in breach of this Law.

Chapter II

PROTECTION OF CYBERSECURITY OF INFORMATION SYSTEMS

Article 8 *Classification of information system levels*

1. An information system is classified into the following 5 levels based on the degree of damage to national security, social order and safety, or the lawful rights and interests of organizations and individuals, or public interests in the case of an incident [breakdown] or a breach of the law on cybersecurity:

   (a) [Information system at] level 1 which may harm the lawful rights and interests of organizations and individuals;

   (b) [Information system at] level 2 which may seriously harm the lawful rights and interests of organizations and individuals or harm public interests;

   (c) [Information system at] level 3 which may cause a particularly serious harm to the lawful rights and interests of organizations and individuals; or which may seriously harm public interests; or which may harm or seriously harm social order and safety or harm national security;

   (d) [Information system at] level 4 which may cause a particularly serious harm to public interests, social order and safety or may seriously harm national security;

   (dd) [Information system at] level 5 which may cause a particularly serious harm to national security.

2. The Government shall provide detailed regulations on criteria for determining information system levels; on the authority, sequence, and procedures for determining information system levels and on measures, responsibilities and obligations to ensure cybersecurity at each information system level.

Article 9 *Information systems critical for national security*

1. Information system critical for national security means an information system which plays a strategic and particularly important role in terms of politics, national defence, security, diplomacy, economy, and society, which if subject to an incident [breakdown] or a breach of the law on cybersecurity may cause harm to national security or serious harm to social order and safety and which is on the list subject to decision of the Prime Minister of the Government.

2. Information systems critical for national security shall be in the following sectors:

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

   (b) Information systems which store and process information classified as State secret;

   (c) Information systems serving the storage and preservation of objects and data of particular importance;

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

   (dd) Information systems serving preservation, manufacture and management of other particularly important material/physical facilities relevant to national security;

   (e) Important information systems serving the operation of central [State] agencies and organizations;

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

   (h) Automatic control and monitoring/surveillance systems in important construction works [or buildings] relevant to national security [or] targets critical for national security.

3. It is required to conduct cybersecurity evaluation of information systems critical for national security and to certify such information systems as satisfying cybersecurity conditions before putting them into operation and use; and regularly conduct cybersecurity inspection and supervision during the process of their use, and promptly respond to and remedy any cybersecurity incident.

4. The Ministry of Public Security shall preside over coordination with related ministries, line ministries, agencies, organizations and individuals to prepare and submit the list of information systems critical for national security to the Prime Minister of the Government for consideration and decision.

5. The Government shall provide detailed regulations on the criteria for determining information systems critical for national security.

Article 10 *Tasks and measures for protecting cybersecurity of information systems*

1. Tasks for protecting cybersecurity of information systems comprise:

   (a) Determining cybersecurity levels of information systems and information systems critical for national security;

   (b) Assessing and managing cybersecurity risks of information systems;

   (c) Expediting, supervising, and inspecting the work of protecting cybersecurity of information systems;

   (d) Organizing implementation of measures for protecting cybersecurity of information systems;

   (dd) Implementing reporting regimes in accordance with regulations;

   (e) Organizing dissemination of and increasing awareness of cybersecurity.

2. Measures for protecting cybersecurity of information systems comprise:

   (a) Issuing the regulations on ensuring cybersecurity during the design, building, management, operation, use, upgrade and decommission of information systems;

   (b) Evaluating cybersecurity of files and designs of information systems;

   (c) Assessing cybersecurity conditions for information systems;

   (d) Applying managerial measures in accordance with standards and technical regulations on cybersecurity, studying and establishing the national firewall system to prevent any threat of or remedy a cybersecurity incident;

   (dd) Organizing implementation of measures for storage and backup to protect cyberinformation security and security of elements constituting information systems;

   (e) Inspecting and supervising the compliance with regulations and assessing efficiency of the managerial and technical measures which have been applied;

   (g) Supervising cybersecurity;

   (h) Responding to and rectifying any cybersecurity incident for information systems.

3. The administrator of an information system at level 1 or 2 shall perform all of the tasks prescribed in clause 1 of this article and choose to apply the measures prescribed in clause 2 of this article based on the actual requirements or ability.

4. The administrator of an information system at level 3 or 4 which is not on the list of information systems critical for national security shall perform all of the tasks prescribed in clause 1 of this article, and the measures prescribed in sub-clauses (a), (d), (dd), (e), (g) and (h) of clause 2 of this article and choose to apply the measures prescribed in sub-clauses (b) and (c) of clause 2 of this article based on the actual requirements or ability.

5. The administrator of an information system on the list of information systems critical for national security shall perform all of the tasks and measures prescribed in clauses 1 and 2 of this article.

6. The Government shall provide detailed regulations on clauses 1 and 2 of this article.

Article 11 *Responsibilities to protect cybersecurity of information systems critical for national security*

1. The administrator of an information system critical for national security shall have the following responsibilities:

   (a) To comply with article 10.5 of this Law;

   (b) Upon establishment, expansion or upgrade of the information system critical for national security, to inspect cybersecurity prior to putting same into operation and exploitation; to annually self-inspect cybersecurity, and assess the conditions on cybersecurity of the information system critical for national security and to notify inspection results in writing before October each year to the authorized CTF;

   (c) To preside over coordination with the authorized CTF to regularly supervise cybersecurity; to formulate mechanisms for self-warning and receipt of warnings of cybersecurity threats; and to propose a plan on emergency response and remedy;

   (d) To formulate a plan to respond to and remedy cybersecurity incidents; to implement such plan upon occurrence of any cybersecurity incident and promptly report to the authorized CTF;

   (dd) To co-ordinate with the CTF to conduct a one-off inspection of cybersecurity.

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

   (a) To evaluate cybersecurity in respect of information systems critical for national security;

   (b) To assess and certify satisfaction of all cybersecurity conditions of information systems critical for national security;

   (c) To conduct one-off inspections of cybersecurity in respect of information systems critical for national security;

   (d) To supervise cybersecurity; to provide warnings and coordinate with information system administrators to remedy and deal with cybersecurity threats or cybersecurity incidents in respect of information systems critical for national security;

   (dd) To preside over coordination of activities of responding to and remedying any cybersecurity incident occurring on an information system critical for national security; to notify information system administrators of detection of a cyberattack or cybersecurity incident;

   (e) To preside over coordination of the Government Cipher Committee to implement measures for protection of information systems critical for national security by using cryptographic solutions or products provided by the Government Cipher Committee for protection of State secrets.

3. The Ministry of National Defence shall preside over evaluation of cybersecurity, assessment of cybersecurity conditions, one-off inspection of cybersecurity, supervision of cybersecurity and coordination of the activities of responding to and remedying cybersecurity incidents occurring within on the military information system managed by it.

4. The Government Cipher Committee shall preside over organizing implementation of the solution of use of cipher codes to protect State secrets in information systems critical for national security; evaluating cybersecurity, assessing cybersecurity conditions, conducting one-off inspections of cybersecurity, supervising cybersecurity and coordinating the activities of responding to and remedying cybersecurity incidents occurring within the cipher information system of the Government Cipher Committee.

Article 12 *Inspection of cybersecurity of information systems of agencies and organizations not on the list of information systems critical for national security****

1. An inspection of cybersecurity of an information system of an agency or organization not on the list of information systems critical for national security shall be conducted in the following cases:

   (a) When there is an act prescribed in clause 12, 13, 14 or 15 of article 2 of this Law;

   (b) When there is a request from the information system administrator.

