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

Law No. 116/2025/QH15

LAW
ON CYBERSECURITY

Pursuant to the Constitution of the Socialist Republic of Vietnam, which was amended and supplemented under Resolution No. 203/2025/QH15;

The National Assembly hereby promulgates the Law on Cybersecurity.

Chapter I
GENERAL PROVISIONS

LuatVietnam.vn

Article 1. Scope of regulation and subjects of application

1. This Law prescribes cybersecurity, cybersecurity protection; rights, obligations, and responsibilities of relevant authorities, organizations, and individuals.

2. This Law applies to:

a) Vietnamese authorities, organizations, and individuals;

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

c) Foreign authorities, organizations, and individuals directly engaged in or related to cybersecurity protection activities, or trading in 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; the protection of information systems and the assurance that information, data, and activities in cyberspace do not cause harm to national security, social order and safety, or rights and legitimate interests of authorities, organizations, and individuals.

2. *Cyberinformation security* means the assurance of the integrity, confidentiality, and availability of information in cyberspace, preventing

LuatVietnam
Tiện ích văn bản luật

unauthorized access, use, disclosure, or modification, sabotage, or other acts threatening or causing harm to national security, social order, and safety.

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

4. *Cybersecurity protection* means the prevention, detection, stopping, and handling of acts that undermine cybersecurity.

5. *Cyberspace* means the environment formed by the network system connecting information technology infrastructure, including telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, and databases; it is a place where humans perform social acts without limitation of space and time.

6. *National cyberspace* means the 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 purpose of creating, providing, transmitting, collecting, processing, storing, and exchanging information in cyberspace.

LuatVietnam.vn

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

9. *Malware* means software capable of causing abnormal activities to a part or the whole of an information system or performing unauthorized copying, modification, or deletion of information stored in an information system.

10. *Malicious hardware* means physical components designed intentionally or added to standard hardware components to collect information and data illegally or to interfere with, cause stoppage to, paralyze, or sabotage computer systems or information systems.

11. *System logs* mean collections of records reflecting the time, users, activities, and status of the system for the purpose of system management, supervision, and security.

12. *Cybercrime* means an act dangerous to society prescribed in the Penal Code, committed by an individual or organization in cyberspace by using information technology or electronic means.

13. *Cyberattack* means an act performed in cyberspace by using information technology or electronic means to appropriate information, cause disorder, disruption, or paralysis to operations, or sabotage or control telecommunications networks, the Internet, computer networks, information

LuatVietnam
Tiện ích văn bản luật

systems, information processing and control systems, databases, or electronic means.

14. *Cyberterrorism* means an act performed in cyberspace by using information technology or electronic means to cause panic among the public or to destabilize politics.

15. *Cyberespionage* means an act performed in cyberspace by using information technology or electronic means to secretly infiltrate to appropriate, collect, or copy information falling within the scope of state secrets, or important data of authorities, organizations, and individuals for the purpose of causing harm to national security, social order, and safety.

16. *Risk of threatening cybersecurity* means a state of cyberspace where signs of threatening to undermine national security or causing serious damage to social order, safety, or rights and legitimate interests of authorities, organizations, and individuals appear.

17. *Cybersecurity incident* means an unexpected event occurring in cyberspace undermining national security, social order, safety, or rights and legitimate interests of authorities, organizations, and individuals.

18. *Dangerous situation regarding cybersecurity* means a state or development in cyberspace where there are factors of attack, infiltration, incitement, disclosure, or loss of information, or other acts threatening to seriously undermine national security, social order, safety, or rights and legitimate interests of authorities, organizations, and individuals.

19. *Digital account* means information used to authenticate, verify, and authorize the use of applications and services in cyberspace.

20. *Civil cryptography* means cryptographic techniques and cryptographic products used to secure or authenticate information not falling within the scope of state secrets to ensure information security for authorities, organizations, and individuals.

21. *Cybersecurity product* means hardware or software with the function of protecting cybersecurity, cyberinformation security, data security, information, data, information systems, or information technology infrastructure.

22. *Cybersecurity service* means a service provided to protect cybersecurity, cyberinformation security, data security, information, data, information systems, or information technology infrastructure.

23. *Cipher information system* means an information system using cipher cryptography to protect information falling within the scope of state secrets for specialized cipher activities directly managed and operated by cipher organizations.

Article 3. State policies on cybersecurity

LuatVietnam
Tiện ích văn bản luật

1. Building a healthy cyberspace, not causing harm to national security, social order and safety, rights and legitimate interests of authorities, organizations, and individuals.

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

3. Prioritizing the allocation of resources for building and developing specialized cybersecurity protection forces, ensuring high-quality human resources for cybersecurity protection; improving capacity for cybersecurity protection forces and organizations and individuals engaged in cybersecurity protection; prioritizing investment in research and development of modern science and technology for cybersecurity protection; having specific mechanisms and preferential policies to mobilize, attract, train, and employ talented people in the field of cybersecurity.

4. Promoting association and investment under public-private partnerships in cybersecurity protection; encouraging and creating conditions for authorities, organizations, and individuals to participate in cybersecurity protection and handle risks of threatening cybersecurity; researching and developing technology, products, services, and applications to protect cybersecurity; utilizing cybersecurity products and services of Vietnam.

5. Expanding international cooperation on cybersecurity to strengthen cybersecurity protection capabilities; preventing and combating cybercrime and transnational cybersecurity threats; acquiring modern technology to improve national cybersecurity autonomy.

Article 4. Principles of cybersecurity protection

1. Compliance with the Constitution and the law regulations; assurance of national security, sovereignty, and interests in cyberspace.

2. Placing under the leadership of the Communist Party of Vietnam; the unified management of the State; mobilizing the synergy of the political system and the entire nation; promoting the core role of specialized cybersecurity protection forces.

3. Closely combining cybersecurity protection with socio-economic development, ensuring human rights, citizens' rights, and personal data protection, creating conditions for authorities, organizations, and individuals to operate lawfully in cyberspace.

4. Applying measures to protect national cyberspace; proactively preventing, detecting, stopping, and struggling to defeat all activities in cyberspace undermining national security, social order, safety, or rights and

LuatVietnam
Tiện ích văn bản luật

legitimate interests of authorities, organizations, and individuals; handling strictly and promptly acts of violating the law on cybersecurity.

5. Deploying cybersecurity protection activities regularly and continuously for national cyberspace infrastructure; proactively applying measures to protect information systems important to national security.

Article 5. Cybersecurity protection measures

1. Cybersecurity protection measures include:

a) Cybersecurity appraisal;

b) Assessment of cybersecurity conditions;

c) Cybersecurity inspection;

d) Cybersecurity supervision:

dd) Response to and remediation of cybersecurity incidents;

e) Combat to protect cybersecurity;

g) Use of cryptography to protect cyberinformation;

h) Use of technical solutions to protect cyberinformation security, data security, and information systems; prevention of information violating the law regulations;

i) Blocking, requesting temporary suspension or suspension of the provision of cyberinformation; suspension or temporary suspension of activities of establishing, providing, and using telecommunications networks, the Internet, and production and use of radio transmitters and transceivers prescribed by the law regulations;

k) Requesting deletion or access to delete unlawful information or false information, fake news in cyberspace undermining national security, social order, safety, or rights and legitimate interests of authorities, organizations, and individuals;

l) Collection of electronic data related to activities undermining national security, social order, safety, or rights and legitimate interests of authorities, organizations, and individuals in cyberspace;

m) Blockade or limitation of the operation of information systems; suspension, temporary suspension, or request for cessation of the operation of information systems; revocation of domain names prescribed by the law regulations;

n) Prosecution, investigation, prosecution, and trial prescribed by the Criminal Procedure Code;

o) Other measures prescribed by the law on national security and handling of administrative violations.

LuatVietnam
Tiện ích văn bản luật

2. The Government shall detail the particulars, sequence, procedures, and competence to apply cybersecurity protection measures, other than those prescribed at Point n and Point o, Clause 1 of this Article.

Article 6. International cooperation on cybersecurity

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

2. International cooperation on cybersecurity covers:

a) Sharing information, data, and early warnings about risks, incidents, and cyberattacks affecting cybersecurity;

b) Building legal frameworks, policies, and mechanisms for cooperation and coordination in cybersecurity protection; negotiating, signing, and engaged in the implementation of treaties and international agreements on cybersecurity;

c) Training, consulting, sharing experiences, and improving professional and technical capacity in the field of cybersecurity;

d) Prevention and combat of cybercrime and high-tech crime; coordination in investigation and handling of violations of the law regulations, cybercrime, and high-tech crime:

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

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

g) Other international cooperation activities on cybersecurity.

