

GOVERNMENT OF VIETNAM

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

No. 333/2026/ND-CP

Hanoi, August 19, 2026

DECREE

ELABORATING ON LAW ON CYBERSECURITY

Pursuant to the Law on Government Organization No. 63/2025/QH15;

Pursuant to the Law on National Security No. 32/2004/QH11;

Pursuant to the Law on Cybersecurity No. 116/2025/QH15;

At the request of the Minister of Public Security of Vietnam;

The Government of Vietnam hereby promulgates the Decree elaborating on the Law on Cybersecurity.

Chapter I

GENERAL PROVISIONS

Article 1. Scope

1. This Decree elaborates on Points a, b, c, d, dd, g, k, l, and m Clause 1 Article 5, Clause 4 Article 25, and Clause 5 Article 34 of the Law on Cybersecurity, including the following contents:

a) Contents, procedures, and competence for applying cybersecurity protection measures, including: cybersecurity appraisal; assessment of cybersecurity conditions; cybersecurity inspection; cybersecurity supervision; response to and remediation of cybersecurity incidents; cybersecurity protection operations; use of cryptography to protect network information; requests for removal of illegal or false information and fake news in cyberspace that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals; collection of electronic data related to activities infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace; termination or suspension of, or requests for cessation of operation of, information systems, and revocation of domain names in accordance with the law;

b) Assurance of cyber information security as prescribed in Clauses 2 and 3 Article 25 of the Law on Cybersecurity;

c) Standards for specialized cybersecurity knowledge and skills; programs and contents of certification training in specialized cybersecurity knowledge and skills.

2. This Decree provides for measures to implement the IP address identification management mechanism applicable to enterprises providing telecommunications and Internet services.

Article 2. Regulated entities and application principles

1. This Decree applies to Vietnamese agencies, organizations, and individuals; foreign agencies, organizations, and individuals in Vietnam; persons of Vietnamese origin whose nationality has not yet been determined and who are residing in Vietnam and have been issued identity certificates; and foreign agencies, organizations, and individuals that directly participate in or are involved in cybersecurity protection activities in Vietnam.

2. The Ministry of National Defense of Vietnam shall manage cybersecurity relating to military and national defense duties; the Ministry of Public Security of Vietnam shall, within its competence, manage cybersecurity relating to the civil and economic activities of military units. For overlapping matters, if any, the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam shall reach agreement by means of regulations on cooperation.

Article 3. Interpretation of terms

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

1. Service user refers to an organization or individual that uses services in cyberspace.
2. Service user in Vietnam refers to an organization or individual that uses cyberspace services within the territory of the Socialist Republic of Vietnam.
3. Services on telecommunications networks refer to telecommunications services and telecommunications application services as prescribed by law.
4. Services on the Internet refer to Internet services and information content services on mobile telecommunications networks as prescribed by law.
5. Value-added services in cyberspace refer to value-added telecommunications services as prescribed by law.
6. Acts in violation of cyber information security laws refer to acts in violation of cybersecurity laws arising from activities to ensure cyber information security, which are committed through cyberspace, information systems, information technology, electronic equipment, or digital devices and fall within the cases prescribed in Article 7 or Article 13 of the Law on Cybersecurity.

7. Cybersecurity major refers to a training major within the groups of majors in cybersecurity and information security, or the major in cybersecurity and the prevention and combat of high-tech crime.

8. Security cryptography refers to cryptographic techniques and products researched, constructed, and developed by the Ministry of Public Security of Vietnam and used to secure or authenticate data within the management scope of the Ministry of Public Security of Vietnam.

Chapter II

PROCEDURES FOR APPLYING CERTAIN CYBERSECURITY PROTECTION MEASURES

Article 4. Principles for application of cybersecurity protection measures

1. The application of cybersecurity protection measures shall comply with the Constitution and the law and ensure the interests of the State and the lawful rights and interests of agencies, organizations, and individuals.
2. Cybersecurity protection measures may only be applied for the proper purposes, to the proper entities, by the competent authorities, and in accordance with the procedures prescribed by law; they may only be implemented after a written approval decision has been issued by a competent person.

Article 5. Procedures for cybersecurity appraisal of information systems important to national security

1. Cybersecurity appraisal shall be conducted for designs, schemes, plans, and solutions for the new construction, upgrading, or expansion of information systems important to national security before their approval to examine and assess whether such information systems satisfy cybersecurity requirements.
2. Where the results of the determination of the information system level have clarified the requirements, scope, contents, and level of cybersecurity assurance applicable to an information system, the competent authority shall adopt and use the contents already assessed and concluded and shall not reappraise such contents unless a change affects the information system level or the degree of importance of the information system to national security.
3. Subjects of cybersecurity appraisal include:
 - a) Detailed design dossiers of investment projects for the new construction, upgrading, or expansion of information systems;
 - b) Schemes, plans, and solutions for the upgrading or expansion of information systems.
4. Contents of cybersecurity appraisal include:

- a) Compliance with cybersecurity regulations, standards, technical regulations, and conditions in the design, construction, upgrading, or expansion of information systems;
- b) The conformity of the cybersecurity protection plan and the plan for response to and remediation of cybersecurity incidents;
- c) The arrangement of human resources, technical conditions, and management measures for the cybersecurity protection of information systems;
- d) Other contents directly related to cybersecurity protection requirements applicable to the information system subject to appraisal.

5. Competence to conduct cybersecurity appraisal is prescribed as follows:

- a) The Ministry of Public Security of Vietnam shall conduct cybersecurity appraisal of information systems important to national security, except for the cases prescribed in Points b and c of this Clause;
- b) The Ministry of National Defense of Vietnam shall conduct cybersecurity appraisal of military information systems;
- c) The Government Cipher Committee shall conduct cybersecurity appraisal of cipher information systems under the Government Cipher Committee.

6. A dossier of request for cybersecurity appraisal includes:

- a) A written request for cybersecurity appraisal, made according to Form No. 01 in the Appendix promulgated together with this Decree;
- b) Dossiers and documents concerning the subject of cybersecurity appraisal, including: detailed design dossiers of investment projects for the new construction, upgrading, or expansion of information systems; and schemes, plans, and solutions for the upgrading or expansion of information systems;
- c) Documents presenting the results of the determination of the cybersecurity level of the information system;
- d) Other documents related to the requested appraisal contents, if any.

7. The procedures for cybersecurity appraisal shall be carried out as follows:

- a) After the information system level has been determined in accordance with the law, the information system administrator shall submit 1 dossier of request for cybersecurity appraisal to the competent authority prescribed in Clause 5 of this Article;

b) Within 3 working days from the date of receipt of the dossier, the competent authority shall examine the validity of the dossier. If the dossier is valid, the authority shall issue a dossier receipt immediately upon completion of the examination. If the dossier is invalid, the authority shall issue a written notice requesting the information system administrator to supplement and complete the dossier;

c) Within a maximum of 25 working days from the date of issuance of the receipt for a valid dossier, the competent authority shall conduct the cybersecurity appraisal and notify the information system administrator in writing of the appraisal results.

8. Where it is necessary to determine the conformity between the actual state of an information system and the dossier of request for appraisal, the competent authority shall conduct an on-site survey and assessment of the information system. The on-site survey and assessment shall not affect the normal operations of the information system administrator or the information system subject to appraisal. The on-site survey and assessment period shall not exceed 7 working days and shall not be included in the appraisal period prescribed in Point c Clause 7 of this Article.

9. The results of cybersecurity appraisal shall serve as the basis for the information system administrator to complete the cybersecurity assurance plan and submit it to the competent authority for approval or to carry out subsequent steps in accordance with the law.

10. Dossiers, documents, information, and results of cybersecurity appraisal shall be managed and protected in accordance with the law on protection of state secrets, the law on cybersecurity, and other relevant laws.

Article 6. Procedures for assessment of cybersecurity conditions for information systems important to national security

1. Assessment of cybersecurity conditions refers to a procedure conducted by a competent authority to examine and determine the extent to which an information system important to national security satisfies cybersecurity conditions before it is put into operation and use.