2. Items subject to a cybersecurity inspection comprise:

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

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

   (c) Measures for protecting State secrets, and for preventing and combating revelation and loss of State secrets via technical channels.

3. An information system administrator is responsible to notify the CTF under the Ministry of Public Security upon discovery of any breach of the law on cybersecurity on the information system under the management of such administrator.

4. The CTF under the Ministry of Public Security shall conduct inspections of cybersecurity of information systems of agencies and organizations in the cases prescribed in clause 1 of this article. Results of cybersecurity inspection shall be kept confidential in accordance with law.

5. The Government shall stipulate the sequence and procedures for cybersecurity inspection as prescribed in this article.

Chapter III

PREVENTION OF AND DEALING WITH AN INFRINGEMENT OF CYBERSECURITY

Article 13 *Information and acts of using information technology and e-facilities to infringe national security and social order and safety in cyberspace*

1. Information with contents being propaganda against the State of the Socialist Republic of Vietnam, and inciting riots, disrupting security or causing public disorder comprises:

   (a) Propagating information and documents with contents distorting, slandering or defaming the people's administrative authorities;

   (b) [Creating] psychological warfare, inciting an invasive war; causing division or hatred between ethnic groups, religions and people of all countries;

   (c) Insulting the [Vietnamese] people, the national flag, national emblem, national anthem, great men, leaders, famous people or national heroes;

   (d) Calling for, mobilizing, instigating, threatening or causing division, conducting armed activities or using violence to oppose the people's administrative authorities;

   (dd) Calling for, mobilizing, inciting, threatening, or embroiling a mass/crowd of people to disrupt or oppose people [officials] conducting their official duties, or obstructing the normal activities of agencies or organizations causing instability to security and order;

   (e) Falsely or inaccurately reflecting national border lines and national sovereignty of Vietnam; publishing and transmitting misleading, inaccurate and incomplete images of the map of Vietnam or misrepresenting Vietnam's national sovereignty;

2. Information with contents undermining unity policies and socio-economic policies of the Socialist Republic of Vietnam comprises:

   (a) Causing conflicts and division among the people's classes or between the people and the people's administrative authorities, the people’s armed forces or socio-political organizations;

(b) Inciting, causing hatred, discrimination, division, or ethnic secession, or infringing upon the equality of ethnic communities in Vietnam;

(c) Inciting, causing conflicts and division between followers of a religion and non-religious persons or among followers of different religions, or causing division between religious believers and the people's administrative authorities, the people's armed forces or socio-political organizations;

(d) Sabotaging or obstructing the implementation of international unity policies;

(dd) Propaganda causing harm directly or indirectly to the lawfully rights and interests of the State in political, economic, social, and international reputation matters;

(e) Calling for or inciting actions which sabotage the implementation of socio-economic policies or cause obstruction to the implementation of such policies;

(g) Calling for or inciting actions which sabotage physical and technical facilities of the Socialist Republic of Vietnam.

3. Information with contents infringing upon the lawful rights and interests of organizations or individuals comprises:

(a) Disseminating distorted, fabricated, or untruthful information, which [adversely] affects the reputation or normal operations of an organization;

(b) Calling for, encouraging, or inciting the boycott of products, services, goods, brands, or trademarks of an organization or enterprise, which causes material or reputational damage to an organization or enterprise;

(c) Impersonating or falsifying information, images, or imitating products, trademarks, or brands of an organization or enterprise by using technological utilities, which [adversely] affects the reputation of an organization or enterprise;

(d) Insulting the honour, reputation, or dignity of another person;

(dd) Distorting the truth, which [adversely] affects the honour, reputation, or dignity of another person;

(e) Fabricating or disseminating information known to be false, which causes damage to the lawful rights and interests of another person;

(g) Making false accusations that another person has committed a crime and reporting him/her to a competent authority;

(h) Impersonating or falsifying an individual's information, image, or voice, which [adversely] affects his/her honour, reputation, or dignity.

4. Acts performed in cyberspace by using information technology and e-facilities to infringe national security and social order and safety comprise:

(a) Posting and/or disseminating information in cyberspace with the contents prescribed in clauses 1, 2 and 3 of this article;

(b) Conducting any act prescribed in article 15.1 of this Law;

(c) Appropriating assets/property; organizing gambling or gambling via the Internet; stealing international telecom charges on the Internet; and breaching copyright and intellectual property in cyberspace;

(d) Falsifying websites of agencies, organizations or individuals; forging, circulating, stealing, buying or selling, collecting or exchanging illegally credit card information or bank accounts of other people; unlawfully issuing, providing or using payment means; forging seals, other documents or papers of agencies or organizations;

(dd) Illegally propagating, advertising, purchasing and selling weapons, explosive materials, supporting tools, firecrackers; narcotics, drug precursors, addictive substances, psychoactive substances; wildlife, endangered, precious and rare animals and other goods and services on the list of those prohibited by law; procuring; disseminating obscene cultural products; sexually abusing children; or committing sexual harassment;

(e) Setting up, providing services or supporting operation, business, trading, purchase and sale, and marketing online for illegal trading floors, websites, and applications in cyberspace, including: e-commerce floors, websites, selling applications, provision of e-commercial services; commodity index-based trading floors; digital asset trading floors or multi-level business;

(g) Using fake identities, fake documents or files or illegally using information of another person to establish an enterprise or set up and register a bank account, securities account, insurance account, tax account and other digital account; illegally collecting, storing, exchanging, purchasing, selling, giving, and publicly disclosing data, information about bank accounts, bank cards, e-wallet accounts, securities accounts, insurance accounts, tax accounts and other types of digital accounts;

(h) Advertising or trading counterfeit products, illegally imported goods or goods of unknown source or origin; goods circulated domestically subject to emergency measures; expired goods;

(i) Guiding other people to conduct acts in breach of law;

(k) Other acts conducted in cyberspace by using IT or e-facilities to breach the law on national security, social order and safety.

Article 14 *Prevention of and dealing with information and acts of using IT or e-facilities to infringe national security, and social order and safety in cyberspace*

1. Information system administrators, and domestic and foreign enterprises providing services on telecom networks and the Internet, and added value services in cyberspace are responsible to implement managerial and technical measures in order to prevent, detect, stop and/or remove information with the contents prescribed in clauses 1 to 3 of article 13 of this Law on the information systems within the managerial scope or when there is a request from the CTF.

2. The CTF and competent agencies shall apply the measures prescribed in article 5.1 of this Law to deal with information in cyberspace with the contents prescribed in clauses 1 to 3 of article 13 of this Law and combat and prevent acts of using IT or e-facilities to infringe upon national security, and social order and safety in cyberspace.

3. Domestic and foreign enterprises providing services on telecom networks and the Internet, and added value services in cyberspace, and information system administrators shall coordinate with the CTF to deal with information in cyberspace with the contents prescribed in clauses 1 to 3 of article 13 of this Law and prevent acts of using IT or e-facilities to infringe upon national security, and social order and safety in cyberspace.

4. Organizations and individuals who compile, publish and disseminate information in cyberspace with the contents prescribed in clauses 1 to 3 of article 13 of this Law must remove such information when so requested by the CTF and shall be liable [for same] in accordance with law.