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

a) The Ministry of Public Security shall be responsible before the Government for presiding over and coordinating the implementation of international cooperation on cybersecurity;

b) The Ministry of National Defence shall be responsible before the Government for implementing international cooperation on cybersecurity within its scope of management;

c) The Ministry of Foreign Affairs shall coordinate with the Ministry of Public Security and the Ministry of National Defence in international cooperation activities on cybersecurity;

LuatVietnam
Tiện ích văn bản luật

d) In cases where international cooperation on cybersecurity relates to the responsibilities of multiple Ministries and sectoral authorities, it shall be decided by the Prime Minister:

dd) International cooperation activities on cybersecurity of other Ministries, sectoral authorities, and localities must have written comments from the Ministry of Public Security before deployment.

Article 7. Prohibited acts regarding cybersecurity

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

a) Propaganda against the State of the Socialist Republic of Vietnam, including: distorting propaganda, defaming the people's administration; psychological warfare, inciting wars of aggression, causing division and hatred between nations, religions, and people of other countries; insulting the nation, the national flag, the national emblem, the national anthem, great men, leaders, famous people, and national heroes;

b) Distorting history, denying revolutionary achievements, undermining the great national unity bloc, insulting religion, gender discrimination, and racism;

c) Fabricating, slandering, or providing false information undermining the honor, dignity, or prestige of others or causing damage to the rights and legitimate interests of other authorities, organizations, and individuals;

d) Falsehoods causing confusion among the People, causing damage to socio-economic activities, causing difficulties for the normal operation of State regulatory authorities or persons performing official duties, undermining the rights and legitimate interests of other authorities, organizations, and individuals; fabricated or false information about products, goods, money, bonds, bills, government bonds, checks, and other valuable papers; fabricated or false information in the fields of finance, banking, e-commerce, multi-level marketing, and securities.

2. Performing the following acts in cyberspace:

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

b) Inciting, calling for, mobilizing, instigating, threatening, or causing division to conduct armed activities or use violence to oppose the people's administration; inciting, calling for, mobilizing, instigating, threatening, or enticing gatherings of large numbers of people to cause disturbances, resist persons performing official duties, or obstruct the operations of authorities and organizations, causing instability to security and order;

LuatVietnam
Tiện ích văn bản luật

c) Appropriating, trading, seizing, or intentionally disclosing information that contain state secrets, work secrets, or trade secrets; appropriating, trading, seizing, or intentionally disclosing personal secrets, family secrets, and privacy affecting the honor, reputation, dignity, rights, and legitimate interests of authorities, organizations, or individuals; intentionally eavesdropping, or illegally recording audio or video of conversations in cyberspace; disclosing information on civil cryptography products, or information on customers lawfully using civil cryptography products; using or trading civil cryptography products of unknown origin;

d) Prostitution activities, social vices, trafficking in persons, or trafficking in human body parts; disseminating obscene or depraved cultural products; inciting or promoting violence, debauched or deviant lifestyles, undermining the fine customs and traditions of the nation, social morality, and public health:

dd) Fraudulently appropriating property; organizing gambling or gambling via the Internet; theft of international telecommunications charges on the Internet platform; propagating, advertising, or trading in goods and services falling within the list of banned goods and services prescribed by the law regulations; violating copyright and intellectual property in cyberspace;

e) Impersonating websites of authorities, organizations, or individuals; counterfeiting, circulating, stealing, trading in, collecting, or exchanging without permission credit card information, bank accounts, crypto assets, or digital assets of others; issuing, providing, or using illegal payment means; counterfeiting documents of authorities or organizations;

g) Using artificial intelligence or new technologies to fake videos, images, or voices of others contrary to the law regulations; creating, posting, or disseminating information prescribed in Clause 1 of this Article;

h) Collecting, using, disseminating, exchanging, transferring, or trading in personal information and data of others illegally;

i) Guiding, instigating, enticing, or inciting others to commit crimes or perform acts of violating the law regulations;

k) Performing other acts in cyberspace by using information technology or electronic means to violate the law on national security, social order, and safety.

3. Carrying out cyberattacks, cyberterrorism, cyberespionage, cybercrime, or high-tech crime; causing incidents, attacking, infiltrating, taking control of, falsifying, interrupting, stalling, paralyzing, or sabotaging information systems.

4. Producing or putting into use tools, means, software, or having acts of obstructing, causing disruption, or disseminating spam emails, spam messages, spam calls, or computer programs harmful to the operation of

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, or electronic means.

5. Infiltrating without permission telecommunications networks, computer networks, information systems, information processing and control systems, databases, or electronic means of others.

6. Resisting or obstructing the activities of cybersecurity protection forces; attacking or illegally disabling to neutralize cybersecurity protection measures.

7. Taking advantage of or abusing cybersecurity protection activities to undermine sovereignty, interests, national security, social order, safety, or rights and legitimate interests of authorities, organizations, and individuals, or to seek illegal profit.

8. Other acts violating the regulations of this Law.

Chapter II
CYBERSECURITY PROTECTION FOR INFORMATION SYSTEMS

LuatVietnam.vn

Article 8. Classification of information system levels

1. Information systems are classified into 5 levels based on the degree of damage to national security, social order, safety, rights, legitimate interests of organizations and individuals, and public interests in case of an incident or an act of violating the law on cybersecurity, as follows:

a) Level 1 may cause damage to the rights and legitimate interests of organizations and individuals;

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

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

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

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

2. The Government shall detail the criteria for determining information system levels; and prescribe the competence, order, and procedures for determining information system levels and measures, responsibilities, and obligations to ensure cybersecurity according to each level of information system.

Article 9. Important information systems relating to national security

LuatVietnam
Tiện ích văn bản luật

1. Important information systems relating to national security are information systems having a strategic and particularly important role in politics, national defense, security, foreign affairs, economy, and society which, in case of an incident or an act of violating the law on cybersecurity, may cause damage to national security or serious damage to social order and safety, falling within the list decided by the Prime Minister.

2. Important information systems relating to national security fall within the following fields:

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

b) Information systems storing and processing information that contain state secrets;

c) Information systems being used for the preservation of artifacts and documents of particularly important value;

d) Information systems being used for the preservation of materials and substances particularly dangerous to humans and the environment:

dd) Information systems being used for the preservation, manufacture, and management of other particularly important material facilities related to national security;

e) Important information systems being used for the activities of authorities and organizations at the central level;

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

h) Automatic control and monitoring systems at important works related to national security and important targets regarding national security.

3. Important information systems relating to national security must undergo cybersecurity appraisal and certification of cybersecurity conditions before being put into operation and use; and undergo regular cybersecurity inspection and cybersecurity supervision during use and timely response to and remediation of cybersecurity incidents.

4. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries, sectoral authorities, authorities, organizations, and individuals in formulating the list of important information systems relating to national security and submitting it to the Prime Minister for consideration and decision.

5. The Government shall detail the criteria for determining important information systems relating to national security.

LuatVietnam
Tiện ích văn bản luật

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

1. Tasks of cybersecurity protection for information systems include:

a) Determining cybersecurity levels of information systems and important information systems relating to national security;

b) Assessing and managing cybersecurity risks of information systems;

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

d) Organizing the deployment of cybersecurity protection measures for information systems:

dd) Implementing the reporting regime as prescribed;

e) Organizing propaganda and raising awareness about cybersecurity.

2. Cybersecurity protection measures for information systems include:

a) Promulgating regulations on ensuring cybersecurity in the design, construction, management, operation, use, upgrade, and cancellation of information systems;

b) Appraising cybersecurity for dossiers and designs of information systems;

c) Assessing cybersecurity conditions for information systems;

d) Applying management measures according to cybersecurity standards and technical regulations; researching and building a national firewall system to prevent and combat risks and remediate cybersecurity incidents:

dd) Organizing the deployment of storage and backup measures to protect cyberinformation security and the security of components constituting information systems;

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

g) Implementing cybersecurity supervision;

h) Responding to and remediating cybersecurity incidents for information systems.

3. Information system managers of Level 1 and Level 2 shall fully perform the tasks prescribed in Clause 1 of this Article and, based on needs and practical capabilities, choose to apply the measures prescribed in Clause 2 of this Article.

4. Information system managers of Level 3 and Level 4 other than those falling within the list of important information systems relating to national security shall fully perform the tasks prescribed in Clause 1 of this Article, the

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

measures prescribed at Points a, d, dd, e, g, and h, Clause 2 of this Article and, based on needs and practical capabilities, choose to apply the measures prescribed at Point b and Point c, Clause 2 of this Article.

5. Information system managers falling within the list of important information systems relating to national security shall fully perform the tasks and measures prescribed in Clause 1 and Clause 2 of this Article.