2. An information system important to national security shall be assessed and certified as eligible for cybersecurity before being put into operation and use. The information system administrator shall maintain the satisfaction of cybersecurity conditions throughout the management, operation, and utilization of the system.

3. An information system important to national security shall be assessed as eligible for cybersecurity when it satisfies the following requirements:

a) Having regulations, processes, and plans for ensuring cybersecurity that comply with the law on cybersecurity, the law on protection of state secrets, cybersecurity standards and technical regulations, and relevant specialized technical standards;

b) Clearly identifying the information system, information, data, technical infrastructure, and important components requiring priority protection; processes for managing, operating, utilizing,

using, and protecting the information system, data, and technical infrastructure; and the responsibilities of each division and individual for managing, operating, and using the system;

c) Having a division or personnel responsible for system operation and administration and cybersecurity protection; personnel performing these duties shall possess appropriate professional qualifications in cybersecurity, information technology, or a relevant technical field and shall be responsible for maintaining the confidentiality of information relating to the information system both during and after the performance of their duties;

d) Clearly defining the functions, duties, entitlements, and responsibilities relating to system operation and administration and cybersecurity protection; ensuring cross-control, limiting conflicts of duties, and satisfying cybersecurity protection requirements;

dd) Ensuring that equipment, hardware, software, databases, source code, application programs, development tools, and other technical components of the system are inspected, managed, reviewed, and updated and that weaknesses, security vulnerabilities, malicious software, malicious hardware, and cybersecurity threats are remedied before such components are put into use and throughout their operation;

e) Products, equipment, hardware, and software for which the specialized cybersecurity protection forces have issued warnings or notices regarding cybersecurity risks shall not be put into use or may only be put into use after measures have been taken to handle and remedy such risks;

g) Having measures to manage, inspect, and control the connection, use, transportation, storage, repair, and destruction of information technology equipment, communication equipment, information-bearing objects, mobile devices, and information storage devices and equipment serving the operation of the information system;

h) Having technical measures to supervise, detect, warn of, prevent, handle, and remedy cybersecurity threats and cybersecurity incidents; separating the production environment from development, inspection, and testing environments; and controlling the installation and use of software, services, tools, and devices on the system;

i) Having a data backup plan and testing data recovery capabilities; segmenting networks based on users, purposes of use, and the degree of importance of system resources; and controlling connections and access between network segments and important system resources;

k) Having solutions to detect and prevent untrusted access, illegal infiltration, denial-of-service attacks, and other forms of cyberattack; and to scan for, detect, issue warnings of, and handle weaknesses, technical vulnerabilities, connections, devices, and software illegally installed on the system;

l) Recording, managing, and storing system logs concerning the information system, users, errors, and cybersecurity incidents in accordance with the law, relevant standards and technical regulations, and cybersecurity protection requirements;

m) Having measures for account management, authorization, access control, secret key management, and authentication methods; controlling the creation, issuance, use, and supervision of accounts with administrative privileges; and reviewing, inspecting, and reapproving users' access rights;

n) Having measures to ensure physical security at system installation locations, data centers, server areas, network equipment areas, storage equipment areas, and critical technical areas; ensuring power supply and systems supporting continuous operation; controlling entry and exit; and preventing risks of illegal infiltration or information collection using technical equipment or devices;

o) The processing, storage, and transmission of information classified as state secrets on an information system shall comply with the laws on protection of state secrets, cipher, and cybersecurity and other relevant laws. Information systems processing state secrets shall be subject to protection measures appropriate to the level of secrecy and cybersecurity protection requirements.

4. The contents of an assessment of cybersecurity conditions include examining and determining the extent to which the conditions prescribed in Clause 3 of this Article and other requirements directly related to ensuring cybersecurity for the information system subject to assessment are satisfied.

5. Competence to assess and certify eligibility for cybersecurity is prescribed as follows:

a) The Ministry of Public Security of Vietnam shall assess and certify eligibility for cybersecurity of information systems important to national security, except for the cases prescribed in Points b and c of this Clause;

b) The Ministry of National Defense of Vietnam shall assess and certify eligibility for cybersecurity of military information systems;

c) The Government Cipher Committee shall assess and certify eligibility for cybersecurity of cipher information systems under the Government Cipher Committee.

6. A dossier of request for an assessment of cybersecurity conditions includes:

a) A written request for certification of eligibility for cybersecurity, made according to Form No. 02 in the Appendix promulgated together with this Decree;

b) The feasibility study report, technical design dossier, construction drawing design dossier, or equivalent documents of the project for investment in the construction, upgrading, or expansion of the information system;

c) The dossier on cybersecurity assurance solutions for the information system important to national security;

d) Documents presenting the results of cybersecurity appraisal, if any;

dd) Other documents related to the requested assessment contents, if any.

7. The procedures for assessment of cybersecurity conditions shall be carried out as follows:

a) The information system administrator shall submit 1 dossier of request for an assessment of cybersecurity conditions to the competent authority prescribed in Clause 5 of this Article;

b) Within a maximum of 3 working days from the date of receipt of the dossier, the competent authority shall examine the validity of the dossier. If the dossier is valid, the authority shall issue a dossier receipt immediately upon completion of the examination. If the dossier is invalid, the authority shall issue a written notice requesting the information system administrator to supplement and complete the dossier;

c) Within a maximum of 25 working days from the date of issuance of the receipt for a valid dossier, the competent authority shall conduct the assessment of cybersecurity conditions;

d) Where the information system fully satisfies the cybersecurity conditions, the head of the competent authority shall issue a Certificate of Eligibility for Cybersecurity for the information system;

dd) Where the information system does not yet satisfy the cybersecurity conditions, the competent authority shall issue a written notice specifying the unsatisfied conditions and requesting the information system administrator to supplement, complete, upgrade, and remedy the system before putting it into operation and use.

8. The information system administrator shall supplement, complete, upgrade, and remedy the unsatisfied contents as requested by the competent authority under Point dd Clause 7 of this Article and ensure that the information system satisfies the cybersecurity conditions before putting it into operation and use.

9. The maintenance of the information system's cybersecurity conditions shall be subject to inspection and post-inspection in accordance with the law. Where the information system administrator fails to comply or fully comply with the requirements prescribed in Clause 8 of this Article but puts the information system into operation and use, it shall be handled in accordance with the law.

10. The Certificate of Eligibility for Cybersecurity shall serve as the basis for the information system administrator to put the information system important to national security into operation and use in accordance with the law.

11. Dossiers, documents, information, and results of the assessment of cybersecurity conditions shall be managed and protected in accordance with the law on protection of state secrets, the law on cybersecurity, and other relevant laws.

Article 7. Procedures for cybersecurity supervision

1. Cybersecurity supervision refers to the collection, receipt, analysis, and processing of information to detect and issue warnings of cybersecurity threats, cybersecurity incidents, weaknesses, security vulnerabilities, malicious software, and malicious hardware for timely prevention, blocking, handling, and remediation.

2. An information system administrator shall organize cybersecurity supervision of information systems within its management scope; develop mechanisms for self-supervision, automatic warnings, and receipt of warnings of cybersecurity threats, cybersecurity incidents, weaknesses, and security vulnerabilities; and maintain a cybersecurity supervision system and a centralized malicious software prevention and combat system that satisfy the requirements for connection and sharing of data on warnings of cybersecurity threats and incidents with competent authorities in accordance with the law.

3. For an information system important to national security, the information system administrator shall regularly cooperate with the specialized cybersecurity protection forces in organizing cybersecurity supervision and ensure the technical conditions, human resources, and information necessary for cybersecurity supervision activities as required for national security protection.

4. The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall conduct cybersecurity supervision of the following subjects, except for military information systems and cipher information systems under the Government Cipher Committee:

- a) National cyberspace;
- b) Information systems important to national security, in accordance with its assigned functions and duties;
- c) Information systems of agencies and organizations within the political system, in accordance with its assigned functions and duties;
- d) Other information systems where necessary in accordance with the Law on Cybersecurity.