5. The Government shall provide detailed regulations on this article.

Article 15 *Prevention of and combatting cyberespionage; and protection of information classified as State secrets, work secrets, business secrets, personal secrets, family secrets and private life in cyberspace*

1. Conduct constituting cyberespionage; and infringement of State secrets, work secrets, business secrets, personal secrets, family secrets or private life in cyberspace comprises:

(a) Appropriating, buying or selling, seizing and/or intentionally disclosing information classified as State secrets, work secrets, or business secrets; appropriating, buying or selling, seizing and/or intentionally disclosing personal secrets, family secrets or private life [adversely] impacting on the honour, reputation, dignity and lawful rights and interests of agencies, organizations and individuals;

(b) Deliberately deleting, damaging, misplacing and/or changing information classified as State secrets, work secrets, business secrets, personal secrets, family secrets and private life which are transmitted and/or stored in cyberspace;

(c) Deliberately altering, cancelling or invalidating technical measures which have been established and/or applied in order to protect information classified as State secrets, work secrets, business secrets, personal secrets, family secrets or private life;

(d) Putting in cyberspace information being State secrets, work secrets, business secrets, personal secrets, family secrets or private life contrary to law;

(dd) Deliberately listening to or recording conversations in sound or images contrary to law;

(e) Other acts of intentional infringement of State secrets, work secrets, business secrets, personal secrets, family secrets or private life.

2. Information system administrators have the following responsibilities:

(a) To inspect [audit] cybersecurity in order to detect and remove malicious codes and malicious hardware and to remedy security weaknesses and vulnerabilities; and to detect, prevent and deal with unlawful infringement activities or other threats to cybersecurity;

(b) To implement managerial and technical measures in order to prevent, detect and block any acts of cyberespionage, infringements of State secrets, work secrets, business secrets, personal secrets, family secrets or private life on the information system and to promptly remove any information related to such conduct;

(c) To coordinate with the CTF and implement its request for prevention and combatting cyberespionage and in order to protect information classified as State secrets, work secrets, business secrets, personal secrets, family secrets or private life on the information system.

3. Agencies or organizations compiling and storing information and data classified as State secrets are responsible to protect such State secrets which have been compiled and stored on computers or other equipment or exchanged in cyberspace, in accordance with the law on protection of State secrets.

4. The Ministry of Public Security has the following responsibilities, except for those prescribed in clauses 5 and 6 of this article:

(a) To inspect [audit] cybersecurity of information systems critical for national security in order to detect and remove malicious codes and malicious hardware, to remedy security weaknesses and vulnerabilities; and to discover, prevent and deal with unlawful acts of infringement;

(b) To inspect cybersecurity of communications equipment, products and services, digital equipment and of e-equipment prior to commissioning same for use on information systems critical for national security;

(c) To supervise cybersecurity of information systems critical for national security in order to detect and deal with activities of unlawfully gathering information classified as State secret;

(d) To detect and deal with unlawful acts of posting, storing or exchanging in cyberspace information and data containing contents classified as State secret;

(dd) To participate in research and manufacture of products which store and transmit information and data with contents classified as State secret in accordance with law, and products which code

information in cyberspace in accordance with the functions and duties allocated [to such Ministry];

(e) To check and inspect the work of State agencies protecting State secrets in cyberspace and the work of cybersecurity protection by administrators of information systems critical for national security;

(g) To arrange training courses to raise the awareness of and knowledge on protection of State secrets in cyberspace, and on prevention of and combatting cyberattacks, and on cybersecurity protection for the cybersecurity protective forces prescribed in article 30.1 of this Law.

5. The Ministry of National Defence is responsible to implement the items prescribed in clause 4 of this article with respect to military information systems.

6. The Government Cipher Committee is responsible to comply with clause 4 of this article with respect to the cipher information system of the Government Cipher Committee; and is responsible to arrange implementation of provisions of the law on use of cryptography in order to protect information classified as State secret which is stored and exchanged in cyberspace.

Article 16 *Prevention of and combating child abuse in cyberspace*

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

2. If a child uses added value services in cyberspace, then the parent or guardian as prescribed in the civil law shall register an account with the information of the parent or guardian and be responsible to supervise and manage the contents which are accessed, posted and shared on such service platforms by the child.

3. Information system administrators or enterprises providing services on telecom networks, the Internet, or added value services in cyberspace are responsible:

(a) To control information on [their] information systems or on services provided by such enterprises in order not to harm or maltreat children or not to infringe upon children's rights;

(b) To block the sharing of and to delete information with the contents which harm or maltreat children or infringe upon their rights;

(c) To set up and deploy technical systems to support the blocking of contents which maltreat children in cyberspace;

(d) To coordinate with agencies, organizations and enterprises in preventing the sources of disseminating information which maltreat children in cyberspace;

(dd) To promptly notify and coordinate with the CTF under the Ministry of Public Security for resolution.

4. Agencies, organizations and individuals participating in activities in cyberspace are responsible to co-ordinate with competent agencies to guarantee children's rights in cyberspace; and prevent and combat child maltreatment in cyberspace.

5. Agencies, organizations, parents, guardians, teachers, child carers and other relevant individuals are responsible to guarantee children's rights and to protect children in accordance with the law on children and this Law when they [the former] participate in cyberspace.

6. The CTF and functional agencies are responsible to take measures to preclude, discover, prevent and strictly deal with the use of cyberspace to harm and/or maltreat children or to infringe upon children's rights.

Article 17 *Preclusion, discovery, prevention of and dealing with malicious software*

1. Agencies, organizations, and individuals are responsible to proactively preclude, discover, and prevent malicious software and to comply with instructions and requirements of the competent State agencies.

2. Administrators of information systems critical for national security shall deploy technical systems in order to promptly preclude, discover, prevent and deal with malicious software.

3. Organizations and enterprises providing services of emails, transmission, and storage of information must have a malicious software filtering system in the process of sending, receiving, and storing information on their own systems and must report same to the competent State agencies in accordance with law.

4. Enterprises providing Internet services shall take measures to manage, preclude, discover, and prevent the dissemination of malicious software and deal with same at the request of competent State agencies.

5. The Ministry of Public Security shall preside over coordinating with the Ministry of National Defence and relevant ministries and line ministries to organize preclusion, discovery, prevention of and dealing with malicious software which causes harm to national security.

Article 18 *Prevention of and combating cyberattacks*

1. Acts constituting a cyberattack and cyberattack-related acts comprise:

   (a) Distributing informatics programs which cause harm to a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility;

   (b) Hindering, disordering, paralyzing, interrupting or stalling the operation of, and/or illegally preventing the transmission of data by cyberspace;

   (c) Infiltrating, harming or appropriating data stored on or transmitted via a telecom network, the Internet, a computer network, information system, information processing and control systems, database or e-facility;

   (d) Infiltrating, creating or exploiting security vulnerabilities or weaknesses and system services in order to appropriate information and/or to earn illicit profit;

   (dd) Producing, purchasing and selling, exchanging or donating tools, devices [equipment] and software with the function of harming a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility in order to use such objects [tools, devices and software] for illegal purposes;

   (e) Performing other acts which [adversely] affect the normal operation of any telecom network, the Internet, computer network, information system, information processing and control system, database or e-facility.

