



CYBER SECURITY AND COUNTER HIGH-TECH CRIMES DEPARTMENT
MINISTRY OF PUBLIC SECURITY

CYBERSECURITY LAW HANDBOOK

ENABLING
DEVELOPMENT
IN THE DIGITAL
ERA

SAFEGUARDING
CYBER
SOVEREIGNTY



UNDERSTANDING
THE LAW



RAISING
AWARENESS



PREVENTING
PROACTIVELY



PENALIZING
VIOLATIONS



CONTENTS



I

GENERAL INTRODUCTION TO THE CYBERSECURITY LAW

1



II

NEW CONTENT IN THE CYBERSECURITY LAW

2



III

CONDITIONS FOR ENFORCEMENT

3



IV

IMPLEMENTATION ACTIVITIES

4



GENERAL INTRODUCTION TO THE CYBERSECURITY LAW





I THE NECESSITY OF PROMUGALTION

The **2025 Cybersecurity Law** was passed by the **15th National Assembly** on December 10, 2025, and **takes effect on July 1, 2026**. The Law was promulgated to meet the requirements of protecting sovereignty, national security, data security, and information security in the context of digital transformation and the Fourth Industrial Revolution.

The Law aims to unify state management focal points, **resolve overlaps** among agencies and between the 2018 Cybersecurity Law and the 2015 Law on Information Security. Simultaneously, the Law addresses new challenges such as cyberattacks, cyberespionage, personal data leakage, toxic and malicious information, and cross-border high-tech crime.

Based on inheriting and consolidating still-appropriate regulations, **the 2025 Cybersecurity Law** establishes a synchronized legal framework for protecting important information systems, technical standards, protective forces, coordination mechanisms, and responsibilities of subjects; thereby both ensuring cybersecurity and creating a stable environment for the digital economy and national digital transformation.



TARGET

I



Unify and finalize the legal framework on cyber security

Eliminate overlaps in state administration

Strengthen the prevention, detection and handling of cybersecurity incidents

Protect data information systems and citizen's rights

Harmonize cybersecurity assurance with digital economy development and digital transformation



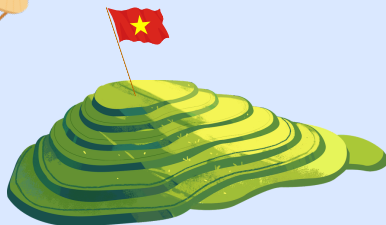


POINT OF VIEW

I



Ensure the leadership of the Party, the unified management of the State, and promote the role of the entire population and specialized forces.



Proactively, independently prevent and respond to cyber risks, while promoting "Make in Vietnam" cybersecurity technologies and products.



Ensure cybersecurity with socio-economic development, digital transformation, and the protection of human rights and citizens' rights.



Focus on the people and their data, enhance data protection, develop high-quality human resources, and raise social awareness.



LAYOUT

I

The Cybersecurity Law 2025 consists of 8 chapters and 45 articles.



Chapter I: General provisions, principles, cybersecurity protection measures, international cooperation, and prohibited acts.

Chapter II: Classification of information into 5 levels and protection of critical information systems for national security.



Chapter III: Prevention, detection, and handling of cybersecurity violation acts; Protection of secrets and children; Prevention and Control of cyberattacks.

Chapter IV: Cybersecurity protection in agencies and organizations; protection of network infrastructure, information, and data.





LAYOUT

I

8 CHAPTERS



45 ARTICLES



Chapter V: Technical standards, regulations, and business conditions for cybersecurity products and services.

Chapter VI: Organization of forces, human resource development, training, technological research, and funding assurance.



Chapter VII: Responsibilities of State Administration, System owners, Service providers, and Network users.

Chapter VIII: Amendments to relevant laws, taking effect from July 1st, 2026, and transitional provisions.





NEW CONTENT IN THE CYBERSECURITY LAW

II



II

NEW CONTENT



Complete and unify the system of concepts to serve as the foundation for cybersecurity management and protection.

Cybersecurity: Encompasses the stability and safety of cyberspace, information systems, data, and online activities.

Information security on networks: Focuses on ensuring the confidentiality, integrity, and availability of information.

Data security: Regulation in data security is independently defined for the first time, recognizing data as a strategic resource that needs to be protected and utilized effectively.

National cyberspace: Affirming Vietnam's sovereignty, jurisdiction, and control over cyberspace.



II

NEW CONTENTS



PROHIBITED ACTS



Preventing the abuse of AI and Deepfake to forge images, videos, or voices for the purposes of fraud, slander, blackmail, or infringement upon honor.



Preventing and combating against economic security infringements, and handling misleading information in finance, banking, securities, e-commerce, and multi-level marketing activities.



Controlling platforms and services supporting unauthorized models, including digital asset trading and illegal business ecosystems.