5. The procedures for the specialized cybersecurity protection forces to conduct cybersecurity supervision are prescribed as follows:

- a) Before implementing a cybersecurity supervision measure, the specialized cybersecurity protection forces shall notify the information system administrator in writing of the reasons, scope, contents, duration, and requirements for cooperation in supervision, except in an emergency involving the protection of national security;
- b) In an emergency where prior notice cannot be given, the specialized cybersecurity protection forces shall immediately implement the cybersecurity supervision measure and send a written notice to the information system administrator within 24 hours from the time of implementation;

c) The specialized cybersecurity protection forces shall implement technical measures for cybersecurity supervision within the notified scope and contents or as required to handle the emergency;

d) Information collected during the supervision process shall be analyzed and assessed to promptly detect and issue warnings of cybersecurity threats, cybersecurity incidents, weaknesses, security vulnerabilities, malicious software, and malicious hardware;

dd) Upon detecting a cybersecurity threat, a cybersecurity incident, or signs of impact on national security or social order and safety, the specialized cybersecurity protection forces shall promptly notify the information system administrator for cooperation in handling and remediation;

e) The results of cybersecurity supervision shall be compiled and notified to the information system administrator to the extent necessary and reported to the competent authority in accordance with the law.

6. During cybersecurity supervision, the information system administrator shall:

a) Cooperate with the specialized cybersecurity protection forces in implementing cybersecurity supervision measures;

b) Ensure the technical conditions necessary for cybersecurity supervision activities in accordance with lawful requests of the specialized cybersecurity protection forces;

c) Provide and update information relating to the configuration, connection, and operation of the information system at the request of a competent authority;

d) Receive and handle warnings of cybersecurity threats and cybersecurity incidents and implement remedial measures as requested by the specialized cybersecurity protection forces.

7. Telecommunications enterprises and enterprises providing Internet and information technology services shall cooperate with, provide necessary technical information and data to, and assist the specialized cybersecurity protection forces in cybersecurity supervision activities in accordance with the law.

8. Cybersecurity supervision shall be conducted within the proper competence and scope and for the proper purposes and cybersecurity protection requirements and shall not unlawfully affect the normal operations of agencies, organizations, individuals, or the information systems subject to supervision.

9. Information, documents, and data collected from cybersecurity supervision activities shall be managed, used, and protected in accordance with the law on protection of state secrets, the law on cybersecurity, and other relevant laws.

Article 8. Procedures for cybersecurity inspection of information systems important to national security

1. Cybersecurity inspection refers to activities that determine the current cybersecurity status of an information system, its infrastructure, and information stored, processed, or transmitted therein to prevent, detect, and handle cybersecurity threats and cybersecurity incidents and propose measures to ensure the safe and continuous operation of the information system.

2. An information system important to national security shall undergo cybersecurity inspection in the following cases:

- a) When electronic equipment or cybersecurity services are put into use in the information system;
- b) When a change in the current status of the information system affects cybersecurity assurance requirements;
- c) During regular annual inspections;
- d) During an ad hoc cybersecurity inspection upon the occurrence of a cybersecurity incident or an act infringing upon cybersecurity; when required for the state management of cybersecurity; or upon expiry of the period for remedying weaknesses or security vulnerabilities as required or recommended by the specialized cybersecurity protection forces.

3. Subjects of cybersecurity inspection include:

- a) Hardware systems, software, digital devices, network devices, and other technical components of the information system;
- b) Regulations, processes, plans, and measures for ensuring cybersecurity;
- c) Information stored, processed, or transmitted in the information system;
- d) Plans for response to and remediation of cybersecurity incidents;
- dd) Measures to protect state secrets and prevent and combat the disclosure or loss of state secrets through technical channels;
- e) Personnel participating in the administration, operation, and cybersecurity protection of the information system.

4. Contents of a cybersecurity inspection include:

- a) Compliance with laws on ensuring cybersecurity and protecting state secrets in cyberspace;

- b) The implementation, maintenance, and effectiveness of regulations, processes, plans, and measures for ensuring cybersecurity;
- c) The implementation, maintenance, and effectiveness of plans for response to and remediation of cybersecurity incidents;
- d) The detection and assessment of weaknesses, security vulnerabilities, malicious software, and malicious hardware, and penetration testing of the system where necessary;
- dd) Other contents appropriate to the purpose of the inspection and the nature and cybersecurity protection requirements of the information system.

5. The administrator of an information system important to national security shall:

- a) Organize cybersecurity self-inspections of information systems within its management scope in the cases prescribed in Points a, b, and c Clause 2 of this Article;
- b) Send a written notice of the results of the annual cybersecurity inspection to the competent specialized cybersecurity protection forces before October 1 each year;
- c) Cooperate with the specialized cybersecurity protection forces during an ad hoc cybersecurity inspection;
- d) Comply with requests to remedy cybersecurity threats, cybersecurity incidents, weaknesses, and security vulnerabilities in accordance with the inspection conclusions of the competent authority.

6. Ad hoc cybersecurity inspections of information systems important to national security are prescribed as follows:

- a) Before conducting an inspection, the specialized cybersecurity protection forces shall notify the information system administrator in writing at least 12 hours in advance in the event of a cybersecurity incident or an act infringing upon cybersecurity, or at least 72 hours in advance where the inspection is required for the state management of cybersecurity or the period for remedying weaknesses or security vulnerabilities in accordance with the recommendations of the specialized cybersecurity protection forces has expired;
- b) Within 25 working days from the date of completion of the inspection, the specialized cybersecurity protection forces shall notify the inspection results and issue requirements to the information system administrator where weaknesses or security vulnerabilities are detected and shall provide guidance on or participate in remediation at the request of the information system administrator;
- c) The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall conduct ad hoc cybersecurity inspections of information systems important to national security, except for military information systems managed by the Ministry of National

Defense of Vietnam, cipher information systems under the Government Cipher Committee, and cryptographic products provided by the Government Cipher Committee to protect information classified as state secrets.

The specialized cybersecurity protection force under the Ministry of National Defense of Vietnam shall conduct ad hoc cybersecurity inspections of military information systems.

The Government Cipher Committee shall conduct ad hoc cybersecurity inspections of cipher information systems under the Government Cipher Committee and cryptographic products provided by the Government Cipher Committee to protect information classified as state secrets;

d) The administrator of an information system important to national security shall cooperate with the specialized cybersecurity protection forces in conducting an ad hoc cybersecurity inspection.

7. The procedures for a cybersecurity inspection conducted by the specialized cybersecurity protection forces are prescribed as follows:

a) Notify the information system administrator of the inspection plan or cybersecurity inspection decision, except for an ad hoc inspection intended to promptly prevent a threat to national security or social order and safety;

b) Establish an inspection team in accordance with the assigned functions, duties, and competence;

c) Conduct the cybersecurity inspection in accordance with the inspection plan or decision; ensure cooperation with the information system administrator and avoid interrupting the normal operation of the information system, except where necessary to protect national security;

d) Prepare a record of the process, contents, and results of the cybersecurity inspection;

dd) Notify the information system administrator in writing of the cybersecurity inspection results within 3 working days from the date of completion of the inspection;

e) Request the information system administrator to remedy any cybersecurity threats, cybersecurity incidents, weaknesses, security vulnerabilities, or violations of cybersecurity laws detected during the inspection.

8. Where an ad hoc inspection cannot be notified in advance, the specialized cybersecurity protection forces shall immediately conduct the inspection within their competence and notify the information system administrator in writing within 24 hours from the commencement of the inspection.

9. Where the current status of an information system must be preserved for the investigation, verification, or handling of a violation of the law, the handling of a cybersecurity incident, or the remediation of weaknesses or security vulnerabilities, the specialized cybersecurity protection forces shall issue a written request for the information system administrator to implement one or

more necessary measures, including temporarily preserving the system's configuration, technical status, data, and system logs or restricting, adjusting, or suspending part of the information system's operation. The written request shall clearly state the reasons, purposes, scope, applicable measures, and implementation period.