2. Information system administrators are responsible to apply technical measures to prevent and avoid the acts prescribed in sub-clauses (a), (b), (c), (d) and (e) of clause 1 above with respect to information systems within their managerial scope.

3. When a cyberattack occurs and infringes or threatens to infringe national sovereignty, interest and security and/or causes serious harm to social order and safety, the CTF shall preside over coordination with information system administrators and relevant organizations and individuals to apply measures to determine the origin of the cyberattack and collect evidence; and shall require enterprises providing services on telecom networks, the Internet and other added value services on cyberspace [cyberspace service providers] to block and filter information in order to prevent and eliminate acts of cyberattack, and shall promptly provide complete relevant information and data.

4. The responsibility to prevent and combat cyberattack is regulated as follows:

(a) The Ministry of Public Security shall preside over coordination with relevant ministries, line ministries and localities to prevent, detect and deal with the acts prescribed in clause 1 of this article which infringe or threaten to infringe national sovereignty, interests and security or cause serious harm to social order and safety throughout the entire country, except in the cases prescribed in sub-clauses (b) and (c) below;

(b) The Ministry of National Defence shall preside over coordination with relevant ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to military information systems;

(c) The Government Cipher Committee shall preside over coordination with relevant ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to cipher information systems under such Committee.

Article 19 *Prevention of and combating cyberterrorism*

1. Competent State agencies are responsible to apply measures stipulated in this Law and the law on prevention of and combating against terrorism, to deal with cyberterrorism.

2. Information system administrators shall regularly review and inspect information systems within their managerial scope in order to eliminate cyberterrorism threats.

3. Any agency, organization or individual which detects any indication or any act of cyberterrorism must promptly notify a cybersecurity protective force thereof. An agency receiving such notice is responsible to receive complete/full news of such cyberterrorism and promptly notify same to the CTF.

4. The Ministry of Public Security shall preside over coordination with relevant ministries and line ministries to implement the prevention of and combating against cyberterrorism, to apply measures to neutralize cyberterrorism sources, to deal with cyberterrorism, and to minimize consequences occurring to information systems, except in the cases prescribed in clauses 5 and 6 of this article.

5. The Ministry of National Defence shall preside over coordination with relevant ministries and line ministries to implement the prevention of and combating against cyberterrorism, to apply measures to neutralize cyberterrorism sources, to deal with cyberterrorism, and to minimize consequences occurring to military information systems.

6. The Government Cipher Committee shall preside over coordination with relevant ministries and line ministries to prevent and combat cyberterrorism, and to apply measures to neutralize cyberterrorism sources, to deal with cyberterrorism, and to minimize consequences occurring to cipher information systems under such Committee.

Article 20 *Prevention of and dealing with dangerous cybersecurity situations*

1. Dangerous cybersecurity situations comprise:

(a) The presence of inciting information in cyberspace resulting in possible occurrence of riots, security disruption or terrorism;

(b) Attack on information systems critical for national security;

(c) Attack on a number of information systems on a large scale and of high strength;

(d) Attack on networks for the purpose of destroying important construction works regarding national security and important targets regarding national security;

(dd) Cyberattacks which seriously infringe national sovereignty, interest and security; or which cause particularly serious harm to social order and safety and the lawful rights and interests of agencies, organizations and individuals.

2. The responsibility to prevent dangerous cybersecurity situations is regulated as follows:

(a) The Cybersecurity Task Force shall coordinate with administrators of information systems critical for national security to implement technical solutions and professional activities to prevent, detect and deal with dangerous cybersecurity situations;

(b) Telecom, Internet and IT enterprises, enterprises providing services on telecom networks, the Internet and other added value services on cyberspace and relevant agencies, organizations and individuals are responsible to coordinate with the CTF under the Ministry of Public Security in preventing, detecting and dealing with dangerous cybersecurity situations.

3. The measures to deal with a dangerous cybersecurity situation comprise:

(a) Immediately implementing emergency plans for prevention and response regarding cybersecurity, and preventing, excluding or mitigating loss and damage caused by such dangerous situation;

(b) Sending a notice to relevant agencies, organizations and individuals;

(c) Collecting relevant information; and continuous monitoring and supervision of such dangerous situation;

(d) Analysing and assessing information about and forecasts of possible impact and the scope of impact and the level of loss and damage caused by such dangerous situation;

(dd) Ceasing provision of network information in specific areas or disconnecting international network gateways;

(e) Arranging forces and equipment to prevent and eliminate such dangerous situation;

(g) Other measures as stipulated in the *Law on National Security*.

4. A dangerous cybersecurity situation shall be dealt with as follows:

(a) Any agency, organization or individual which discovers a dangerous cybersecurity situation must promptly notify the CTF and immediately apply the measures prescribed in sub-clauses (a) and (b) of clause 3 above;

(b) The Prime Minister of the Government shall consider and make a decision on, or authorize the Minister of Public Security to consider and make a decision on dealing with any dangerous cybersecurity situation throughout the entire country or in each locality or for a specific target.

The Prime Minister of the Government shall consider and make a decision on, or authorize the Minister of National Defence to consider and make a decision on dealing with any dangerous cybersecurity situation occurring to military information systems and cipher information systems under the Government Cipher Committee;

(c) The CTF shall preside over coordination with relevant agencies, organizations and individuals to apply the measures prescribed in clause 3 above to deal with any dangerous cybersecurity situation;

(d) Relevant agencies, organizations and individuals are responsible to coordinate with the CTF to implement measures to prevent and deal with any dangerous cybersecurity situation.

Article 21 *Fighting to protect cybersecurity*

1. *Fighting to protect cybersecurity* means an organized activity conducted by a CTF in cyberspace in order to protect national security and ensure social order and safety.

2. Items of fighting to protect cybersecurity comprise:

(a) Supervising cyberinformation and preventing, combating and dealing with any organization or individual engaged in the use of cyberspace to infringe national security, social order and safety;

(b) Using technical solutions to prevent information in breach of law;

(c) Preventing and combating attacks, and protecting the stable operation of information systems critical for national security;

(d) Paralyzing or restricting the use of cyberspace when such use causes harm to national security or causes particularly serious harm to social order and safety;

(dd) Proactively attacking and neutralizing targets in cyberspace in order to protect national security and ensure social order and safety.

3. The Ministry of Public Security shall preside over coordination with relevant ministries and line ministries in fighting to protect cybersecurity; the Ministry of National Defence shall preside over coordination with relevant ministries and line ministries in fighting to protect cybersecurity of military information systems.

Article 22 *Prevention of conflicts of information in cyberspace*

1. *Conflict of information* means the use of information technological and technical measures by two or more domestic and foreign organizations to cause harm to any information and/or information system in cyberspace, [adversely] impacting on national security, and social order and safety.

2. *Prevention of conflict of information in cyberspace* means the implementation of technological and technical measures to supervise, discover, warn, identify origins, block and filter, remove, refute, shape public opinion, remedy, and impose a penalty and other measures to preclude any conflict of information in cyberspace.

3. Organizations and individuals shall, within the scope of their duties and powers, have the following responsibilities:

(a) To prevent conflicts of information in cyberspace from their information systems; cooperate to identify sources, repel cyberattacks and remedy consequences of cyberattacks conducted through information systems of domestic and foreign organizations and individuals;

(b) To prevent activities of domestic and foreign organizations and individuals which aim at creating conflicts of information in cyberspace;

(c) To preclude domestic and foreign organizations and individuals from organizing the posting and dissemination of information in cyberspace which causes serious impact on national defence, national security, and social order and safety.