Protecting personal data and digital identity, strictly prohibiting the unauthorized collection, trading, exchange, or utilization of other people's information.



Preventing fake accounts and profiles, and handling the unauthorized opening, trading, or use of bank accounts, e-wallets, stocks, and other digital accounts.



II

NEW CONTENT



PROHIBITED ACTS ABUSING AI, Deepfake

Identifying illegal information, fake news, and handling mechanisms in cyberspace.



Article 7 – Cybersecurity Law 2025 – Prohibiting from posting and sharing of fake and misleading information, deepfake: A breakthrough in cyberspace protection.



Clause 4, Article 7 – The Law of Network Information Safety 2015 – Prohibiting the establishment of fraudulent and deceptive information systems.



Clauses 4 and 6, Article 6 – Law on Electronic Transactions 2023 – Handling acts of forgery, falsification, and unauthorized deletion or destruction of data; and the misappropriation of accounts and electronic certificates.



Point b, Clause 1, Article 40 – Law on Telecommunications 2023 – Responsibilities of telecommunication enterprises in ensuring safety, protection of users, and coordinating in handling violations.





II

NEW CONTENT

PROHIBITED ACTS ABUSING AI, Deepfake

Comprehensive legal framework



Network Information Safety Law 2025

Ensuring system safety, data protection as well as control over unauthorized access.



Electronic Transactions Law 2023

Establishing the legal validity of data messages and authentication mechanism in the digital environment.

Telecommunication Law 2023

Setting requirements for service safety, user protection, and coordination in handling violations.



Cybersecurity Law 2025

Penal Code 2015 (Amended in 2017)

Criminal prosecution for acts of slander, humiliation, and data infringement.

Civil Code 2015

Protecting personal rights, image, honor, reputation, and personal privacy.





II

NEW CONTENT



PROHIBITED ACTS ABUSING AI, Deepfake

Specific Solutions

Completing the legal framework.

- Cybersecurity
- Personal data protection
- Responsibilities of digital platforms
- Cooperating mechanism for handling information infringement

Application of technology

- Data monitoring and analysis
- Identifying fake content
- Tracing the origin of information
- Assessing the virality of infringing content

Enhancing digital skills for individuals and organizations.

- Fact-checking information before sharing
- Identifying fake news
- Proactively protecting personal data, images, and identity information
- Preventing risks of being exploited to create fake content

Propagating and raising public awareness.

- Boosting community "resilience" against fake and misleading news
- Rebutting false and hostile allegations
- Researching and applying fact-checking models to minimize damages



II

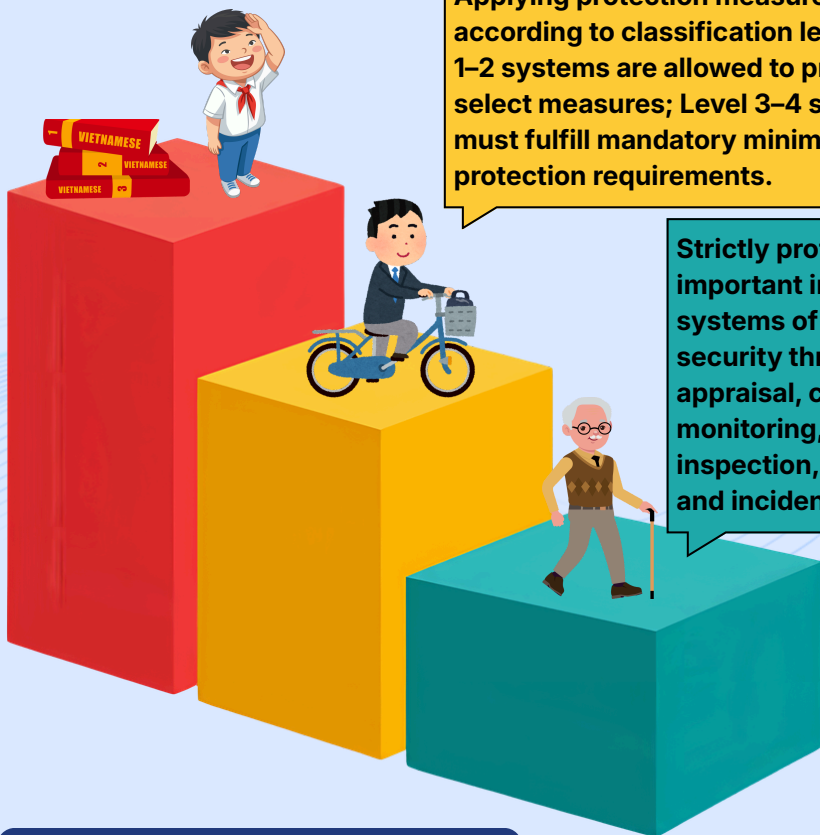
Protecting cybersecurity by levels for information system



Classifying information systems into 5 levels, from low impact to particularly severe harm to national security.