10. A cybersecurity inspection shall be conducted based on proper grounds, within the proper competence and scope, for the proper purposes, and in accordance with the specified inspection contents, and shall not unlawfully affect the normal operations of agencies, organizations, individuals, or the information system subject to inspection.

11. Inspection records and results and information, documents, and data collected during a cybersecurity inspection shall be managed, used, and protected in accordance with the law on protection of state secrets, the law on cybersecurity, and other relevant laws.

Article 9. Procedures for response to and remediation of cybersecurity incidents affecting information systems important to national security

1. Response to and remediation of cybersecurity incidents refer to activities involving the detection, identification, prevention, containment, handling, and remediation of cybersecurity incidents and the restoration of information system operations upon the occurrence of such incidents.

2. Activities for response to and remediation of cybersecurity incidents include:

- a) Detecting and identifying a cybersecurity incident;
- b) Preserving the incident scene and collecting and preserving information, data, documents, and evidence related to the cybersecurity incident;
- c) Containing and isolating the cybersecurity incident and limiting the scope of its impact;
- d) Analyzing, assessing, classifying, and determining the severity of the cybersecurity incident;
- dd) Implementing measures to respond to and remedy the cybersecurity incident and restore the normal operation of the information system;
- e) Verifying the cause and tracing the origin of the cybersecurity incident.

3. An information system administrator shall:

- a) Develop, issue, implement, and maintain a plan for response to and remediation of cybersecurity incidents affecting information systems within its management scope;
- b) Promptly detect, identify, and classify cybersecurity incidents and implement the plan for response to and remediation of cybersecurity incidents;

c) Immediately notify the competent specialized cybersecurity protection forces where a cybersecurity incident exceeds its handling capacity or a dangerous cybersecurity situation arises;

d) Cooperate with and provide the information, documents, data, and necessary technical conditions required for the specialized cybersecurity protection forces to coordinate the response to and remediation of cybersecurity incidents;

dd) Report the results of the handling and remediation of cybersecurity incidents to the competent specialized cybersecurity protection forces in accordance with regulations.

4. The requirements to notify and report cybersecurity incidents prescribed in Points c and dd Clause 3 of this Article do not apply to military information systems or cipher information systems under the Government Cipher Committee. The notification and reporting of cybersecurity incidents involving military information systems and cipher information systems under the Government Cipher Committee shall comply with regulations of the Ministry of National Defense of Vietnam and the law on cipher.

5. Upon receiving information concerning a cybersecurity incident, the competent specialized cybersecurity protection forces shall perform the following duties:

a) Guide the information system administrator in applying temporary measures to prevent and limit damage;

b) Assess the nature, severity, and scope of impact of the cybersecurity incident;

c) Decide on, or propose, a plan for coordinating the response to and remediation of the cybersecurity incident within their competence;

d) Direct and supervise activities for the response to and remediation of the cybersecurity incident where necessary;

dd) Compile, report, and assess the results of the handling of the cybersecurity incident in accordance with regulations.

6. In an emergency involving the protection of national security or social order and safety, the competent specialized cybersecurity protection forces may immediately apply necessary measures to coordinate the response to and remediation of the cybersecurity incident in accordance with the law and shall concurrently notify the information system administrator for cooperation in implementation.

7. The procedures for coordinating the response to and remediation of a cybersecurity incident are as follows:

a) The information system administrator shall detect, identify, and classify the cybersecurity incident and immediately implement initial response measures;

b) Where the incident exceeds its handling capacity or a dangerous cybersecurity situation arises, the information system administrator shall notify the competent specialized cybersecurity protection forces;

c) The specialized cybersecurity protection forces shall assess the incident and provide guidance on, or decide on, a plan for coordinating the response to and remediation of the cybersecurity incident within their competence;

d) The information system administrator shall implement measures to respond to and remedy the cybersecurity incident in accordance with the determined plan or the guidance of the specialized cybersecurity protection forces;

dd) Relevant agencies, organizations, enterprises, and individuals shall cooperate, provide information and technical assistance, and make available the resources necessary for activities coordinating the response to and remediation of the cybersecurity incident at the request of a competent authority;

e) After completing the response to and remediation of the incident, the information system administrator shall compile the handling results, assess the causes and consequences and the measures applied, and submit a report to the competent specialized cybersecurity protection forces.

8. The response to and remediation of cybersecurity incidents shall be carried out through the National Cybersecurity Incident Response and Remediation Network under the unified coordination of the Ministry of Public Security of Vietnam, ensuring cooperation among the specialized cybersecurity protection forces, ministries, central authorities, local authorities, agencies, organizations, enterprises, and relevant individuals in accordance with the law.

9. Telecommunications enterprises, enterprises providing Internet services, and information technology enterprises shall cooperate, provide technical information and data, and arrange the technical conditions necessary for the specialized cybersecurity protection forces to perform their duties of coordinating the response to and remediation of cybersecurity incidents in accordance with the law.

10. Information, documents, data, and evidence collected during the response to and remediation of cybersecurity incidents shall be managed, used, and protected in accordance with the law on protection of state secrets, the law on cybersecurity, and other relevant laws.

Article 10. Procedures for implementing measure of using cryptography to protect network information

1. The specialized cybersecurity protection forces shall use encryption measures employing cipher cryptography to protect network information when storing or transmitting information or documents containing state secrets in cyberspace. The use of cipher cryptography shall comply with the law on cipher, the law on protection of state secrets, and the law on cybersecurity.

2. For data and information within the management scope of the Ministry of Public Security of Vietnam, the specialized cybersecurity protection forces may use security cryptography to secure or authenticate data for the purposes of protecting national security and social order and safety and ensuring cybersecurity.

3. Where necessary for reasons of national security or social order and safety or to protect the lawful rights and interests of agencies, organizations, and individuals, the specialized cybersecurity protection forces shall send written requests to relevant agencies, organizations, and individuals to encrypt information not classified as state secrets before storing or transmitting such information on the Internet. The written request shall clearly state the reasons, scope, contents of the information to be encrypted, and applicable encryption measures.

Article 11. Procedures for implementing measure of requesting removal of illegal or false information and fake news in cyberspace that infringe upon national security, social order and safety, or lawful rights and interests of agencies, organizations, and individuals

1. Cases in which the measure may be applied:

a) Where information in cyberspace is determined by a competent authority to contain content infringing upon national security, constituting propaganda against the State of the Socialist Republic of Vietnam, inciting riots, disrupting security, or disturbing public order in accordance with the law;

b) Where there are legal grounds to determine that information in cyberspace contains insulting or slanderous content; infringes upon economic management order; or is fabricated or false, causes public panic, and causes serious damage to socio-economic activities to the extent that its removal must be requested;

c) Other information in cyberspace containing the contents prescribed in Clause 2 Article 7 of the Law on Cybersecurity, in accordance with the law.

2. The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall:

a) Decide to apply the measure of requesting the removal of illegal or false information and fake news in cyberspace that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals as prescribed in Clause 1 of this Article;

b) Send written requests to enterprises providing services on telecommunications networks, services on the Internet, or value-added services in cyberspace, and to information system administrators, to remove illegal or false information and fake news in cyberspace that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals as prescribed in Clause 1 of this Article;

c) Inspect compliance with the requested measure by relevant entities;

d) Exchange and share information on the implementation of this measure, except where the contents constitute state secrets or relate to operational requirements of the Ministry of Public Security of Vietnam.

3. Within its assigned functions, duties, and entitlements, the specialized cybersecurity protection force under the Ministry of National Defense of Vietnam shall decide to apply the measure of requesting the removal of illegal or false information and fake news in cyberspace that infringe upon national security or military security as prescribed in Clause 1 of this Article with respect to military information systems.