4. The Government shall provide detailed regulations on this article.

Chapter IV

CYBERSECURITY PROTECTIVE ACTIVITIES

Article 23 *Implementation of cybersecurity protective activities in State agencies, political organizations and socio-political organizations at the central and local levels*

1. Contents of implementation of cybersecurity protective activities comprise:

(a) Formulating and completing rules and regulations on use of local computer networks and Internet-connected computer networks; plans for ensuring cybersecurity of information systems; and plans for responding to and remedying cybersecurity incidents;

(b) Applying and implementing plans, measures and technology to protect cybersecurity of information systems and of information and data archived, drafted and transmitted on information systems within the scope of their managerial authority [managed by such State agencies and political organizations];

(c) Organizing retraining on cybersecurity knowledge for cadres [senior officials], other officials and employees; increasing the capability of cybersecurity protective forces to protect cybersecurity;

(d) Protecting cybersecurity in the following activities: providing public services in cyberspace; providing information to, exchanging information with and collecting information from agencies, organizations and individuals, sharing information internally and with other agencies or during other activities in accordance with Government regulations;

(dd) Conducting investment in and building physical infrastructure in conformity with conditions for ensuring implementation of cybersecurity protective activities for information systems;

(e) Inspecting cybersecurity of information systems; preventing and combating breaches of the law on cybersecurity; responding to and remedying cybersecurity incidents.

2. Heads of agencies and organizations are responsible to carry out cybersecurity protective activities within the scope of their managerial authority.

Article 24 *Protection of cybersecurity of national cyberspace infrastructure and international network gateways*

1. The protection of cybersecurity of the national cyberspace infrastructure and international network gateways must closely combine requirements on cybersecurity protection with requirements on socio-economic development; international network gateways are encouraged to be located within the territory of Vietnam; and organizations and individuals are encouraged to participate in investment in building national cyberspace infrastructure.

2. Agencies, organizations and individuals managing and exploiting national cyberspace infrastructure and international network gateways have the following responsibilities:

(a) To protect cybersecurity within their managerial authority; to be subject to management, investigation and inspection by, and to comply with requirements on cybersecurity protection of competent State agencies;

(b) To facilitate and implement necessary technical measures and professional activities when requested in order for competent State agencies to perform cybersecurity protective tasks.

Article 25 *Assurance of cyberinformation security*

1. Websites, portals or specialized pages on social media of agencies, organizations and individuals must not provide, upload or transmit any information with the contents prescribed in clauses 1 to 3 of article 13 and article 15.1 of this Law and other information containing contents infringing national security.

2. Any domestic or foreign enterprise providing services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam has the following responsibilities:

(a) To authenticate information when a user registers a digital account; to maintain confidentiality of information and accounts of users; to provide user information to the CTF under the Ministry of Public Security no later than 24 hours after the time of a written request or email, phone call or other communication forms as confirmed in order to serve verification, investigation of and dealing with breaches of the law on cybersecurity; in an emergency case where there is a threat of infringement of national security or threat of human life, it is required to provide information no later than 3 hours;

(b) To prevent the sharing of information, to delete information, and to remove services and applications with the contents in breach of this Law no later than 24 hours after the time of a request from the CTF under the Ministry of Public Security, and to save system logs in order to serve verification, investigation of and dealing with breaches of the law on cybersecurity within a [specified] period stipulated by law; in an emergency case where there is a threat of infringement of national security, it is required to block and delete information no later than 6 hours;

(c) Not to provide or to cease provision of services on telecom networks and on the Internet and value added services to organizations and individuals who upload in cyberspace information with the contents prescribed in clauses 1 to 3 of article 13, or clauses 1 and 2 of article 14 of this Law, when requested by the CTF under the Ministry of Public Security;

(d) To store personal information of service users, and data created by service users comprising: account name, period of use of services, payment information for service use fees, access IP address and other relevant data within a [specified] period stipulated by law after users terminate their use of services.

3. Domestic and foreign enterprises providing services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying out activities of collecting, exploiting [using], analysing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must apply data protective measures in accordance with law and store such data in Vietnam for a [specified] period stipulated by the Government.

Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam.

4. The Government shall provide detailed regulations on clauses 2 and 3 of this article.

Article 26 *Assurance of data security*

1. *Assurance of data security* means a total of technical, organizational and legal measures to protect data and to prevent and fight against infringement of data security.

2. The contents of assurance of data security comprise:

(a) Formulating policies and setting up procedures for assurance of data security;

(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 mechanisms for closely controlling personnel directly involved in data processing;

(dd) Periodically inspecting and assessing risks in order to promptly discover, prevent and deal with threats of data security;

(e) Inspecting and assessing cross-border data transmission; conditions for ensuring data security in information systems critical for national security, databases, data centres, and data storage systems;

(g) Other contents stipulated by law.

3. The Government shall provide detailed regulations on clause 2 of this article and on the responsibility to ensure data security.

Chapter V

STANDARDS AND TECHNICAL REGULATIONS, CYBERSECURITY PRODUCTS AND SERVICES

Article 27 *Standards and technical regulations on cybersecurity*

1. Cybersecurity standards and cybersecurity technical regulations shall apply to information systems, hardware, software, systems for management and operation of cybersecurity, cybersecurity products and services, information technology and network connection devices.

2. The certification of compliance with regulations on cybersecurity, announcement of compliance with regulations on cybersecurity, certification of conformity with standards on cybersecurity, and

announcement of conformity with standards on cybersecurity shall be implemented in accordance with the law on standards and technical regulations.

3. The assessment of compliance with regulations or conformity with standards on cybersecurity to serve information systems critical for national security and serve the State administration of cybersecurity shall be implemented at an organization certifying such compliance or conformity as designated by the Minister of Public Security.

4. The Ministry of Public Security has the following responsibilities:

   (a) To formulate draft national standards on cybersecurity;

   (b) To manage the quality of cybersecurity products and services, except for civil cryptography products and services;

   (c) To register, appoint and manage activities of cybersecurity conformity certification organizations, except for cases prescribed in clause 6 of this article.

5. The Minister of Public Security shall issue the national technical regulations on cybersecurity.

6. The Ministry of National Defence shall register, appoint and manage activities of cybersecurity conformity certification organizations in the military sector.

   The Government Cipher Committee shall assist the Minister of National Defence in managing the quality of civil cryptography products and services; and registering, appointing and managing activities of cybersecurity conformity certification organizations with respect to civil cryptography products and services.

Article 28 *Cybersecurity products and services*

1. Cybersecurity products comprise:

   (a) Civil cryptography products;

   (b) Cybersecurity inspection and assessment products;

   (c) Cybersecurity supervision products;

   (d) Anti-attack and anti-intrusion products;

   (dd) Other cybersecurity products.

2. Cybersecurity services comprise:

   (a) Services of inspection and assessment of cybersecurity;

   (b) Information security services not using civil cryptography;

   (c) Civil cryptography services;

   (d) Cybersecurity consultancy services;

   (dd) Cybersecurity supervision services;

   (e) Cybersecurity incident response services;

   (g) Data recovery services;

   (h) Services of preventing and fighting cyberattacks;

   (f) Other cybersecurity services.