6. The Government shall detail Clause 1 and Clause 2 of this Article.

Article 11. Responsibilities for cybersecurity protection for important information systems relating to national security

1. Owners of important information systems relating to national security shall:

a) Implement the regulations in Clause 5, Article 10 of this Law;

b) Perform cybersecurity inspection before putting the systems into operation and exploitation when establishing, expanding, or upgrading important information systems relating to national security; periodically every year, perform cybersecurity self-inspection and assessment of cybersecurity conditions for important information systems relating to national security and notify the inspection results in writing before October each year to the competent specialized cybersecurity protection force;

c) Assume the prime responsibility for, and coordinate with the competent specialized cybersecurity protection force in regularly performing cybersecurity supervision; build a mechanism for self-warning and receiving warnings about risks of threatening cybersecurity; devise plans for emergency response and remediation;

d) Build plans for response to and remediation of cybersecurity incidents; deploy response and remediation plans when cybersecurity incidents occur and timely report to the competent specialized cybersecurity protection force;

dd) Coordinate with the specialized cybersecurity protection force in performing unexpected cybersecurity inspections.

2. The Ministry of Public Security shall, regarding important information systems relating to national security, other than military information systems and cipher information systems under the Government Cipher Committee prescribed by the law regulations:

a) Appraise cybersecurity for important information systems relating to national security;

b) Assess and certify sufficient cybersecurity conditions for important information systems relating to national security;

LuatVietnam
Tiện ích văn bản luật

c) Perform unexpected cybersecurity inspections for important information systems relating to national security;

d) Implement cybersecurity supervision; warn and coordinate with information system managers to remediate and handle risks of threatening cybersecurity and cybersecurity incidents for important information systems relating to national security:

dd) Assume the prime responsibility for the coordination of activities to respond to and remediate cybersecurity incidents occurring to important information systems relating to national security; notify information system managers upon detection of cyberattacks or cybersecurity incidents;

e) Assume the prime responsibility for, and coordinate with the Government Cipher Committee in deploying measures to protect important information systems relating to national security that use cryptographic solutions and products provided by the Government Cipher Committee to protect state secrets.

3. The Ministry of National Defence shall assume the prime responsibility for cybersecurity appraisal, assessment of cybersecurity conditions, unexpected cybersecurity inspection, cybersecurity supervision, and coordination of activities to respond to and remediate cybersecurity incidents for military information systems managed by the Ministry of National Defence.

4. The Government Cipher Committee shall assume the prime responsibility for organizing the deployment of solutions using cipher cryptography to protect state secret information in important information systems relating to national security; appraise cybersecurity, assess cybersecurity conditions, perform unexpected cybersecurity inspection, cybersecurity supervision, and coordinate activities to respond to and remediate cybersecurity incidents for cipher information systems under the Government Cipher Committee.

Article 12. Cybersecurity inspection for information systems of authorities and organizations not falling within the list of important information systems relating to national security

1. Cybersecurity inspection for information systems of authorities and organizations not falling within the list of important information systems relating to national security shall be conducted in the following cases:

a) When there is an act prescribed in Clauses 12, 13, 14, and 15, Article 2 of this Law;

b) Upon the request of the information system manager.

2. Subjects of cybersecurity inspection include:

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

LuatVietnam
Tiện ích văn bản luật

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

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

3. Information system managers are responsible for notifying the specialized cybersecurity protection force under the Ministry of Public Security upon detection of acts of violating the law on cybersecurity on information systems under their management scope.

4. The specialized cybersecurity protection force under the Ministry of Public Security shall conduct cybersecurity inspections for information systems of authorities and organizations in the cases prescribed in Clause 1 of this Article. Results of cybersecurity inspections shall be kept confidential prescribed by the law regulations.

5. The Government shall prescribe the order and procedures for cybersecurity inspection prescribed in this Article.

Chapter III
PREVENTION AND HANDLING OF ACTS THAT UNDERMINE CYBERSECURITY

LuatVietnam.vn

Article 13. Information and acts of using information technology and electronic means to undermine national security, social order, and safety in cyberspace

1. Information with propaganda against the State of the Socialist Republic of Vietnam, inciting riots, disrupting security, or disturbing public order includes:

a) Propagating information and documents distorting, defaming, or insulting the people's administration;

b) Psychological warfare, inciting wars of aggression, causing division and hatred between nations, religions, and people of other countries;

c) Insulting the nation, the national flag, the national emblem, the national anthem, great men, leaders, famous people, and national heroes;

d) Calling for, mobilizing, instigating, threatening, or causing division to conduct armed activities or use violence to oppose the people's administration:

dd) Calling for, mobilizing, instigating, threatening, or enticing gatherings of large numbers of people to cause disturbances, resist persons performing official duties, or obstruct the normal operation of authorities and organizations, causing instability to security and order;

LuatVietnam
Tiện ích văn bản luật

e) Reflecting falsely or inaccurately the national border and national sovereignty of Vietnam; posting or transmitting false, inaccurate, or incomplete images of the map of Vietnam or misrepresenting the national sovereignty of Vietnam.

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

a) Causing conflict or division among strata of the people, between the people and the people's administration, the people's armed forces, or socio-political organizations;

b) Inciting, causing hatred, discrimination, division, or ethnic separatism, or undermining the right to equality in the community of ethnic groups of Vietnam;

c) Inciting, causing conflict or division between religious followers and non-religious people, or between followers of different religions; dividing religious believers from the people's administration, the people's armed forces, or socio-political organizations;

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

dd) Propaganda causing direct or indirect harm to the rights, legitimate interests of the State regarding politics, economy, society, and international prestige;

e) Calling for or inciting sabotage of the implementation of socio-economic policies, or causing obstruction to the enforcement of policies;

g) Calling for or inciting sabotage of the material-technical foundations of the Socialist Republic of Vietnam.

3. Information undermining the rights, legitimate interests of organizations and individuals includes:

a) Spreading distorted, fabricated, or false information affecting the prestige or normal operation of organizations;

b) Calling for, mobilizing, or instigating a boycott of products, services, goods, brands, or trademarks of organizations or enterprises, causing material damage or damage to the prestige of organizations or enterprises;

c) Impersonating or counterfeiting information, images, products, trademarks, or brands of organizations or enterprises by using technological utilities, causing influence to the prestige of organizations or enterprises;

d) Insulting the honor, prestige, or dignity of others:

dd) Distorting falsely, causing influence to the honor, prestige, or dignity of others;

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

e) Fabricating or spreading information known to be false causing damage to the rights, legitimate interests of others;

g) Fabricating crimes of others and denouncing them to competent authorities;

h) Impersonating or counterfeiting information, images, or voices of individuals, causing influence to the prestige, honor, or dignity of individuals.

4. Acts performed in cyberspace by using information technology or electronic means undermining national security and social order and safety include:

a) Posting or disseminating in cyberspace the information prescribed in Clauses 1, 2, and 3 of this Article;

b) Performing acts prescribed in Clause 1, Article 15 of this Law;

c) Appropriating property; organizing gambling or gambling via the Internet; theft of international telecommunications charges on the Internet platform; violating copyright and intellectual property in cyberspace;

d) Impersonating websites of authorities, organizations, or individuals; counterfeiting, circulating, stealing, trading in, collecting, or exchanging without permission credit card information or bank accounts of others; issuing, providing, or using illegal payment means; counterfeiting seals, documents, or other papers of authorities or organizations;

dd) Propagating, advertising, or trading illegally in weapons, explosives, tactical gear, or firecrackers; narcotics, narcotic precursors, addictive substances, or psychotropic substances; wild, endangered, precious, and rare animals and other goods and services falling within the list of banned goods and services prescribed by the law regulations; brokering prostitution; disseminating depraved cultural products; child sexual abuse; sexual harassment;

e) Establishing or providing services or supporting the operation, business, transaction, trading, or online marketing for illegal exchanges, websites, or applications in cyberspace, including: e-commerce exchanges, websites, or applications selling goods or providing e-commerce services; exchanges based on commodity indices; digital asset exchanges; or multi-level marketing business;

g) Using fake identities, documents, or dossiers or using illegally information of others to establish enterprises, establish, or register bank accounts, securities accounts, insurance accounts, tax accounts, and other digital accounts; collecting, stockpiling, exchanging, trading in, donating, or making public illegally data, information on bank accounts, bank cards, e-wallet accounts, securities accounts, insurance accounts, tax accounts, and other types of digital accounts;

LuatVietnam
Tiện ích văn bản luật

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

i) Guiding others to perform acts of violating the law regulations;

k) Other acts performed in cyberspace by using information technology or electronic means violating the law on national security, social order, and safety.

Article 14. Prevention and handling of information and acts of using information technology and electronic means to undermine national security, social order, and safety in cyberspace

1. Information system managers, and domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace are responsible for deploying management and technical measures to prevent, detect, stop, and remove the information prescribed in Clauses 1, 2, and 3, Article 13 of this Law on information systems under their management scope or upon the request of the specialized cybersecurity protection force.

2. The specialized cybersecurity protection force and competent authorities shall apply the measures prescribed in Clause 1, Article 5 of this Law to handle in cyberspace the information prescribed in Clauses 1, 2, and 3, Article 13 of this Law and fight against, prevent, and combat acts of using information technology and electronic means to undermine national security, social order, and safety in cyberspace.

3. Domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace and information system managers shall coordinate with the specialized cybersecurity protection force to handle in cyberspace the information prescribed in Clauses 1, 2, and 3, Article 13 of this Law and prevent and combat acts of using information technology and electronic means to undermine national security, social order, and safety in cyberspace.

4. Organizations and individuals drafting, posting, or disseminating in cyberspace the information prescribed in Clauses 1, 2, and 3, Article 13 of this Law must remove the information upon the request of the specialized cybersecurity protection force and bear responsibility prescribed by the law regulations.

5. The Government shall detail this Article.

Article 15. Prevention and combat of cyberespionage; protection of information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy in cyberspace

LuatVietnam
Tiện ích văn bản luật

1. Acts of cyberespionage; undermining state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy in cyberspace include:

a) Appropriating, trading, seizing, or intentionally disclosing information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy affecting the honor, reputation, dignity, rights, and legitimate interests of authorities, organizations, or individuals;

b) Intentionally deleting, damaging, losing, or changing information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy transmitted or stored in cyberspace;

c) Intentionally changing, canceling, or neutralizing technical measures built and applied to protect information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy;

d) Putting onto cyberspace information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy contrary to the law regulations:

dd) Intentionally listening to, recording audio, or recording video of conversations without permission;

e) Other acts of intentionally undermining state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy.

LuatVietnam.vn

2. Information system managers shall:

a) Inspect cybersecurity to detect and remove malware and malicious hardware, and fix security weaknesses and vulnerabilities; detect, prevent, and handle illegal intrusion activities or other risks threatening cybersecurity;

b) Deploy management and technical measures to prevent, detect, and stop acts of cyberespionage or infringement upon state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy on information systems and promptly remove information related to these acts;

c) Coordinate and implement requests of the specialized cybersecurity protection force regarding the prevention and combat of cyberespionage and protection of information that contain state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy on information systems.

3. Authorities and organizations drafting or storing information and documents containing state secrets are responsible for protecting state secrets drafted or stored on computers or other devices or exchanged in cyberspace prescribed by the law on protection of state secrets.

4. The Ministry of Public Security shall, unless otherwise prescribed in Clause 5 and Clause 6 of this Article:

LuatVietnam
Tiện ích văn bản luật

a) Inspect cybersecurity for important information systems relating to national security to detect and remove malware and malicious hardware, and fix security weaknesses and vulnerabilities; detect, prevent, and handle illegal intrusion activities;

b) Inspect cybersecurity for telecommunications equipment, products, and services, digital devices, and electronic devices before putting them into use in important information systems relating to national security;

c) Supervise cybersecurity for important information systems relating to national security to detect and handle activities of illegally collecting information that contain state secrets;

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

dd) Participate in research and production of products for storing and transmitting information and documents containing state secrets prescribed by the law regulations and products for encrypting information in cyberspace according to assigned functions and tasks;

e) Inspect and check the protection of state secrets in cyberspace of State regulatory authorities and protecting cybersecurity of owners of important information systems relating to national security;

LuatVietnam.vn

g) Organize training and drills to raise awareness and knowledge about protecting state secrets in cyberspace, preventing and combating cyberattacks, and protecting cybersecurity for the cybersecurity protection forces prescribed in Clause 1, Article 30 of this Law.

5. The Ministry of National Defence is responsible for implementing Clause 4 of this Article for military information systems.

6. The Government Cipher Committee is responsible for implementing Clause 4 of this Article for cipher information systems under the Government Cipher Committee; and is responsible for organizing the implementation of the law regulations in using cryptography to protect information that contain state secrets stored or exchanged in cyberspace.

Article 16. Prevention and combat of child abuse in cyberspace

1. Children have the right to access information, participate in social activities, play, entertain, have personal secrets and privacy protected, and other rights in cyberspace prescribed by the law regulations.

2. When children use value-added services in cyberspace, parents or guardians prescribed by the civil law shall register accounts using the information of the parents or guardians and are responsible for supervising and managing the content that children access, post, and share on those service platforms.

LuatVietnam
Tiện ích văn bản luật

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

a) Control the content of information on information systems or services provided by enterprises so as not to cause danger to children, abuse children, or undermine children's rights;

b) Stop the sharing of and delete information causing danger to children, abusing children, or undermining children's rights;

c) Build and deploy technical systems to support activities of stopping content abusing children in cyberspace;

d) Coordinate with authorities, organizations, and enterprises to implement the stopping of sources disseminating information abusing children in cyberspace:

dd) Promptly notify and coordinate with the specialized cybersecurity protection force under the Ministry of Public Security for handling.

4. Authorities, organizations, and individuals engaged in activities in cyberspace are responsible for coordinating with competent authorities in ensuring the rights of children in cyberspace; and preventing and combating child abuse in cyberspace.

LuatVietnam.vn

5. Authorities, organizations, parents, guardians, teachers, caregivers, and other relevant individuals are responsible for ensuring the rights of children and protecting children when engaged in cyberspace prescribed by the law on children and the regulations of this Law.

6. The specialized cybersecurity protection force and functional authorities are responsible for applying measures to prevent, detect, stop, and handle strictly acts of using cyberspace to cause danger to children, abuse children, or undermine children's rights.

Article 17. Prevention, detection, stopping, and handling of malware

1. Authorities, organizations, and individuals are responsible for proactively preventing, detecting, and stopping malware and complying with the guidelines and requests of competent State regulatory authorities.

2. Owners of important information systems relating to national security shall deploy technical systems to prevent, detect, stop, and handle malware promptly.

3. Organizations and enterprises providing email services or information transmission and storage services must have malware filtering systems during the process of sending, receiving, and storing information on their systems and report to competent State regulatory authorities prescribed by the law regulations.

LuatVietnam
Tiện ích văn bản luật

4. Enterprises providing Internet services shall have measures to manage, prevent, detect, and stop the dissemination of malware and handle it upon the request of competent State regulatory authorities.

5. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with the Ministry of National Defence and relevant Ministries and sectoral authorities in organizing the prevention, detection, stopping, and handling of malware causing damage to national security.

Article 18. Prevention and combat of cyberattacks

1. Acts of cyberattack and acts related to cyberattacks include:

a) Disseminating computer programs harmful to telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, and electronic means;

b) Causing obstruction, disorder, paralysis, interruption, or stoppage of operations, or blocking illegally the transmission of data of cyberspace;

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

d) Infiltrating, creating, or exploiting security weaknesses, vulnerabilities, and system services to appropriate information or gain illicit profits:

dd) Producing, trading in, exchanging, or donating tools, devices, or software with features causing harm to telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic means to be used for unlawful purposes;

e) Other acts causing influence to the normal operation of telecommunications networks, the Internet, computer networks, information systems, information processing and control systems, databases, or electronic means.

2. Information system managers are responsible for applying technical measures to prevent and stop acts prescribed at Points a, b, c, d, and e, Clause 1 of this Article for information systems under their management scope.

3. When a cyberattack occurs undermining or threatening to undermine sovereignty, interests, or national security, or causing serious damage to social order and safety, the specialized cybersecurity protection force shall assume the prime responsibility for, and coordinate with the information system manager and relevant organizations and individuals in taking measures to determine the origin of the cyberattack and collect evidence; and requesting enterprises providing services on telecommunications networks, the Internet, and value-added services

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

in cyberspace to block and filter information to prevent and eliminate the cyberattack and provide relevant information and documents fully and promptly.

4. Responsibilities for preventing and combating cyberattacks are prescribed as follows:

a) The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries, sectoral authorities, and localities in preventing, detecting, and handling acts prescribed in Clause 1 of this Article undermining or threatening to undermine sovereignty, interests, or national security, or causing serious damage to social order and safety nationwide, unless otherwise prescribed at Point b and Point c of this Clause;

b) The Ministry of National Defence shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in preventing, detecting, and handling acts prescribed in Clause 1 of this Article for military information systems;

c) The Government Cipher Committee shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in preventing, detecting, and handling acts prescribed in Clause 1 of this Article for cipher information systems under the Government Cipher Committee.

Article 19. Prevention and combat of cyberterrorism

1. Competent State regulatory authorities are responsible for applying measures in accordance with the regulations of this Law and the law regarding prevention and combat of terrorism to handle cyberterrorism.

2. Information system managers shall regularly review and inspect information systems under their management scope to eliminate risks of cyberterrorism.

3. Upon detecting signs or acts of cyberterrorism, authorities, organizations, and individuals must timely report to the cybersecurity protection force. Authorities receiving reports are responsible for fully receiving reports on cyberterrorism and timely notifying the specialized cybersecurity protection force.

4. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in deploying cyberterrorism prevention and combat, applying measures to neutralize sources of cyberterrorism, handling cyberterrorism, and mitigating the impact of their consequences on information systems, unless otherwise prescribed in Clause 5 and Clause 6 of this Article.