Article 12. Procedures for implementing measure of collecting electronic data related to activities infringing upon national security, social order and safety, or lawful rights and interests of agencies, organizations, and individuals in cyberspace

1. Electronic data refers to symbols, letters, numbers, images, sounds, or similar forms created, stored, transmitted, or received by electronic means.

2. Competence to decide on the implementation of the measure of collecting electronic data is prescribed as follows:

a) The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall decide to implement the measure of collecting electronic data to serve the investigation and handling of acts infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace;

b) The specialized cybersecurity protection force under the Ministry of National Defense of Vietnam shall decide to apply the measure of collecting electronic data to serve the investigation of violations and crimes that cause insecurity or unsafety or infringe upon national security or military security in cyberspace.

3. The collection of electronic data related to activities infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace shall be conducted in accordance with the law and shall satisfy the following principles and requirements:

a) Electronic data shall not be interfered with or altered;

b) Data collection shall be approved by a competent person prescribed in Clause 2 of this Article, conducted in accordance with the proper processes using recognized and verifiable equipment and software, and shall ensure the integrity of electronic data stored in electronic media;

c) A person collecting electronic data shall possess adequate professional capacity and be assigned by a competent person prescribed in Clause 2 of this Article to perform the task of collecting electronic data in accordance with the law;

d) The electronic data collection process shall be documented in records and images and, where necessary, shall be repeatable to produce similar results. Where necessary, an independent third party may be invited to witness and certify the process.

4. The seizure of media used to store, transmit, or process electronic data related to activities infringing upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals in cyberspace shall be conducted in accordance with the law.

Article 13. Procedures for implementing measure of terminating or suspending, or requesting cessation of operation of, information systems and revoking domain names

1. Cases in which the measure may be applied:

a) There are documents proving that the operation of an information system violates national security or cybersecurity laws;

b) An information system is being used to infringe upon national security or social order and safety.

2. The Minister of Public Security of Vietnam shall directly decide on the termination or suspension of, or request for cessation of operation of, an information system, or the suspension or revocation of a domain name involved in activities violating cybersecurity laws.

3. The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall implement decisions on the termination or suspension of, or requests for cessation of operation of, information systems or the suspension or revocation of domain names.

4. The procedures for implementing the measure are as follows:

a) Prepare a report on the application of the measure of terminating or suspending, or requesting the cessation of operation of, an information system or suspending or revoking a domain name;

b) Issue a decision on the termination or suspension of, or request for cessation of operation of, an information system or the suspension or revocation of a domain name;

c) Send a written request to relevant agencies, organizations, and individuals to terminate or suspend, or request the cessation of operation of, an information system, or send a written request to the Ministry of Science and Technology of Vietnam to suspend or revoke a domain name in accordance with the procedures prescribed by law. The written request shall clearly state the reasons, duration, contents, and recommendations;

d) In an urgent case where it is necessary to promptly prevent the operation of an information system from endangering national security or to prevent potentially harmful consequences, the Ministry of Public Security of Vietnam may directly request, or send a written request by fax or

email to, an agency, organization, or individual to terminate or suspend, or request the cessation of operation of, the information system.

Within 24 hours from the time the request is made, the Ministry of Public Security of Vietnam shall send a written request for the termination or suspension of, or request for cessation of operation of, the information system. If no written decision is issued within this period, the information system may resume its operation. Depending on the nature, severity, and consequences of the delay in sending the written request, the responsible official and relevant persons shall bear responsibility in accordance with the law;

dd) The termination or suspension of, or request for cessation of operation of, an information system shall be documented in a record. The record shall specify the time, location, and grounds and shall be made in 2 copies. The competent authority shall retain one copy, and the agency, organization, or individual owning or managing the information system shall retain the other copy;

e) For the suspension or revocation of a domain name in the cases prescribed in Clause 1 of this Article, the competent authority shall send a written request to the Ministry of Science and Technology of Vietnam to suspend or revoke the domain name in accordance with the procedures prescribed by law.

5. Where an information system is terminated or suspended, or the cessation of its operation is requested, without the grounds prescribed in Clause 2 of this Article, the head or deputy head of the competent authority and relevant officials shall bear responsibility before the law and, if damage is caused to a relevant agency, organization, or individual, shall pay compensation in accordance with the law.

Article 14. Responsibilities of agencies, organizations, and individuals for implementing cybersecurity protection measures

1. The specialized cybersecurity protection forces shall provide specific guidance to relevant agencies, organizations, and individuals on compliance with the procedures for applying certain cybersecurity protection measures.

2. Within the scope of their respective responsibilities and entitlements, agencies, organizations, and individuals shall promptly cooperate with and assist the specialized cybersecurity protection forces in complying with the procedures for applying certain cybersecurity protection measures.

3. Where an enterprise providing cross-border services is declared by a competent authority to have violated Vietnamese law, Vietnamese organizations and enterprises shall cooperate with competent authorities in preventing, combating, and handling the enterprise's violations of the law.

4. Any act of exploiting or abusing cybersecurity protection measures to violate the law shall, depending on the nature and severity of the violation, be handled in accordance with the law.

Where such an act causes damage to the lawful rights and interests of an organization or individual, compensation shall be paid in accordance with the law.

5. For information systems not included in the list of information systems important to national security, the Ministry of Public Security of Vietnam and the Ministry of National Defense of Vietnam shall cooperate in the protection of cybersecurity in a consistent manner in accordance with their assigned functions and duties:

a) The Ministry of Public Security of Vietnam shall act as the focal agency taking charge of civil and economic activities; activities involving the protection of national security, social order and safety, and cybersecurity; and the prevention and combat of cybercrime, cyberterrorism, and cyber espionage;

b) The Ministry of National Defense of Vietnam shall act as the focal agency taking charge of activities to safeguard the Fatherland in cyberspace.

Chapter III

ASSURANCE OF CYBER INFORMATION SECURITY

Article 15. Principles for assurance of cyber information security

1. Activities for the assurance of cyber information security in the provision of services on telecommunications networks, the Internet, and value-added services in cyberspace in Vietnam shall ensure national sovereignty in cyberspace; protect national security and social order and safety; and ensure the lawful rights and interests of agencies, organizations, and individuals in accordance with the law.

2. The application of measures for the assurance of cyber information security shall combine state management measures and technical measures in a consistent manner and be appropriate to the nature, scale, and scope of operation of the services provided by organizations and individuals and the level of risk to cyber information security.

3. The collection, storage, processing, use, and provision of information and data during the provision of services in cyberspace shall comply with the law on cybersecurity, the law on personal data protection, and other relevant laws of Vietnam.

Article 16. Activities for assurance of cyber information security

1. Domestic and foreign enterprises providing services on telecommunications networks, services on the Internet, and value-added services in cyberspace in Vietnam shall conduct activities for the assurance of cyber information security in accordance with this Article and other relevant laws of Vietnam.

2. Activities involving the verification and protection of service users' information and accounts include:

- a) Verifying users' information when they register digital accounts in accordance with the law;
- b) Verifying accounts using Vietnamese mobile telephone numbers. Where a user does not have a Vietnamese mobile telephone number, the account shall be verified using the user's personal identification number or another lawful electronic identification method in accordance with the law on electronic identification and authentication;
- c) Where a service user uses a livestreaming feature for commercial purposes, the account shall be verified using the user's personal identification number in accordance with the law;
- d) Applying necessary state management and technical measures to ensure the security and confidentiality of users' information and accounts and permitting only verified accounts to post and share information and use interactive features on the system.

3. Activities involving the provision of information for the assurance of cyber information security include:

- a) Providing service users' information to the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam upon receipt of a valid request made pursuant to Vietnamese law for the verification, investigation, and handling of violations of the law;
- b) Requests for and provision of information shall be made in writing, by electronic means, or in another form that ensures authentication of the requesting entity and confidentiality of the information provided in accordance with the law;
- c) Information shall be provided no later than 24 hours from the time the request is received. In an emergency threatening national security or human life, information shall be provided no later than 3 hours.