3. The Government shall provide detailed regulations on this article.

Article 29 *Business of cybersecurity products and services*

1. Enterprises conducting business of cybersecurity products and services must have licences for business of cybersecurity products and services.

2. An enterprise conducting business of cybersecurity products and services shall have the following responsibilities:

   (a) To correctly implement the licence for business of cybersecurity products and services; to comply with the law on cybersecurity and other relevant laws;

   (b) To ensure that the quality of cybersecurity products and services conforms with the applicable standards which are announced and corresponding technical regulations in accordance with the law on the quality of products and goods and the law on standards and technical regulations before circulation in the market;

   (c) To prepare, store and maintain confidentiality of information of customers, and to manage files and documents on technical and technological solutions of products, and on the provision of services in accordance with law;

   (d) To refuse to provide cybersecurity products and services [to any organization or individual] when discovering that the organization or individual has committed a breach of the law on use of cybersecurity products and services, or a breach of the agreed commitments on use of products and services provided by the enterprise;

   (dd) To coordinate with, facilitate and comply with requirements of the CTF to implement cybersecurity protective measures.

3. The Government shall provide regulations on issuance, temporary suspension, and revocation of licences for business of cybersecurity products and services; on import and export of cybersecurity products; and on business of cybersecurity products and services.

Chapter VI

FORCES AND CONDITIONS FOR ENSURING CYBERSECURITY

Article 30 *Cybersecurity protective forces*

1. Cybersecurity protective forces comprise:

   (a) Cybersecurity Task Forces [CTFs] to be arranged under the Ministry of Public Security and the Ministry of National Defence;

   (b) Other cybersecurity protective forces to be arranged under ministries, line ministries, provincial people's committees, agencies and organizations which directly manage information systems critical for national security;

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

2. The Government shall provide detailed regulations on clause 1 of this article; and regulations on the coordination among cybersecurity protective forces.

Article 31 *Assurance of cybersecurity protective human resources*

1. The State shall train and develop cybersecurity protective human resources, ensuring [satisfaction of the requirements on] quantity and quality, and satisfaction of the requirements on capability to protect national security.

2. CTFs shall be given priority for personnel arrangement according to work positions and title standards, and shall be subject to mechanisms for recruitment, admission, employment, training, retraining, compensation, and talent attraction in accordance with special policies stipulated by the Government.

3. Administrators of information systems critical for national security shall have the following responsibilities:

(a) To arrange specialized departments or personnel appropriate to the protective level of the system;

(b) To ensure that persons performing cybersecurity duties satisfy criteria on professional qualifications and expertise;

(c) To regularly organize retraining and update skills for teams of personnel involved in operation, supervision, response to and dealing with network incidents.

Article 32 *Selection, training and development of cybersecurity protective forces*

1. Any Vietnamese citizen who satisfies all the standards on ethics, health, [professional] qualifications and knowledge of cybersecurity and IT, and who expresses readiness may be selected to join cybersecurity protective forces.

2. Priority shall be given to training and development of high-quality cybersecurity protective forces; and discovery of young talents in cybersecurity and IT for the purpose of educational orientation, selection, attraction and employment in the sector of cybersecurity.

3. Priority shall be given to development of cybersecurity training establishments which satisfy international standards; and it is encouraged to promote association of, and create opportunities for co-operation on cybersecurity between the State sector and the private sector both domestic and foreign.

Article 33 *Education and retraining on cybersecurity knowledge and activities*

1. Contents of education and retraining on cybersecurity knowledge shall be presented in the subject of national defence and security taught at schools and in programs on retraining on national defence and security knowledge in accordance with the Law on Education on National Defence and Security.

2. The Ministry of Public Security shall preside over co-ordination with relevant ministries and branches to organize retraining on cybersecurity activities for cybersecurity protective forces and for State officials, staff and employees who participate in protecting cybersecurity.

   The Ministry of National Defence and the Government Cipher Committee shall organize retraining on cybersecurity activities for entities within their managerial scope.

Article 34 *Training on advanced cybersecurity knowledge and skills*

1. Cybersecurity protective forces stipulated in sub-clauses (a) and (b) of article 30.1 of this Law must satisfy the requirements on advanced cybersecurity knowledge and skills.

2. Persons directly administering and operating information systems at levels 3, 4 and 5 in State agencies, organizations and enterprises must be trained on advanced cybersecurity knowledge and skills and be issued with certificates, except for individuals having undertaken specialized training on cybersecurity.

3. The Ministry of Public Security shall preside over coordination with relevant ministries and line ministries to organize training on advanced cybersecurity knowledge and skills, except for the case prescribed in clause 4 below.

4. The Ministry of National Defence and the Government Cipher Committee shall organize training on advanced cybersecurity knowledge and skills for entities within their managerial scope.

5. The Government shall stipulate standards on advanced cybersecurity knowledge and skills; and programs, contents and certification of training on advanced cybersecurity knowledge and skills.

Article 35 *Dissemination of knowledge about cybersecurity*

1. The State formulates policies for dissemination of knowledge about cybersecurity throughout the entire country and encourages State agencies to coordinate with private organizations and individuals to implement educational programs and to increase awareness of cybersecurity; and prioritizes the dissemination and provision of guidance to children, the elderly, and people having cognitive difficulties to increase the ability to self-protect their lawful rights and interests in cyberspace.

2. Ministries, branches, agencies and organizations are responsible to formulate and implement activities of disseminating cybersecurity knowledge to their cadres, officials, staff and employees.

3. Provincial people's committees are responsible to formulate and implement activities of disseminating knowledge about, and increasing awareness of cybersecurity for local agencies, organizations and individuals.

Article 36 *Research and development of cybersecurity*

1. Contents of research and development of cybersecurity comprise:

   (a) Establishment of systems of cybersecurity protective software and equipment;

   (b) Methods of evaluating whether cybersecurity protective software and equipment satisfy standards, and minimizing the existence of security vulnerabilities or weaknesses, and malware;

   (c) Methods of checking whether the hardware and software which is provided in fact functions properly;

   (d) Methods of protecting State secrets, work-related secrets, business secrets, personal secrets, family secrets and private life [personal privacy], and the capability of maintaining confidentiality when transmitting information in cyberspace;

   (dd) Determination of the sources of information transmitted in cyberspace;

   (e) Resolution of cybersecurity threats;

   (g) Establishment of the network range and the cybersecurity testing environment;

   (h) Technical initiatives increasing cybersecurity awareness and skills;

   (i) Cybersecurity forecasts;

   (k) Practical research and theoretical development of cybersecurity.

2. Relevant agencies, organizations and individuals have the right to research and develop cybersecurity.

Article 37 *Improvement of self-autonomy regarding cybersecurity*

1. The State encourages and facilitates agencies, organizations and individuals to improve their self-autonomy regarding cybersecurity and to increase the productivity, inspection, assessment and testing of digital devices, network services and network applications.

2. The Government shall implement the following measures in order to improve self-autonomy of agencies, organizations and individuals regarding cybersecurity:

   (a) Directing the formulation of policies, strategies, and planning for development of cybersecurity industry; standards and technical regulations with respect to hardware and software products to proactively preclude cybersecurity threats right from the formation of products.