5. The Ministry of National Defence shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in deploying cyberterrorism prevention and combat, apply measures to neutralize sources of

LuatVietnam.vn
Tiện ích văn bản luật

cyberterrorism, handle cyberterrorism, and limit to the lowest level the consequences occurring to military information systems.

6. The Government Cipher Committee shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in deploying cyberterrorism prevention and combat, and applying measures to neutralize sources of cyberterrorism, handle cyberterrorism, and limit to the lowest level the consequences occurring to cipher information systems under the Government Cipher Committee.

Article 20. Prevention and handling of dangerous situations regarding cybersecurity

1. Dangerous situations regarding cybersecurity include:

a) Appearance of information inciting on cyberspace with a risk of causing riots, security disruption, or terrorism;

b) Attacks on important information systems relating to national security;

c) Attacks on multiple information systems on a large scale and high intensity;

d) Cyberattacks aiming to destroy important works relating to national security or important targets regarding national security:

dd) Cyberattacks seriously undermining sovereignty, interests, and national security; or causing particularly serious damage to social order, safety, rights, and legitimate interests of authorities, organizations, and individuals.

2. Responsibilities for preventing dangerous situations regarding cybersecurity are prescribed as follows:

a) The specialized cybersecurity protection force shall coordinate with owners of important information systems relating to national security to deploy technical and professional solutions to prevent, detect, and handle dangerous situations regarding cybersecurity;

b) Telecommunications, Internet, and information technology enterprises, enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace, and relevant authorities, organizations, and individuals are responsible for coordinating with the specialized cybersecurity protection force under the Ministry of Public Security in preventing, detecting, and handling dangerous situations regarding cybersecurity.

3. Measures to handle dangerous situations regarding cybersecurity include:

a) Deploying immediately plans for prevention and emergency response regarding cybersecurity, preventing, eliminating, or mitigating damage caused by dangerous situations regarding cybersecurity;

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

b) Notifying relevant authorities, organizations, and individuals;

c) Collecting relevant information; continuously monitoring and supervising dangerous situations regarding cybersecurity;

d) Analyzing and assessing information, forecasting the possibility, scope of influence, and level of damage caused by dangerous situations regarding cybersecurity:

dd) Stopping the provision of cyberinformation in specific areas or disconnecting international network gateways;

e) Arranging forces and means to prevent and eliminate dangerous situations regarding cybersecurity;

g) Other measures prescribed by the Law on National Security.

4. The handling of dangerous situations regarding cybersecurity is prescribed as follows:

a) Upon detecting a dangerous situation regarding cybersecurity, authorities, organizations, and individuals shall timely notify the specialized cybersecurity protection force and immediately apply the measures prescribed at Point a and Point b, Clause 3 of this Article;

b) The Prime Minister shall consider and decide or authorize the Minister of Public Security to consider, decide, and handle dangerous situations regarding cybersecurity nationwide or in each locality or for a specific target.

The Prime Minister shall consider and decide or authorize the Minister of National Defense to consider, decide, and handle dangerous situations regarding cybersecurity for military information systems and cipher information systems under the Government Cipher Committee;

c) The specialized cybersecurity protection force shall assume the prime responsibility for, and coordinate with relevant authorities, organizations, and individuals in applying the measures prescribed in Clause 3 of this Article to handle dangerous situations regarding cybersecurity;

d) Relevant authorities, organizations, and individuals are responsible for coordinating with the specialized cybersecurity protection force to implement measures to prevent and handle dangerous situations regarding cybersecurity.

Article 21. Combat to protect cybersecurity

1. Combat to protect cybersecurity means an organized activity performed by the specialized cybersecurity protection force in cyberspace to protect national security and ensure social order and safety.

2. The combat to protect cybersecurity covers:

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

a) Supervising cyberinformation and preventing, struggling against, and handling organizations and individuals having activities of using cyberspace to undermine national security, social order, and safety;

b) Using technical solutions to prevent information violating the law regulations;

c) Preventing and combating attacks and protecting the stable operation of important information systems relating to national security;

d) Paralyzing or limiting activities of using cyberspace to cause harm to national security or cause particularly serious damage to social order and safety:

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

3. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in implementing the combat to protect cybersecurity; the Ministry of National Defence shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in implementing the combat to protect cybersecurity regarding military information systems.

Article 22. Prevention of information conflict in cyberspace

1. Information conflict is where two or more domestic and foreign organizations use technological and information technical measures to cause damage to information and information systems in cyberspace, affecting national security, social order, and safety.

2. Prevention of information conflict in cyberspace is the implementation of technological and technical measures to supervise, detect, warn, determine origins, block, filter, remove, refute, guide public opinion, remediate, penalize, and other measures to eliminate information conflict in cyberspace.

3. Organizations and individuals, within the scope of their tasks and powers, shall:

a) Prevent information conflict in cyberspace from their information systems; cooperate in determining sources, pushing back, and remediating consequences of cyberattacks performed through information systems of domestic and foreign organizations and individuals;

b) Prevent the activities of domestic and foreign organizations and individuals with the purpose of creating information conflict in cyberspace;

c) Eliminate the organization of implementing posting and dissemination of information in cyberspace having serious influence on national defense, national security, social order, and safety of domestic and foreign organizations and individuals.

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

4. The Government shall detail this Article.

Chapter IV
CYBERSECURITY PROTECTION ACTIVITIES

Article 23. Deployment of cybersecurity protection activities in State regulatory authorities, political organizations, and socio-political organizations at central and local levels

1. Contents of deployment of cybersecurity protection activities include:

a) Building and perfecting regulations and statutes on the use of internal computer networks and computer networks connected to the Internet; plans for ensuring cybersecurity for information systems; plans for response to and remediation of cybersecurity incidents;

b) Applying and deploying plans, measures, and technologies for protecting cybersecurity for information systems and information and documents stored, drafted, and transmitted on information systems under management scope;

c) Organizing training on cybersecurity knowledge for cadres, civil servants, public employees, and workers; improving cybersecurity protection capacity for cybersecurity protection forces;

d) Protecting cybersecurity in activities of providing public services in cyberspace, providing, exchanging, and collecting information with authorities, organizations, and individuals, sharing information internally and with other authorities or in other activities prescribed by the Government:

dd) Investing in and building physical infrastructure facilities suitable to conditions ensuring the deployment of cybersecurity protection activities for information systems;

e) Inspecting cybersecurity for information systems; preventing and combating acts of violating the law on cybersecurity; responding to and remediating cybersecurity incidents.

2. Heads of authorities and organizations are responsible for deploying cybersecurity protection activities under their management.

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

1. Cybersecurity protection for national cyberspace infrastructure and international network gateways must ensure a close combination between requirements of cybersecurity protection and requirements of socio-economic development; encourage international gateways located in the territory of

LuatVietnam
Tiện ích văn bản luật

Vietnam; and encourage organizations and individuals to participate in investing in building national cyberspace infrastructure.

2. Authorities, organizations, and individuals managing and exploiting national cyberspace infrastructure and international network gateways shall:

a) Protect cybersecurity under their management; be subject to management, inspection, and examination and implement requirements on cybersecurity protection of competent State regulatory authorities;

b) Create conditions and implement necessary technical and professional measures for competent State regulatory authorities to perform cybersecurity protection tasks when requested.

Article 25. Assurance of cyberinformation security

1. Websites, web portals, or specialized pages on social networks of authorities, organizations, and individuals must not provide, post, or transmit the information prescribed in Clauses 1, 2, 3, Article 13 and Clause 1, Article 15 of this Law and other information undermining national security.

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

a) Authenticate information when users register digital accounts; secure user information and accounts; provide user information to the specialized cybersecurity protection force under the Ministry of Public Security no later than 24 hours from the time of receiving a request in writing or via email, telephone, or other confirmed forms of exchange for the verification, investigation, and handling of acts of violating the law on cybersecurity; in emergency cases threatening to undermine national security, threatening human life, the request for providing information is no later than 03 hours;

b) Prevent the sharing of information, delete information, and remove services or applications with contents violating the regulations of this Law no later than 24 hours from the time of receiving a request from the specialized cybersecurity protection force under the Ministry of Public Security and save system logs for the verification, investigation, and handling of acts of violating the law on cybersecurity for a period prescribed by the law regulations; in emergency cases threatening to undermine national security, the request for preventing and deleting information is no later than 06 hours;

c) Not provide or cease providing services on telecommunications networks, the Internet, and value-added services to organizations and individuals posting on cyberspace the information prescribed in Clauses 1, 2, and 3, Article 13, and Clause 1 and Clause 2, Article 14 of this Law upon the request of the specialized cybersecurity protection force under the Ministry of Public Security;

LuatVietnam
Tiện ích văn bản luật

d) Store personal information of service users and data created by service users, including account names, service usage time, service fee payment information, access IP addresses, and other relevant data for a period prescribed by the law regulations after users finish using the service.