4. Activities involving the prevention and handling of information, services, and applications in violation of cyber information security laws include:

- a) Restricting or blocking access to, or removing, information, services, and applications in Vietnam that violate cyber information security laws at the request of the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam;
- b) A request prescribed in Point a of this Clause shall be complied with no later than 24 hours from the time it is received. In an emergency threatening national security, the request shall be complied with no later than 6 hours from the time it is received;
- c) Applying state management and technical measures to restrict, suspend, or cease the provision of services to organizations and individuals that repeatedly post information in violation of cyber information security laws, at the request of a competent authority and in accordance with the law;

d) Restricting visibility in Vietnam or temporarily locking a personal account, page, community group, or content channel used to post information in violation of cyber information security laws in the following cases:

Within a period of 30 days, where information in violation of cyber information security laws is posted at least 3 times, visibility in Vietnam shall be restricted, or the account, page, group, or channel shall be temporarily locked for a maximum period of 60 days, depending on the nature and severity of the violation;

Within a period of 90 days, where information in violation of cyber information security laws is posted at least 10 times, visibility in Vietnam shall be restricted, or the account, page, group, or channel shall be temporarily locked for a maximum period of 180 days, depending on the nature and severity of the violation;

dd) Indefinitely restricting visibility in Vietnam or indefinitely locking a personal account, page, community group, or content channel used to commit, continue committing, disseminate, organize, direct, or assist in the commission of acts in violation of cybersecurity laws in the following cases:

Posting or disseminating information that infringes upon the national security of the Socialist Republic of Vietnam;

The account, page, group, or channel has been temporarily locked at least 3 times at the request of a competent authority but continues to be used to commit acts in violation of cybersecurity laws;

There are grounds to determine that the personal account, page, community group, or content channel continues to be used as a tool or means for committing acts in violation of cybersecurity laws and that indefinite account locking is necessary and appropriate to the nature and severity of the violation;

e) An account subject to indefinite locking may be considered for restoration in any of the following cases: the grounds for applying the measure no longer exist; an error occurred during verification or handling; new circumstances arise that alter the grounds for applying the measure; or a competent authority determines that the account was not used to commit acts in violation of cybersecurity laws.

5. Activities involving the suspension or cessation of service provision to ensure cyber information security include refraining from providing, suspending, or ceasing the provision of services to organizations and individuals that post information falling within the cases prescribed in Clauses 1, 2, and 3 Article 13 and Clause 2 Article 14 of the Law on Cybersecurity at the request of the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam. The suspension or cessation of service provision shall be applied to the proper scope and entities, for the proper duration, and in accordance with relevant laws.

6. Activities involving the storage and management of system logs include:

- a) Storing and managing system logs for state management, assurance of cyber information security, and handling of violations of the law;
- b) System logs shall contain at least information on service users' accounts, login and logout times, IP addresses, source ports used for login and logout, and logs of the processing of posted information;
- c) System logs shall be stored in a manner that enables data retrieval for at least 12 months and satisfies requirements for the verification, investigation, and handling of violations of the law.

Article 17. Measures for assurance of cyber information security

- 1. Measures for assurance of cyber information security include state management, technical, and professional measures prescribed by law.
- 2. Based on the nature, severity, and scope of impact of a threat or violation, a competent state authority may require enterprises, organizations, and individuals providing or using services in cyberspace to apply one or more measures for the assurance of cyber information security.
- 3. The application of a measure for the assurance of cyber information security shall comply with the principles prescribed in Article 15 of this Decree and shall not unlawfully infringe upon the lawful rights and interests of agencies, organizations, or individuals.

Article 18. Responsibilities for assurance of cyber information security

- 1. Enterprises, organizations, and individuals providing or using services in cyberspace shall cooperate with the specialized cybersecurity protection forces and competent state authorities in implementing activities and measures for the assurance of cyber information security.
- 2. Telecommunications enterprises, enterprises providing Internet services, web hosting services, or data center services, and enterprises providing telecommunications application services shall:
 - a) Block and remove illegal online content, services, and applications no later than 24 hours from the time a request is made in writing, by telephone, or by email by the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam;
 - b) Refuse to provide, or suspend the provision of, telecommunications services, Internet services, or other services to organizations and individuals that use such services to post illegal information online upon receipt of a valid request from the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam;
 - c) Telecommunications enterprises and enterprises providing Internet services shall connect to the technical system, receive coordination requests to block and remove harmful or illegal information, report the results through the technical system, and implement other handling measures as requested by the Ministry of Public Security of Vietnam;

d) Telecommunications enterprises and enterprises providing Internet services shall ensure the technical infrastructure, connection systems, processing capacity, transmission and sharing of information and data, and other necessary conditions during service provision to satisfy requirements for the assurance of cyber information security and facilitate the implementation of cybersecurity protection solutions and measures in accordance with the law and valid requests of the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam.

3. Upon detecting an act in violation of cyber information security laws, an agency, organization, or individual shall notify and cooperate with the competent authority in accordance with the law.

Article 19. Data storage and establishment of branches or representative offices assuming legal responsibility in Vietnam

1. Data required to be stored in Vietnam includes:

a) Personal information of service users in Vietnam;

b) Data generated by service users in Vietnam, including service account names, service usage time, credit card information, email addresses, the most recent login and logout IP addresses, and telephone numbers registered and associated with accounts or data.

2. Domestic enterprises shall store the data prescribed in Clause 1 of this Article in Vietnam.

3. Data storage and establishment of branches or representative offices assuming legal responsibility in Vietnam by foreign enterprises are prescribed as follows:

a) A foreign enterprise conducting business activities in Vietnam in any of the following fields: telecommunications services; storage or sharing of data in cyberspace; provision of domain name registration and maintenance services to service users in Vietnam; e-commerce; online payment; payment intermediary services; transportation connection services in cyberspace; social networks and social media; online video games; online applications; or services for providing, managing, or operating other information in cyberspace in the form of messages, voice calls, video calls, emails, or online chats shall store the data prescribed in Clause 1 of this Article and establish a branch or representative office assuming legal responsibility in Vietnam where: The services provided by the enterprise have been used to commit acts in violation of cybersecurity laws; the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam has issued written notices and requests for cooperation in preventing, investigating, and handling such acts on 3 occasions over a period not exceeding 6 months; and the foreign enterprise fails to provide remedial solutions, fails to comply, fails to comply fully with the scope or quantity of each matter specified in the written requests, or prevents, obstructs, neutralizes, or renders ineffective the cybersecurity protection measures implemented by the specialized cybersecurity protection force;

b) Where a foreign enterprise is unable to comply with a requirement of cybersecurity laws due to a force majeure event, it shall notify the specialized cybersecurity protection force under the

Ministry of Public Security of Vietnam within 3 working days for verification of the force majeure event. In this case, the enterprise shall have 25 working days to find a remedial solution.

4. Where the data collected, utilized, analyzed, or processed by an enterprise does not include all types of data prescribed in Clause 1 of this Article, the enterprise shall cooperate with the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam in confirming and storing the types of data that it is currently collecting, utilizing, analyzing, or processing.

Where an enterprise additionally collects, utilizes, analyzes, or processes any data type prescribed in Clause 1 of this Article, it shall cooperate with the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam in supplementing and updating the list of data required to be stored in Vietnam and publicly notifying users thereof.

5. Enterprises may decide on the method of storing data in Vietnam, provided that the data can be retrieved and promptly provided at the request of a competent authority and that information security is ensured in accordance with national standards and technical regulations.

6. The procedures for requiring foreign enterprises to store data and establish branches or representative offices in Vietnam are as follows:

a) The Minister of Public Security of Vietnam shall issue a decision requiring data storage and the establishment of a branch or representative office in Vietnam;

b) The specialized cybersecurity protection force under the Ministry of Public Security of Vietnam shall notify, guide, monitor, supervise, and urge the enterprise to comply with the requirements for data storage and establishment of a branch or representative office in Vietnam and shall concurrently notify relevant authorities so that they may perform their state management functions within their competence;

c) Within 12 months from the date on which the Minister of Public Security of Vietnam issues the decision, the enterprises prescribed in Point a Clause 3 of this Article shall complete the data storage and establishment of a branch or representative office in Vietnam.