   (b) Promoting transfer, research, control [ability to master/own] and development of technology, products, services of cybersecurity industry;

   (c) Promoting application of new technology and advanced technology relating to cybersecurity;

   (d) Organizing training, developing and optimizing use [employment] of high-quality cybersecurity human resources;

(dd) Strengthening the business environment, improving competitive conditions, and assisting enterprises to research and produce products, services and applications for the purpose of cybersecurity protection.

3. Activities of investment in and attracting resources for development of infrastructure of cybersecurity industry comprise:

(a) Activities of investment in construction of infrastructure of cybersecurity industry are industries and trades entitled to special investment incentives or entitled to incentives and support in accordance with the laws on investment, tax, land and other relevant laws;

(b) The State prioritizes arrangement of budget capital sources to make investment in construction of infrastructure of cybersecurity industry, comprising: establishments for research, design, production, and testing of cybersecurity products and services; major national laboratories for cybersecurity; establishments for calibration, testing and assessment of cybersecurity products and services; big data centres; centralized cybersecurity industrial zones; and cybersecurity industrial complexes;

(c) Infrastructure of cybersecurity industry invested by the State as prescribed in sub-clause (b) above is one type of infrastructure asset and is managed, exploited and operated in accordance with the law on management and use of public assets;

(d) Organizations and enterprises are permitted to import technology lines, equipment, machinery, and tools serving the activities of training, research and development of cybersecurity products and services;

(dd) State agencies, organizations and enterprises prioritize the use of cybersecurity products and services which are produced domestically.

4. The Ministry of Public Security shall advise and assist the Government to build and develop infrastructure of cybersecurity industry in order to improve self-autonomy of cybersecurity.

Article 38 *Funds for cybersecurity protective activities*

1. State agencies, organizations and enterprises, political organizations, socio-political organizations and public professional units guaranteed by the State budget must arrange funds for cybersecurity protection in their annual expenditure estimates for implementation of the duties of digital transformation and information technology application; and arrange at least 15% of the total funds for implementing programs, schemes and projects for investment in digital transformation, and information technology application to protect cybersecurity.

2. Agencies, organizations and units other than those stipulated in clause 1 above shall guarantee funds for cybersecurity protection on their own.

Chapter VII

RESPONSIBILITIES OF AGENCIES, ORGANIZATIONS AND INDIVIDUALS FOR CYBERSECURITY

Article 39 *Responsibilities for State administration of cybersecurity*

1. The Government shall exercise uniform State administration of cybersecurity.

2. The Ministry of Public Security is a coordinating agency to assist the Government to exercise State administration of cybersecurity; and liable before the Government to implement the following contents of State administration of cybersecurity, except for the contents prescribed in clauses 3 and 4 below:

(a) To promulgate or submit to the competent State agency to promulgate legal instruments on cybersecurity;

(b) To formulate and propose strategies, guidelines, policies, plans and options for cybersecurity protection; to study, establish, develop and use security cryptography to protect data security within the managerial scope of the Ministry of Public Security;

(c) To coordinate with related agencies to organize dissemination, and refute information with contents opposing the State of the Socialist Republic of Vietnam as prescribed in article 13.1 of this Law;

(d) To request enterprises providing services on telecom networks, the Internet, and other added value services in cyberspace, and administrators of information systems to remove any information with contents breaching the law on cybersecurity on the services or information systems directly managed by the enterprises, agencies or organizations;

(dd) To prevent and combat the use of cyberspace to infringe national sovereignty, interest and security, social order and safety; and to prevent and combat cybercrime;

(e) To ensure security of information in cyberspace, and data security; to formulate mechanisms to manage IP address identification; to authenticate information [used to] register digital accounts; to give warnings and to share information on cybersecurity and cybersecurity threats;

(g) To advise and make a proposal to the Government and the Prime Minister for consideration and decision on allocation and co-ordination to implement measures for cybersecurity protection and to prevent or deal with any cybersecurity infringement if the contents of State administration relate to the managerial scope of multiple ministries and branches;

(h) To mobilize experts, scientists, State officials with advanced knowledge and to expropriate systems, facilities, and equipment in a case of emergency to protect national security, and ensure social order and safety in cyberspace;

(i) To organize drills to prevent and combat cyberattacks; to carry out drills to respond to and remedy cybersecurity incidents occurring within any information system critical for national security;

(k) To conduct inspections and investigations, resolve complaints and denunciations, and deal with breaches of the law on cybersecurity.

3. The Ministry of National Defence is liable before the Government to exercise State administration of cybersecurity within its managerial scope as follows:

(a) To promulgate or submit to the competent State agency to promulgate legal instruments on cybersecurity within its managerial scope;

(b) To formulate and propose strategies, guidelines, policies, plans and options for cybersecurity protection on matters within its managerial scope;

(c) To prevent and combat, within its managerial scope, the use of cyberspace to infringe national security;

(d) To co-ordinate with the Ministry of Public Security to organize drills to prevent and combat cyberattacks; to carry out drills to respond to and remedy cybersecurity incidents within any information system critical for national security; and to commence implementation of cybersecurity protective work;

(dd) To conduct inspections and investigations, resolve complaints and denunciations, and deal with breaches of the law on cybersecurity within its managerial scope.

4. The Government Cipher Committee shall assist the Minister of National Defence to exercise State administration of civil cryptography and cybersecurity within its managerial scope in accordance with law.

5. Ministries, ministerial equivalent agencies, and Government agencies shall, within the scope of their functions, duties and powers, perform the work of cybersecurity protection; and coordinate with the Ministry of Public Security to exercise State administration of cybersecurity.

6. Provincial people's committees shall perform the work of cybersecurity protection in localities; and coordinate with the Ministry of Public Security to exercise State administration of cybersecurity.

Article 40 *Responsibilities of administrators of information systems in protection of cybersecurity*

1. Administrators of information systems shall have the following responsibilities:

   (a) To protect information systems in accordance with this Law;

   (b) To connect cybersecurity monitoring systems, centralized systems for prevention and fighting ransomware to the National Cybersecurity Centre of the Ministry of Public Security or cybersecurity centres of provinces and cities to support monitoring of cybersecurity;

   (c) To report any cybersecurity incident to the specialized agency of the Ministry of Public Security or the Ministry of National Defence.

2. Administrators of information systems using the State budget shall, in addition to the responsibilities prescribed in clause 1 above, have the following responsibilities:

   (a) To have a plan to guarantee cybersecurity evaluated by the competent State agency upon establishment, expansion or upgrade of information systems;

   (b) To appoint individuals or departments in charge of cybersecurity.

Article 41 *Responsibilities of enterprises providing services in cyberspace*

1. To comply with the law on cybersecurity.

2. To give warnings of the possibility of a loss of cybersecurity during use of the services in cyberspace provided by such enterprise and to provide guidelines on preventive measures to service users; to formulate emergency response plans for ensuring cybersecurity to proactively deal with cybersecurity vulnerabilities, risks and incidents.

3. When a cybersecurity incident occurs, to immediately implement emergency response plans for ensuring cybersecurity, and at the same time immediately make a report to the CTF in accordance with this Law.

4. To apply technical measures and solutions to ensure cybersecurity for the activities of processing data and processing personal data in accordance with this Law, the law on data, the law on protection of personal data and other relevant laws.

5. To take responsibility to identify IP addresses of organizations and individuals using Internet services; provide IP address identification information for the CTF to implement cybersecurity protective measures.