3. Domestic and foreign enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam having activities of collecting, exploiting, analyzing, and processing data on personal information, data on relationships of service users, and data created by service users in Vietnam must apply data protection measures prescribed by the law regulations and store this data in Vietnam for a period prescribed by the Government.

Foreign enterprises prescribed in this Clause must establish branches or representative offices in Vietnam.

4. The Government shall detail Clause 2 and Clause 3 of this Article.

Article 26. Assurance of data security

1. Assurance of data security is the totality of technical, organizational, and legal measures to protect data and prevent and combat infringement upon data security.

LuatVietnam.vn

2. Contents of assurance of data security include:

a) Building policies and establishing processes on assurance of data security;

b) Applying measures, standards, and technical regulations prescribed by the law on cybersecurity;

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

d) Deploying mechanisms to strictly control personnel directly engaged in data processing:

dd) Inspecting and assessing risks periodically to detect, prevent, and handle timely risks of threatening data security;

e) Inspecting and assessing cross-border data transfer; conditions ensuring data security in important information systems relating to national security, databases, data centers, and data storage systems;

g) Other contents prescribed by the law regulations.

3. The Government shall detail Clause 2 of this Article; and prescribe responsibilities for assurance of data security.

Chapter V

LuatVietnam
Tiện ích văn bản luật

CYBERSECURITY STANDARDS, TECHNICAL REGULATIONS, PRODUCTS, AND SERVICES

Article 27. Cybersecurity standards and technical regulations

1. Cybersecurity standards and cybersecurity technical regulations are applied to information systems, hardware, software, cybersecurity management and operation systems, cybersecurity products and services, information technology, and network-connected devices.

2. Certification of cybersecurity conformity, declaration of cybersecurity conformity, certification of cybersecurity standard conformity, and declaration of cybersecurity standard conformity shall be implemented prescribed by the law on standards and technical regulations.

3. Assessment of standard conformity and regulation conformity regarding cybersecurity for important information systems relating to national security and for the purpose of State-level governance of cybersecurity shall be performed at conformity certification organizations designated by the Minister of Public Security.

4. The Ministry of Public Security shall:

a) Build drafts of national standards on cybersecurity;

b) Manage the quality of cybersecurity products and services, other than civil cryptographic products and services;

c) Register, designate, and manage the operation of cybersecurity conformity certification organizations, unless otherwise prescribed in Clause 6 of this Article.

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

6. The Ministry of National Defence shall register, designate, and manage the operation of cybersecurity conformity certification organizations in the military field.

The Government Cipher Committee shall assist the Minister of National Defense in performing quality management of civil cryptographic products and services; and register, designate, and manage the operation of cybersecurity conformity certification organizations for civil cryptographic products and services.

Article 28. Cybersecurity products and services

1. Cybersecurity products include:

a) Civil cryptographic products;

LuatVietnam
Tiện ích văn bản luật

b) Cybersecurity inspection and assessment products;

c) Cybersecurity supervision products;

d) Anti-attack and anti-intrusion products;

dd) Other cybersecurity products.

2. Cybersecurity services include:

a) Cybersecurity inspection and assessment services;

b) Information security services not using civil cryptography;

c) Civil cryptographic services;

d) Cybersecurity consulting services:

dd) Cybersecurity supervision services;

e) Cybersecurity incident response services;

g) Data recovery services;

h) Cyberattack prevention and combat services;

i) Other cybersecurity services.

3. The Government shall detail this Article.

LuatVietnam.vn

Article 29. Trading in cybersecurity products and services

1. Enterprises trading in cybersecurity products and services must have a license for trading in cybersecurity products and services.

2. Enterprises trading in cybersecurity products and services shall:

a) Implement correctly the license for trading in cybersecurity products and services; comply with the law on cybersecurity and other relevant law regulations;

b) Ensure the quality of cybersecurity products and services consistent with the announced applicable standards and corresponding technical regulations prescribed by the law on product and goods quality and the law on standards and technical regulations before circulation on the market;

c) Create, keep, and secure customer information, and manage dossiers and documents on technical and technological solutions of products and service provision activities prescribed by the law regulations;

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

LuatVietnam
Tiện ích văn bản luật

dd) Coordinate, create conditions, and implement requests of the specialized cybersecurity protection force to implement cybersecurity protection measures.

3. The Government shall prescribe the issuance, temporary suspension, and revocation of licenses for trading in cybersecurity products and services; prescribe the import and export of cybersecurity products; and prescribe the trading in cybersecurity products and services.

Chapter VI

FORCES AND CONDITIONS ENSURING CYBERSECURITY

Article 30. Cybersecurity protection forces

1. Cybersecurity protection forces include:

a) Specialized cybersecurity protection forces arranged at the Ministry of Public Security and the Ministry of National Defence;

b) Cybersecurity protection forces arranged at Ministries, sectoral authorities, provincial-level People's Committees, and authorities and organizations directly managing important information systems relating to national security;

LuatVietnam.vn

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

2. The Government shall detail Clause 1 of this Article; and prescribe the coordination among cybersecurity protection forces.

Article 31. Assurance of human resources for cybersecurity protection

1. The State shall train and develop human resources for cybersecurity protection ensuring quantity and quality, meeting the requirements of national cybersecurity protection capacity.

2. Specialized cybersecurity protection forces shall be prioritized for personnel arrangement according to job positions and title standards, and be subject to mechanisms for recruitment, admission, employment, training, fostering, remuneration, and attraction of talent according to specific policies prescribed by the Government.

3. Owners of important information systems relating to national security shall:

a) Arrange specialized divisions or personnel suitable to the protection level of the system;

LuatVietnam
Tiện ích văn bản luật

b) Ensure persons performing cybersecurity tasks meet professional and vocational standards;

c) Regularly foster and update skills for personnel related to operation, supervision, rescue, and handling of network incidents.

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

1. Vietnamese citizens who have sufficient standards regarding moral qualities, health, qualifications, and knowledge of cybersecurity and information technology, and who have aspirations may be recruited into the cybersecurity protection force.

2. To prioritize training and developing high-quality cybersecurity protection forces; to discover young talents in cybersecurity and information technology for study orientation, recruitment, attraction, and utilization in the field of cybersecurity.

3. To prioritize the development of cybersecurity training institutions reaching international standards; to encourage linkages and creation of cooperation opportunities on cybersecurity between the public sector and the private sector, domestically and abroad.

LuatVietnam.vn

Article 33. Education and fostering of cybersecurity knowledge and professional skills

1. The content of education and fostering of cybersecurity knowledge shall be included in the subject of national defense and security education in schools and the program for fostering national defense and security knowledge prescribed by the Law on National Defense and Security Education.

2. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in fostering cybersecurity professional skills for the cybersecurity protection force and civil servants, public employees, and workers engaged in cybersecurity protection.

The Ministry of National Defence shall organize fostering of cybersecurity professional skills for subjects under its management scope.

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

1. Cybersecurity protection forces prescribed at Point a and Point b, Clause 1, Article 30 of this Law must meet requirements for in-depth cybersecurity knowledge and skills.

2. Persons directly administering and operating information systems of Level 3, Level 4, and Level 5 in State regulatory authorities, organizations, and enterprises must be trained in in-depth cybersecurity knowledge and skills and be

LuatVietnam
Tiện ích văn bản luật

issued with certificates, unless for individuals already trained in cybersecurity majors.

3. The Ministry of Public Security shall assume the prime responsibility for, and coordinate with relevant Ministries and sectoral authorities in organizing training on in-depth cybersecurity knowledge and skills, unless otherwise prescribed in Clause 4 of this Article.

4. The Ministry of National Defence shall organize training on in-depth cybersecurity knowledge and skills for subjects under its management scope.

5. The Government shall prescribe standards for in-depth cybersecurity knowledge and skills; and programs and contents of training on in-depth cybersecurity knowledge and skills.

Article 35. Dissemination of cybersecurity knowledge

1. The State has policies to disseminate cybersecurity knowledge nationwide, encouraging State regulatory authorities to coordinate with private organizations and individuals to implement education programs and raise awareness about cybersecurity; prioritizing dissemination and guidance for children, the elderly, and persons with difficulties in cognition to improve the ability to self-protect their rights and legitimate interests in cyberspace.

2. Ministries, sectoral authorities, authorities, and organizations are responsible for building and deploying activities to disseminate cybersecurity knowledge to cadres, civil servants, public employees, and workers within their Ministries, sectoral authorities, authorities, and organizations.

3. Provincial-level People's Committees are responsible for building and deploying activities to disseminate knowledge and raise awareness about cybersecurity for authorities, organizations, and individuals in their localities.