7. The procedures for establishing a branch or representative office in Vietnam shall comply with business, commerce, and enterprise laws and other relevant laws.

8. An enterprise that fails to comply with this Article shall, depending on the nature and severity of its violation, be handled in accordance with the law.

Article 20. Duration of data storage and establishment of branches or representative offices in Vietnam

1. The data storage period prescribed in Article 19 of this Decree shall commence when an enterprise receives a data storage request and end when the request expires. The minimum storage period shall be 24 months.

2. The period for maintaining a branch or representative office in Vietnam as prescribed in Article 19 of this Decree shall commence when an enterprise receives a request to establish a branch or representative office in Vietnam and end when the enterprise ceases its operations in Vietnam or the prescribed service is no longer provided in Vietnam.

3. System logs serving the investigation and handling of acts in violation of cybersecurity laws as prescribed in Point b Clause 2 Article 25 of the Law on Cybersecurity shall be retained for at least 12 months.

Chapter IV

IP ADDRESS IDENTIFICATION MANAGEMENT

Article 21. Principles of IP address identification

1. IP address identification management shall ensure the accuracy, integrity, and unique traceability of the organization or individual registered to use the service, the registered installation address of the Internet connection line for a fixed broadband network, and the registered telephone number for a mobile telecommunications network.

2. Enterprises providing telecommunications services and enterprises providing Internet services shall establish and maintain technical systems to record, store, and manage information serving IP address identification, linked to subscriber information, service usage times, and relevant service information in accordance with the law.

3. IP address identification shall be conducted throughout the allocation, use, and revocation of IP addresses, ensuring continuity and consistency and the capacity to satisfy state management requirements and facilitate cybersecurity protection measures.

Article 22. Contents and technical requirements for IP address identification

1. When allocating an IP address to an organization or individual, an enterprise providing telecommunications or Internet services shall apply technical measures to accurately identify the subscriber information at the time of IP address allocation.

2. System log data on the allocation and management of IP addresses shall be synchronized with the national time standard and shall contain at least the following information:

a) Source IP address, source port, destination IP address, destination port, and connection protocol;

b) Where Network Address Translation is used, complete IP address mapping information shall be stored;

c) The start and end times of the connection session, synchronized with the national time standard;

d) The identifier of the gateway allocating the public IP address (Gateway ID) and the connection session identifier (Session ID);

dd) Information on the subscriber and account using the IP address at the corresponding time.

3. The system log data prescribed in Clause 2 of this Article shall be stored fully and continuously for at least 12 months. The data storage system shall ensure integrity, security, and confidentiality; prevent alteration or deletion; and enable the extraction and provision of data in real time to the specialized cybersecurity protection forces for the implementation of cybersecurity protection measures.

Article 23. Provision of IP address identification information to specialized cybersecurity protection forces

1. Enterprises providing telecommunications or Internet services shall establish and maintain appropriate technical mechanisms capable of connecting with the technical systems of the specialized cybersecurity protection force under the Ministry of Public Security of Vietnam and providing information serving IP address identification in accordance with the law.

2. Specific requests for the provision of IP address identification information shall be handled according to the following procedures:

a) The provision shall be based on a lawful written request or valid electronic request from the specialized cybersecurity protection forces for the implementation of cybersecurity protection measures or the verification, investigation, or handling of acts in violation of cybersecurity laws;

b) Enterprises providing telecommunications or Internet services shall provide complete and accurate IP address identification information, including the individual's full name, organizational information, personal identification number, subscriber name or code, registered installation address of the Internet connection line for a fixed broadband network, and registered telephone number for a mobile telecommunications network, at the corresponding time, as requested by the specialized cybersecurity protection forces;

c) Information shall be provided no later than 24 hours from the time the request is received. In an emergency related to national security, the prevention and combat of cyberterrorism, a cyberattack, or a particularly serious crime, information shall be provided within 3 hours.

3. The use, disclosure, or utilization of IP address identification information for commercial purposes is strictly prohibited, except as otherwise prescribed by law.

Chapter V

TRAINING IN IN-DEPTH CYBERSECURITY KNOWLEDGE AND SKILLS

Article 24. Requirements for in-depth cybersecurity knowledge and skills

1. The entities prescribed in Clause 1 Article 34 of the Law on Cybersecurity shall be determined to satisfy the requirements for in-depth cybersecurity knowledge and skills if they meet any of the following criteria:

- a) Having received undergraduate or higher education in cybersecurity as a specialized discipline;
- b) Having received undergraduate or higher education in information technology or a closely related discipline and possessing a professional cybersecurity certificate prescribed in Clause 5 of this Article;
- c) Having received undergraduate or higher education in information technology or a closely related discipline and having at least 5 years of experience in cybersecurity protection and the prevention and combat of crimes using high technology;
- d) Having received undergraduate or higher education in information technology or a closely related discipline and having received the in-depth cybersecurity knowledge and skills training prescribed in Clause 2 of this Article.

2. Based on their job positions and assigned functions and duties, the individuals prescribed in Clause 2 Article 34 of the Law on Cybersecurity shall receive training in the foundational cybersecurity knowledge and skills prescribed in Clause 3 of this Article and at least one area of in-depth cybersecurity knowledge and skills prescribed in Clause 4 of this Article, except for individuals already trained in cybersecurity as a specialized discipline.

3. Foundational cybersecurity knowledge and skills include:

- a) Knowledge of cybersecurity laws, policies, and strategies, including the Law on Cybersecurity and its implementing documents; regulations on personal data protection and protection of state secrets in cyberspace; the rights, obligations, and responsibilities of agencies, organizations, and individuals in cybersecurity protection; and international treaties on cybersecurity to which Vietnam is a contracting party;
- b) General cybersecurity knowledge, including cybersecurity concepts, scope, and protected entities; common cybersecurity threats; principles for ensuring cybersecurity; secure system architecture; international standards and benchmarks; and cybersecurity technology development trends.

4. In-depth cybersecurity knowledge and skills include:

- a) Cybersecurity governance, policies, and law;
- b) Cybersecurity incident response and handling and digital forensics;
- c) Inspection and assessment of cybersecurity weaknesses and vulnerabilities and software security;

- d) Cybersecurity supervision, analysis, and early warning of cybersecurity risks and threats;
- dd) Research and development of cybersecurity products and systems;
- e) Cybersecurity design and architecture;
- g) Deployment and operation of information systems and assurance of their cybersecurity;
- h) Security of cloud computing, OT/IoT systems, and emerging technologies;
- i) Data security, privacy, and information management.

5. An individual who possesses a valid cybersecurity certificate issued by a foreign organization and recognized by the Ministry of Public Security of Vietnam as equivalent to the in-depth knowledge and skills prescribed in Clause 4 of this Article shall only be required to participate in training in the foundational knowledge and skills prescribed in Clause 3 of this Article.

6. The Minister of Public Security of Vietnam shall promulgate the training program framework and the standards for the knowledge and skills prescribed in Clauses 3 and 4 of this Article as a consistent basis for organizing training, assessing results, and issuing certificates nationwide, except for entities within the management scope of the Ministry of National Defense of Vietnam and the Government Cipher Committee.

7. The Minister of National Defense of Vietnam shall promulgate the training program framework and standards for in-depth cybersecurity knowledge and skills as a consistent basis for organizing training, assessing results, and issuing certificates to cybersecurity protection forces within its management scope.

8. The requirements for in-depth cybersecurity knowledge and skills prescribed in Clause 1 of this Article shall be implemented according to the following roadmap:

- a) Agencies, organizations, and state-owned enterprises shall review the persons currently holding the positions prescribed in Clause 1 Article 34 of the Law on Cybersecurity, allocate funding, and organize training within 24 months from the effective date of this Decree;
- b) Administrators of level-3, level-4, and level-5 information systems within agencies, organizations, and state-owned enterprises shall review the persons within their management scope who currently hold the positions prescribed in Clause 2 Article 34 of the Law on Cybersecurity, allocate funding, and organize training within 36 months from the effective date of this Decree.