6. To coordinate in implementing guidelines of the CTF under the Ministry of Public Security to set up systems for connection and interconnection of technical transmission lines and data transmission lines and satisfy other requisite conditions to implement cybersecurity protective solutions and measures when required to serve investigation, verification and dealing with breaches of the law on cybersecurity.

7. Enterprises providing services on telecom networks, the Internet, and other added value services in cyberspace in Vietnam are responsible to implement the provisions of this article and clauses 2 and 3 of articles 25 of this Law.

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

1. To comply with the law on cybersecurity.

2. To maintain confidentiality of information used for registration, opening, management, and use of their digital accounts. Where a digital account is used to conduct an act in breach of law, depending on the nature and seriousness of such breach, the digital account holder or user shall be subject to disciplinary actions or administrative penalty or criminal liability prosecution; if causing damage to the State's interest or lawful rights and interests of any organization or individual, compensation must be made for any damage in accordance with law.

3. To promptly provide information relating to cybersecurity protection, cybersecurity threats and any cybersecurity intrusion/infringement to the competent agency and/or cybersecurity protective forces.

4. To implement requirements and guidelines of competent agencies during cybersecurity protection; to assist and facilitate agencies, organizations and responsible persons to implement measures for cybersecurity protection.

Chapter VIII

IMPLEMENTING PROVISIONS

Article 43 *Amendments to a number of articles of relevant laws*

1. Replacing a number of phrases, and repealing a number of clauses of the *Law on Archives No. 33/2024/QH15* as follows:

   [Not translated]

2. Replacing and repealing a number of phrases of the *Law on Protection of Interests of Consumers No. 19/2023/QH15* as follows:

   [Not translated]

3. Replacing a number of phrases of the *Law on Charges and Fees No. 97/2015/QH13* as 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 as follows:

   [Not translated]

4. Replacing and repealing a number of phrases of the *Law on Digital Technology Industry No. 71/2025/QH15* as follows:

   [Not translated]

5. Replacing and repealing a number of phrases of the *Law on Data No. 60/2024/QH15* as follows:

   (a) Replacing the phrase "data safety and security" by the phrase "data security" in article 25.4;

   (b) Replacing the phrase "information security and safety" by the phrase "cybersecurity" in article 33.2;

   (c) Repealing the phrase ", information safety" in article 25.4;

   (d) Repealing the phrase "cyberinformation safety," in article 39.4;

   (dd) Repealing the phrase "the law on cyberinformation safety," in article 43.4.

6. Replacing and repealing a number of phrases of the *Law on Cultural Relics No. 45/2024/QH15* as amended by Law No. 84/2025/QH15 as follows:

[Not translated]

7. Replacing and repealing a number of phrases of the *Law on Telecommunications No. 24/2023/QH15* as amended by Law No. 47/2024/QH15 as follows:

   (a) Replacing the phrase “cyberinformation safety” by the phrase “information security” in article 5.8;

   (b) Repealing the phrase “, cyberinformation safety” in the heading of article 5, and in articles 5.1 and 38.2(c);

   (c) Repealing the phrase “cyberinformation safety,” in articles 21.2 and 29.2(b);

8. Replacing and repealing a number of phrases of the *Law on E-transactions No. 20/2023/QH15* as amended by Law No. 60/2024/QH15 as follows:

   (a) Repealing the phrase “cyberinformation safety and” in the heading of article 5;

   (b) Repealing the phrase “the law on cyberinformation safety,” in article 5.1;

   (c) Replacing the phrase “cyberinformation safety” by the phrase "cybersecurity" in articles 20.1(c), 21.2, 29.1(c), 30.6, 44.4, 46.4(a) and 47.1(c);

   (d) Repealing the phrase “cyberinformation safety,” in articles 42.1(d) and 47.1(a).

9. Replacing the phrase “cyberinformation safety” by the phrase "cybersecurity" in article 12.2(b) of the *Law on Corporate Income Tax No. 67/2025/QH15*; in article 169.1 of *the Law on Land No. 31/2024/QH15* as 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*.

10. Replacing the phrase “information security and safety” by the phrase "cybersecurity" in article 7.3(a) of the *Law on Water Resources No. 28/2023/QH15* as amended by Law No. 84/2025/QH15.

11. Repealing the phrase “cyberinformation safety;” in article 24.1(dd) of the *Law on Dealing with Administrative Breaches No. 15/2012/QH13* as 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. 56/2024/QH15 and Law No. 88/2025/QH15.

12. Repealing the phrase “cyberinformation safety,” in article 16.6 of the *Law on People's Public Security No. 37/2018/QH14* as 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 article 66.1 of the *Law on Election of Delegates to the National Assembly and Delegates to People's Councils No. 85/2015/QH13* as amended by Law No. 83/2025/QH15.

13. Repealing the phrase “, information safety” in article 136.3 of the *Law on Organization of People's Courts No. 34/2024/QH15* as amended by Law No. 81/2025/QH15; in article 26.1 of the *Law on Electricity No. 61/2024/QH15* as amended by Law No. 94/2025/QH15.

14. Repealing the phrase “information safety,” in article 29.8; the phrase “information safety and” in clauses 2 and 7 of article 29 of the *Law on Chemicals No. 69/2025/QH15*.

15. Repealing the phrase “information safety,” in articles 51.3, 52.1 and 52.5 of the *Law on Tendering No. 22/2023/QH15* as amended by Law No. 57/2024/QH15 and Law No. 90/2025/QH15; in article 23.1(e) of *the Law on Civil Defence No. 18/2023/QH15* as amended by Law No. 98/2025/QH15.

16. Repealing the phrase “, the law on ensuring information safety” in article 7.4 of the *Law on Atomic Energy No. 94/2025/QH15*.

17. Repealing article 49.3 of the *Law on Libraries No. 46/2019/QH14*.

Article 44 *Effectiveness*

1. This Law is of full force and effect as from 1 July 2026.

2. The *Law on Cyberinformation Safety No. 86/2015/QH13* as amended by Law No. 35/2018/QH14*;* and the *Law on Cybersecurity No. 24/2018/QH14* shall expire from the effective date of this Law.

Article 45 *Transitional provisions*

1. In the case of any information system with the level determined in accordance with the *Law on Cyberinformation Safety No. 86/2015/QH13* as amended by Law No. 35/2018/QH14, the determined level shall remain unchanged from the effective date of this Law; and within 12 months from the effective date of this Law, it is required to ensure the conditions, standards and measures for cybersecurity protection corresponding to the level in accordance with this Law.

2. Types of licences for business of cyberinformation safety products and services and civil cryptography in accordance with the *Law on Cyberinformation Safety No. 86/2015/QH13* as amended by Law No. 35/2018/QH14 which were issued before the effective date of this Law shall be valid until the expiry date recorded in such licences.

3. Products, services, solutions, and technical facilities for ensuring cyberinformation safety in accordance with the *Law on Cyberinformation Safety No. 86/2015/QH13* as amended by Law No. 35/2018/QH14 which were put into use before the effective date of this Law shall continue to be used; and within 12 months from the effective date of this Law, must satisfy the cybersecurity conditions in accordance with this Law.

This Law was passed by Legislature XV of the National Assembly of the Socialist Republic of Vietnam at the 10th session on 10 December 2025.

CHAIRMAN OF THE NATIONAL ASSEMBLY

Tran Thanh Man