Article 36. Cybersecurity research and development

1. Contents of cybersecurity research and development include:

a) Building systems of software and equipment for protecting cybersecurity;

b) Methods for appraising software and equipment for protecting cybersecurity to meet standards and limit the existence of security weaknesses, vulnerabilities, and malware;

c) Methods for inspecting hardware and software supplied to ensure they perform correct functions;

d) Methods for protecting state secrets, work secrets, trade secrets, personal secrets, family secrets, and privacy; and security capabilities when transmitting information in cyberspace:

dd) Determining the origin of information transmitted in cyberspace;

LuatVietnam
Tiện ích văn bản luật

e) Resolving risks of threatening cybersecurity;

g) Building cyber ranges and cybersecurity testing environments;

h) Technical initiatives to improve awareness and skills regarding cybersecurity;

i) Cybersecurity forecasting;

k) Researching practice and developing cybersecurity theory.

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

Article 37. Improving cybersecurity autonomy capacity

1. The State encourages and creates conditions for authorities, organizations, and individuals to improve cybersecurity autonomy capacity and improve the ability to manufacture, inspect, assess, and verify digital devices, network services, and network applications.

2. The Government shall implement the following measures to improve cybersecurity autonomy capacity for authorities, organizations, and individuals:

a) Directing the formulation of policies, strategies, and plans for cybersecurity industry development; standards and technical regulations for hardware and software products to proactively eliminate cybersecurity risks right from product formation;

b) Promoting transfer, research, mastery, and development of security industry technologies, products, and services to protect cybersecurity;

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

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

dd) Strengthening the business environment and improving competitive conditions to support enterprises researching and producing products, services, and applications to protect cybersecurity.

3. Activities of investment and attraction of resources for developing cybersecurity industry infrastructure include:

a) Activities of investing in building cybersecurity industry infrastructure are business lines eligible for special investment incentives, enjoying incentives and support prescribed by the law on investment, tax, land, and other relevant laws;

b) The State prioritizes the allocation of budget capital to invest in building cybersecurity industry infrastructure including: Facilities for research, design, production, and testing of cybersecurity products and services; Key national

LuatVietnam
Tiện ích văn bản luật

laboratories on cybersecurity; Facilities for measurement, testing, and assessment of cybersecurity products and services; Big data centers; Concentrated cybersecurity industrial zones; and Cybersecurity industrial complexes;

c) Cybersecurity industry infrastructure invested by the State prescribed at Point b of this Clause is a type of infrastructure asset and is managed, exploited, and operated prescribed by the law on management and use of public assets;

d) Organizations and enterprises are permitted to import technological lines, equipment, machinery, and tools for the purpose of training, research, and development of cybersecurity products and services:

dd) State regulatory authorities, organizations, and enterprises shall prioritize the use of domestic cybersecurity products and services.

4. The Ministry of Public Security shall advise the Government to plan, build, and develop cybersecurity industry infrastructure to improve cybersecurity autonomy capacity.

Article 38. Funding for cybersecurity protection

1. State regulatory authorities, organizations, and enterprises, political organizations, socio-political organizations, and public non-business units guaranteed by the state budget must arrange funding for cybersecurity protection in the estimates for implementing tasks of digital transformation and information technology application annually of their authorities, organizations, and units; arranging a minimum of 15% of the total funding for implementing programs, schemes, and projects on investment in digital transformation and information technology application to protect cybersecurity.

2. Authorities, organizations, and units not falling within the regulations in Clause 1 of this Article shall self-guarantee funding for cybersecurity protection for their authorities, organizations, and units.

Chapter VII

RESPONSIBILITIES OF AUTHORITIES, ORGANIZATIONS, AND INDIVIDUALS REGARDING CYBERSECURITY

Article 39. Responsibilities for State-level governance of cybersecurity

1. The Government performs unified State-level governance of cybersecurity.

2. The Ministry of Public Security is the focal authority assisting the Government in performing State-level governance of cybersecurity; and is responsible before the Government for performing the following contents of

LuatVietnam
Tiện ích văn bản luật

State-level governance of cybersecurity, other than contents prescribed in Clause 3 and Clause 4 of this Article:

a) Promulgating or submitting to competent State regulatory authorities to promulgate and guide the implementation of legal normative documents on cybersecurity;

b) Building and proposing strategies, guidelines, policies, plans, and schemes for cybersecurity protection; researching, building, developing, and using security cryptography to protect data security under the management scope of the Ministry of Public Security;

c) Coordinating with relevant authorities to organize propaganda and refutation of information opposing the State of the Socialist Republic of Vietnam prescribed in Clause 1, Article 13 of this Law;

d) Requesting enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace, and information system managers to eliminate information violating the law on cybersecurity on services and information systems directly managed by enterprises, authorities, and organizations:

dd) Preventing and struggling against activities of using cyberspace to undermine sovereignty, interests, national security, social order, safety and preventing and combating cybercrime;

e) Ensuring information security in cyberspace and data security; building mechanisms for managing IP address identification; authenticating digital account registration information; warning and sharing cybersecurity information and risks of threatening cybersecurity;

g) Advising and proposing the Government and the Prime Minister to consider and decide on the assignment and coordination of implementing cybersecurity protection measures, and preventing and handling acts that undermine cybersecurity in cases where State-level governance contents relate to the management scope of multiple Ministries and sectoral authorities;

h) Requisitioning experts, scientists, specialized staff, and systems in emergency cases to protect national security and ensure social order and safety in cyberspace;

i) Organizing drills for preventing and combating cyberattacks; and drills for responding to and remediating cybersecurity incidents for important information systems relating to national security;

k) Inspecting, examining, settling complaints and denunciations, and handling violations of the law on cybersecurity.

LuatVietnam.vn
Tiện ích văn bản luật

3. The Ministry of National Defence is responsible before the Government for performing State-level governance of cybersecurity under its management scope as follows:

a) Promulgating or submitting to competent State regulatory authorities to promulgate and guide the implementation of legal normative documents on cybersecurity within its management scope;

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

c) Preventing and struggling against activities of using cyberspace to undermine national security within its management scope;

d) Coordinating with the Ministry of Public Security to organize drills for preventing and combating cyberattacks, drills for responding to and remediating cybersecurity incidents for important information systems relating to national security, and deploying the implementation of cybersecurity protection work;

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

4. The Government Cipher Committee shall assist the Minister of National Defense in performing State-level governance of civil cryptography and cybersecurity under its management scope prescribed by the law regulations.

5. Ministries, ministerial-level authorities, and Government-attached agencies, within the scope of their functions, tasks, and powers, shall implement cybersecurity protection work; and coordinate with the Ministry of Public Security in performing State-level governance of cybersecurity.

6. Provincial-level People's Committees shall implement cybersecurity protection work locally; and coordinate with the Ministry of Public Security in performing State-level governance of cybersecurity.

Article 40. Responsibilities of information system managers in cybersecurity protection

1. Information system managers shall:

a) Implement information system protection prescribed by this Law;

b) Connect cybersecurity supervision systems and centralized malware prevention and combat systems to the National Cybersecurity Center of the Ministry of Public Security or the Cybersecurity Center of the province or city to support cybersecurity supervision;

c) Report cybersecurity incidents to the specialized authority of the Ministry of Public Security or the Ministry of National Defence.

2. Information system managers using the state budget shall implement the responsibilities prescribed in Clause 1 of this Article and shall:

LuatVietnam
Tiện ích văn bản luật

a) Have plans for ensuring cybersecurity appraised regarding cybersecurity by competent State regulatory authorities when establishing, expanding, or upgrading information systems;

b) Designate individuals or divisions in charge of cybersecurity.

Article 41. Responsibilities of enterprises providing services in cyberspace

1. Comply with the law on cybersecurity.

2. Warn of the possibility of loss of cybersecurity in the use of services in cyberspace provided by them and guide preventive measures for service users; build emergency response plans ensuring cybersecurity to proactively handle weaknesses, risks, and cybersecurity incidents.

3. When a cybersecurity incident occurs, immediately deploy emergency response plans ensuring cybersecurity, and simultaneously report immediately to the specialized cybersecurity protection force prescribed by this Law.

4. Apply technical measures and solutions to ensure cybersecurity for data processing activities and personal data processing prescribed by this Law, the law on data, the law on personal data protection, and other relevant law regulations.

5. Be responsible for identifying IP addresses of organizations and individuals using internet services; and provide IP address identification information to the specialized cybersecurity protection force to implement cybersecurity protection measures.

6. Coordinate implementation according to the guidelines of the specialized cybersecurity protection force under the Ministry of Public Security to establish connection systems, connect technical transmission lines, transmit data, and meet other necessary conditions to deploy cybersecurity protection solutions and measures when requested for the investigation, verification, and handling of acts of violating the law on cybersecurity.

7. Enterprises providing services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam are responsible for implementing the regulations in this Article, Clause 2 and Clause 3, Article 25 of this Law.