Applying protection measures in according to classification levels: Level 1–2 systems are allowed to proactively select measures; Level 3–4 systems must fulfill mandatory minimum protection requirements.

Strictly protecting important information systems of national security through appraisal, certification, monitoring, periodic inspection, reporting, and incident response.





II

Protecting cybersecurity by levels of information systems



Data control and protection are not commensurate with data's value and exploitation level in the digital economy, leading to data exposure, loss, and personal data infringement.

Cyberspace is facing numerous threats, such as cyberattacks, cyber espionage, and the exposure or loss of government secrets.

The use of high technology to commit crimes, causing substantial property damage to citizens.

Agencies and organizations are responsible for advising, organizing execution, and enforcing cybersecurity protection, as well as ensuring the implementation of cybersecurity protection measures.



II

Enterprises are responsible for providing services on telecommunication networks, the Internet, and value-added services in cyberspace in Vietnam.



1



Rapid response to infringing content: Removing and blocking infringing information or services within 24 hours; in emergency cases related to national security, no later than 6 hours.

2



Proactive prevention: Enterprises must deploy technical measures to detect, warn, block, and handle content that infringe upon national security and social order.

3



Service suspension: Blocking or discontinuing services to organizations or individuals in serious violation may be executed upon request from specialized agencies.

4



Incident response and reporting: Developing response plans, alerting users, and coordinating in handling when cybersecurity incidents occur.

5



Tracing and investigation: Identifying IP addresses, providing information, and establishing technical connections as requested by competent authorities.



II

Affirming that data security assurance is a vital component of cybersecurity protection.



1 Establishing data security as an independent legal concept, including assurance of data quality, integrity, and usability.

Managing the entire data lifecycle using technical, organizational, and legal measures such as access control, encryption, personnel managing, and risk assessment.

2

3 Strengthening cross-border data control and protecting critical databases, data centers, and storage systems.

Strictly prohibiting the unauthorized collection, use, trading, and dissemination of personal data.

4

5 Establishing a legal basis for handling data violations, preventing and combating fraud, impersonation, property appropriation, and other high-tech crimes.



II

Strengthening cyber protection regulations for children while expanding them to cover the elderly and individuals with cognitive or behavioral difficulties.

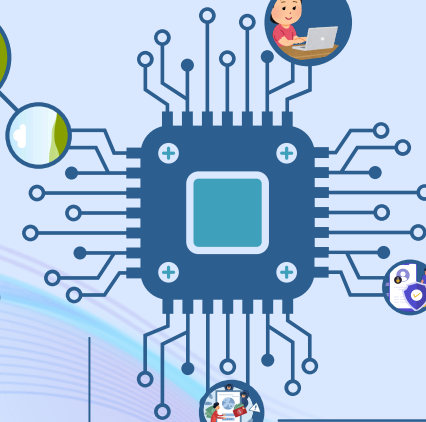


Parents and guardians must actively monitor and manage their children's online accounts and network use.



Building a multi-layered protection network: Families, enterprises, and government agencies must share these responsibilities, not evade them.

Enterprises must proactively deploy technical solutions to detect, block, and remove child abuse content, and provide clear reporting tools.



Vulnerable groups, such as the elderly and cognitive difficulties, receive early warnings, support, and priority when handling fraud and abuse cases.



II

Encouraging cybersecurity R&D and prioritizing investment in domestic infrastructure, products, and services.



1 Developing the domestic cybersecurity industry through special investment incentive mechanisms for cybersecurity protection products, services, and infrastructure.

2 Prioritizing "Make in Vietnam" products that meet technical, quality, and security requirements, thereby creating market opportunities for domestic enterprises.

Promoting research, development, and technology mastery, forming a complete value chain from R&D, testing, and certification to commercialization.

3

4 Ensuring financial resources, requiring a minimum allocation of 15% of the total budget in digital transformation and IT application programs and projects for cybersecurity.

Integrating cybersecurity into system design from the outset, minimizing situations in which security is added only after deployment.

5





II

NEW CONTENT IN THE CYBERSECURITY LAW



Mandating adequate resource allocation for cybersecurity in digital transformation and IT projects.



Allocating a minimum of 15% of the total budget in digital transformation and IT application programs and projects for cybersecurity protection.



Comprehensive investment throughout the project lifecycle, including equipment, security solutions, monitoring services, incident response, and human resource training.



Reducing risks and remediation costs, while minimizing data leaks, service disruptions, and security technical debt.



Enhancing transparency, auditability, and accountability among project owners, regulatory authorities, and organizational leaders.

Ensuring safe, stable, and sustainable digital transformation, while enhancing the efficiency of public investment.



II

NEW CONTENT IN THE CYBERSECURITY LAW



Establishing a legal framework for international cybersecurity cooperation based on national sovereignty and aligning domestic law with the UN Convention against Cybercrime (Hanoi Convention).