Article 25. Training in in-depth cybersecurity knowledge and skills

1. A training provider may organize training in in-depth cybersecurity knowledge and skills for the entities prescribed in Article 34 of the Law on Cybersecurity when it fully satisfies the following conditions:

- a) It is lawfully established and operating in accordance with Vietnamese law;
- b) It has physical facilities, technical infrastructure, classrooms, practice rooms, simulation and exercise systems, and teaching materials appropriate to the training contents;
- c) It has a contingent of instructors satisfying the standards for in-depth knowledge and skills corresponding to those prescribed in Article 24 and the requirements prescribed in Article 27 of this Decree;
- d) It has curricula, materials, and teaching contents consistent with the training program framework and standards for in-depth cybersecurity knowledge and skills.

2. A provider of training in in-depth cybersecurity knowledge and skills shall:

- a) Organize training in accordance with the prescribed program framework and standards for knowledge and skills, assess results, and issue certificates in accordance with regulations;
- b) Retain dossiers and documents related to each training course for at least 5 years and submit a report on the training results to the Ministry of Public Security of Vietnam within 25 working days from the completion date of the course;
- c) Fully update information concerning the provider, trainees, and instructors on the management system in accordance with regulations;
- d) Submit periodic or ad hoc reports at the request of the state management authority for cybersecurity.

3. A training provider wishing to receive guidance and assistance from the Ministry of Public Security of Vietnam regarding training programs, contents, and methods may apply to join the Network of Providers of Training in In-depth Cybersecurity Knowledge and Skills managed by the Ministry of Public Security of Vietnam.

4. Training providers under the management of the Ministry of National Defense of Vietnam shall submit reports in accordance with regulations of the Ministry of National Defense of Vietnam.

Article 26. Network of Providers of Training in In-depth Cybersecurity Knowledge and Skills

1. The Ministry of Public Security of Vietnam shall establish and manage the Network of Providers of Training in In-depth Cybersecurity Knowledge and Skills for the following purposes:

- a) Assisting and guiding providers in developing training programs, curricula, and materials;
- b) Sharing experience, materials, and tools serving training activities;

- c) Organizing advanced training and capacity-building activities for instructors;
- d) Supervising and assessing the quality of training activities;
- dd) Strengthening connections and cooperation among training providers.

2. A provider wishing to join the Network shall submit an application to the Ministry of Public Security of Vietnam. The application dossier includes:

- a) An application to join the Network, made according to Form No. 03 in the Appendix promulgated together with this Decree;
- b) Documents proving its lawful establishment and operation;
- c) Information on physical facilities, its contingent of instructors, curricula, materials, and teaching contents demonstrating its capacity to organize training.

3. The Ministry of Public Security of Vietnam shall examine the dossier and approve the provider's admission to the Network within 15 working days from the date of receipt of a complete and valid dossier. Approval to join the Network is not a mandatory condition for a provider to organize training.

4. A provider participating in the Network shall have the following rights:

- a) To access training support materials, tools, and platforms provided by the Ministry of Public Security of Vietnam;
- b) To participate in advanced training and capacity-building activities organized by the Ministry of Public Security of Vietnam;
- c) To receive professional and technical assistance and guidance;
- d) To exercise other rights in accordance with the law.

5. A provider participating in the Network shall:

- a) Organize training in accordance with the program framework and standards for knowledge and skills promulgated by the Ministry of Public Security of Vietnam;
- b) Periodically report the results of its training activities;
- c) Participate in the Network's general activities;
- d) Comply with inspections and supervision by the Ministry of Public Security of Vietnam.

6. A provider shall be suspended from or have its participation in the Network terminated in any of the following cases:

- a) It seriously violates regulations on the organization of training;
- b) It issues certificates contrary to regulations;
- c) It fails to fully perform the responsibilities of a Network member;
- d) It submits a written request to withdraw from the Network.

Article 27. Requirements for instructors providing training in in-depth cybersecurity knowledge and skills

1. An instructor providing training in in-depth cybersecurity knowledge and skills shall possess an undergraduate or higher degree in cybersecurity, information technology, electronics and telecommunications, or another relevant discipline appropriate to the teaching contents.

2. An instructor providing training in in-depth cybersecurity knowledge and skills shall satisfy either of the following conditions:

- a) Having at least 3 years of practical experience in the field of cybersecurity;
- b) Possessing a professional cybersecurity certificate appropriate to the field taught.

3. An instructor providing training in in-depth cybersecurity knowledge and skills shall possess pedagogical capacity and the ability to communicate knowledge and provide practical instruction in a manner satisfying the requirements of the training activities.

Article 28. Conditions for issuance of certificates of training in in-depth cybersecurity knowledge and skills

1. An individual shall be issued a certificate of training in in-depth cybersecurity knowledge and skills when fully satisfying the following conditions:

- a) Attending at least 80% of the training course duration;
- b) Fully completing all assignments and practical exercises during the training course;
- c) Satisfying the requirements of the end-of-course test and assessment in accordance with regulations.

2. A certificate of training in in-depth cybersecurity knowledge and skills shall:

- a) Be signed and sealed by the head of the training provider;

b) Specify the full name of the certificate holder, the modules of knowledge and skills completed, the training duration, and the date of issuance.

3. A training provider shall send information on the certificates issued to the Ministry of Public Security of Vietnam for updating and management in accordance with regulations. For training providers within the management scope of the Ministry of National Defense of Vietnam or the Government Cipher Committee, the submission of information and management of certificates shall comply with regulations of the Ministry of National Defense of Vietnam and the Government Cipher Committee, respectively.

4. Agencies, organizations, and state-owned enterprises shall periodically review training needs and organize or appoint their officials to participate in refresher and knowledge-updating courses to ensure that they continue to satisfy the requirements of their job positions prescribed in Clauses 1 and 2 Article 34 of the Law on Cybersecurity.

Article 29. Responsibilities of Ministry of Public Security of Vietnam for management of cybersecurity training activities

1. Promulgate the program framework and standards for in-depth cybersecurity knowledge and skills for consistent nationwide application.

2. Develop, maintain, update, and manage a database on cybersecurity training providers, trainees, and instructors.

3. Provide detailed guidance on training programs and contents; standards and procedures for assessing learning outcomes; forms of training certificates; procedures for applying to join the Network; and standards for physical facilities and equipment serving training activities.

4. Organize support, advanced training, and capacity-building activities for training providers and instructors.

5. Conduct inspections and supervision, and handle violations arising from activities of training in in-depth cybersecurity knowledge and skills in accordance with the law.

Chapter VI

IMPLEMENTATION PROVISIONS

Article 30. Entry into force

This Decree comes into force as of August 19, 2026.

Article 31. Transitional provisions

Dossiers of request for cybersecurity appraisal and dossiers of request for assessment of cybersecurity conditions that were validly received by competent authorities in accordance with

Decree No. 53/2022/ND-CP before the effective date of this Decree but have not yet been resolved shall continue to be processed in accordance with Decree No. 53/2022/ND-CP.

Article 32. Implementation responsibilities

Ministers, Directors of ministerial agencies, Presidents of People's Committees of provinces and centrally affiliated cities, and relevant agencies, organizations, and individuals shall implement this Decree.

**ON BEHALF OF THE GOVERNMENT
PP. PRIME MINISTER
DEPUTY PRIME MINISTER**

Pham Gia Tuc

*This translation is made by **THƯ VIỆN PHÁP LUẬT**, Ho Chi Minh City, Vietnam and for reference purposes only. Its copyright is owned by **THƯ VIỆN PHÁP LUẬT** and protected under Clause 2, Article 14 of the Law on Intellectual Property. Your comments are always welcomed*