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

1. Comply with the law on cybersecurity.

2. Be responsible for securing information on registering, opening, managing, and using their digital accounts. In case of using digital accounts to perform acts of violating the law regulations, depending on the nature and severity of the violation, the digital account owner or digital account user shall

LuatVietnam
Tiện ích văn bản luật

be disciplined, administratively sanctioned, or examined for penal liability; if causing damage to the interests of the State or the rights and legitimate interests of organizations and individuals, they must compensate for damage prescribed by the law regulations.

3. Timely provide information related to cybersecurity protection, risks of threatening cybersecurity, and acts that undermine cybersecurity to competent authorities and cybersecurity protection forces.

4. Implement requests and guidelines of competent authorities in cybersecurity protection; and help and create conditions for authorities, organizations, and persons with responsibilities to conduct cybersecurity protection measures.

Chapter VIII
IMPLEMENTATION PROVISIONS

Article 43. Amending and supplementing a number of articles of relevant laws

1. To replace a number of phrases and annul a Clause in the Law No. 33/2024/QH15 on Archives as follows:

a) To replace the phrase "information safety" at Point b, Clause 1, Article 35; the phrase "cyberinformation security" at Point b, Clause 2, Article 36; and the phrase "information safety and security" at Clause 3, Article 60 with the phrase "cybersecurity";

b) To annul Clause 4, Article 58.

2. To replace and remove a number of phrases in the Law on Protection of Consumers' Rights No. 19/2023/QH15 as follows:

a) To replace the phrase "information safety" with the phrase "information security" at Point d, Clause 1, Article 16; the phrase "information safety and security" with the phrase "cybersecurity" at Clause 1, Article 15, the title of Article 19, Clause 1 and Clause 3, Article 19;

b) To remove the phrase "cyberinformation security," at Clause 3, Article 19.

3. To replace a number of phrases in the Law on Fees and Charges No. 97/2015/QH13, of which a number of articles were amended and supplemented under 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.

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

89/2025/QH15, Law No. 94/2025/QH15, Law No. 95/2025/QH15, and Law No. 118/2025/QH15 as follows:

a) To replace the phrase "information safety" with the phrase "cybersecurity" at Subsection 10, Section VI of Part A and Subsection 16, Section III of Part B of Appendix No. 01 - List of fees and charges;

b) To replace the phrase "cyberinformation security" with the phrase "cybersecurity" at Subsection 11, Section VI of Part A of Appendix No. 01 - List of fees and charges.

4. To replace and remove a number of phrases in the Law No. 71/2025/QH15 on Digital Technology Industry as follows:

a) To replace the phrase "information safety" with the phrase "cybersecurity" at Point a, Clause 1, Article 25;

b) To remove the phrase "cyberinformation security," at Article 10.

5. To replace and remove a number of phrases in the Law on Data No. 60/2024/QH15 as follows:

a) To replace the phrase "data safety and security" with the phrase "data security" at Clause 4, Article 25;

b) To replace the phrase "information security and safety" with the phrase "cybersecurity" at Clause 2, Article 33;

c) To remove the phrase ", information safety" at Clause 4, Article 25;

d) To remove the phrase "cyberinformation security," at Clause 4, Article 39:

dd) To remove the phrase "the law on cyberinformation security," at Clause 4, Article 43.

6. To replace and remove a number of phrases in the Law on Cultural Heritage No. 45/2024/QH15, of which a number of articles were amended and supplemented under Law No. 84/2025/QH15 as follows:

a) To replace the phrase "cyberinformation security" with the phrase "cybersecurity" at Clause 4, Article 59;

b) To remove the phrase "cyberinformation security," at Point c, Clause 2, Article 86.

7. To replace and remove a number of phrases in the Law on Telecommunications No. 24/2023/QH15, of which a number of articles were amended and supplemented under Law No. 47/2024/QH15 as follows:

a) To replace the phrase "cyberinformation security" with the phrase "information security" at Clause 8, Article 5;

LuatVietnam.vn
LuatVietnam
Tiện ích văn bản luật

b) To remove the phrase ", cyberinformation security" at the title of Article 5 and Clause 1, Article 5, Point c, Clause 2, Article 38;

c) To remove the phrase "cyberinformation security," at Clause 2, Article 21 and Point b, Clause 2, Article 29.

8. To replace and remove a number of phrases in the Law on E-Transactions No. 20/2023/QH15, of which a number of articles were amended and supplemented under Law No. 60/2024/QH15 as follows:

a) To remove the phrase "cyberinformation security and" in the title of Article 5;

b) To remove the phrase "the law on cyberinformation security," at Clause 1, Article 5;

c) To replace the phrase "cyberinformation security" with the phrase "cybersecurity" at Point c, Clause 1, Article 20, Clause 2, Article 21, Point c, Clause 1, Article 29, Clause 6, Article 30, Clause 4, Article 44, Point a, Clause 4, Article 46, and Point c, Clause 1, Article 47;

d) To remove the phrase "cyberinformation security," at Point d, Clause 1, Article 42 and Point a, Clause 1, Article 47.

9. To replace the phrase "cyberinformation security" with the phrase "cybersecurity" at Point b, Clause 2, Article 12 of the Law on Corporate Income Tax No. 67/2025/QH15; at Clause 1, Article 169 of the Land Law No. 31/2024/QH15, of which a number of articles were amended and supplemented under 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. To replace the phrase "information security and safety" with the phrase "cybersecurity" at Point a, Clause 3, Article 7 of the Law on Water Resources No. 28/2023/QH15, of which a number of articles were amended and supplemented under Law No. 84/2025/QH15.

11. To remove the phrase "cyberinformation security;" at Point dd, Clause 1, Article 24 of the Law on Handling of Administrative Violations No. 15/2012/QH13, of which a number of articles were amended and supplemented under 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. To remove the phrase "cyberinformation security," at Clause 6, Article 16 of the Law on People's Public Security No. 37/2018/QH14, of which a number of articles were amended and supplemented under 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; at Clause 1, Article 66 of the Law on Election of Deputies to

LuatVietnam
Tiện ích văn bản luật

the National Assembly and Deputies to People's Councils No. 85/2015/QH13, of which a number of articles were amended and supplemented under Law No. 83/2025/QH15.

13. To remove the phrase ", information safety" at Clause 3, Article 136 of the Law on Organization of People's Courts No. 34/2024/QH15, of which a number of articles were amended and supplemented under Law No. 81/2025/QH15; at Clause 1, Article 26 of the Law on Electricity No. 61/2024/QH15, of which a number of articles were amended and supplemented under Law No. 94/2025/QH15.

14. To remove the phrase "information safety," at Clause 8, Article 29; the phrase "information safety and" at Clause 2 and Clause 7, Article 29 of the Law on Chemicals No. 69/2025/QH15.

15. To remove the phrase "information safety," at Clause 3, Article 51, Clause 1 and Clause 5, Article 52 of the Bidding Law No. 22/2023/QH15, of which a number of articles were amended and supplemented under Law No. 57/2024/QH15 and Law No. 90/2025/QH15; at Point e, Clause 1, Article 23 of the Law on Civil Defense No. 18/2023/QH15, of which a number of articles were amended and supplemented under Law No. 98/2025/QH15.

16. To remove the phrase ", the law on ensuring information safety" at Clause 4, Article 7 of the Law on Atomic Energy No. 94/2025/QH15.

17. To annul Clause 3, Article 49 of the Law on Libraries No. 46/2019/QH14.

Article 44. Effect

1. This Law takes effect on July 01, 2026.

2. The Law on Cyberinformation Security No. 86/2015/QH13, of which a number of articles were amended and supplemented under Law No. 35/2018/QH14; Law on Cybersecurity No. 24/2018/QH14 shall cease to be effective from the effective date of this Law.

Article 45. Transitional provisions

1. Information systems already determined with levels in accordance with the Law on Cyberinformation Security No. 86/2015/QH13, of which a number of articles were amended and supplemented under Law No. 35/2018/QH14, shall continue to have their determined levels kept from the effective date of this Law; within 12 months from the effective date of this Law, conditions, standards, and measures for cybersecurity protection must be ensured corresponding to the level prescribed by this Law.

2. Types of licenses for trading in cyberinformation security products and services and civil cryptography specified in the Law on Cyberinformation Security No. 86/2015/QH13, of which a number of articles were amended and

LuatVietnam
Tiện ích văn bản luật

supplemented under Law No. 35/2018/QH14, that are granted before the effective date of this Law shall be valid for use until the end of the term recorded on the license.

3. Products, services, solutions, and technical means for ensuring cyberinformation security as prescribed in the Law on Cyberinformation Security No. 86/2015/QH13, of which a number of articles were amended and supplemented under Law No. 35/2018/QH14 that are put into use before the effective date of this Law shall continue to be used; within 12 months from the effective date of this Law, cybersecurity conditions must be ensured prescribed by this Law.

This Law was passed on December 10, 2025, by the 15th National Assembly of the Socialist Republic of Vietnam at its 10th session.

Chairman of the National Assembly

TRAN THANH MAN

LuatVietnam.vn

LuatVietnam
Tiện ích văn bản luật