1

Cooperation based on respect for sovereignty, non-interference in internal affairs, equality, mutual benefits, and compliance with Vietnam law.

2

Aligning domestic law with international treaties to enable joint investigations, electronic evidence collection, data preservation, and cybercrime tracing.

3

Establishing a substantive coordination mechanism, including communication channels, early-warning sharing, information exchange, training, and drills.

4

Strictly controlling data sharing, especially state secrets, critical data, and personal data.

5

Enhancing Vietnam's capacity and global standing, while safeguarding national interests and national security during the integration process.



CONDITIONS ENSURING IMPLEMENTATION

III



III

CONDITIONS ENSURING IMPLEMENTATION



Estimated resources for Law implementation



No additional administrative procedures, organizational apparatus, or requests for additional personnel shall be created.

Government agencies and organizations shall execute tasks within their assigned functions and duties.

Funding shall be guaranteed from government sources, including the central budget, local budgets, and other lawful sources.

Conditions ensuring implementation

Timely issuing guiding documents and directing implementation.

Reinforcing legal dissemination and raising awareness among agencies, organizations, and citizens.

Regularly inspecting and supervising the implementation of the Law and its guiding documents.





IMPLEMENTING ENFORCEMENT ACTIVITIES

IV



IV

IMPLEMENTING ENFORCEMENT ACTIVITIES



1

Formulating a plan for implementing the Law

2

Submitting to the Prime Minister a proposal to list and assign drafting teams for guiding decrees on information system protection, cybercrime prevention, cybersecurity measures, business operations, cryptography, and defense-managed sectors.



3

Drafting, issuing, or submitting for issuance detailed regulatory documents, expected to be submitted to the Government in April 2026.

4

Organizing legal dissemination and enforcement of the Law and its guiding execution documents.





Question and Answer





On which date was the Cybersecurity Law 2025 passed by the National Assembly, and when does it take effect?



ANSWER

The Law on Cybersecurity No. 116/2025/QH15 was passed by the 15th National Assembly on December 10th, 2025, and shall take effect as of July 1st, 2026.





Which legal documents are replaced by the Cybersecurity Law 2025?



ANSWER

Effective July 1, 2026, the Cybersecurity Law 2025 replaces and consolidates the Network Information Safety Law and Cybersecurity Law No. 24/2018/QH14 into a single legal framework.





How is data security defined under the Cybersecurity Law 2025?



ANSWER

Data security ensures data quality, processing, and use for digital transformation while preventing unauthorized access, alteration, destruction, or threats to national security and public safety.





How are information systems classified?



ANSWER

Information systems are classified into 5 levels based on potential harm to national security, public order, and legal rights caused by system incidents or cyber violations.





How does the Law regulate acts of using artificial intelligence or new technologies for impersonation or forgery?



ANSWER

The Law strictly prohibits using AI or new technologies to forge individuals' videos, images, or voices, as well as posting banned content, providing a legal basis to combat Deepfake fraud, defamation, and abuse.





What is the time limit for online service providers to block and remove reported information upon request?

ANSWER

Domestic and foreign service providers in Vietnam must remove violating content or services within 24 hours of a request from the Ministry of Public Security's cybersecurity force, or within 6 hours in emergencies threatening national security.





What are the responsibilities of parents or guardians in protecting children in cyberspace?



ANSWER

When children use online services, parents or guardians must register accounts with their own information, manage accessed and shared content, and protect children's rights under cybersecurity and child laws.



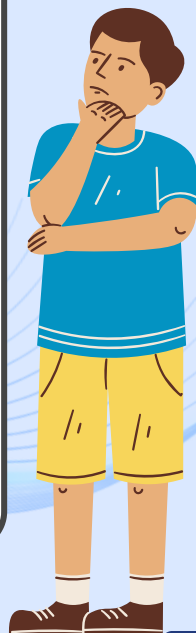


How are acts of illegally trading of personal information and data regulated under the Law?



ANSWER

The Law strictly prohibits illegally collecting, using, trading, or sharing personal data, as well as using fake identities or stolen information to register or trade business, bank, securities, or digital accounts.





What is the minimum funding allocation for cybersecurity in digital transformation and IT application programs and projects?



ANSWER

State-funded entities must allocate annual expenditure and at least 15% of IT and digital transformation project budgets to cybersecurity protection.





How does the Cybersecurity Law 2025 regulate transitional provisions?



ANSWER

Transitional provisions (without a general 12-month period):

1. Systems with previously established levels remain unchanged but must comply with new cybersecurity standards and measures within 12 months of this Law's effective date.
2. Network information security and civil cryptography licenses issued before July 1, 2026, remain valid until their specified expiration date.
3. Network information security products, services, solutions, and equipment deployed before this Law's effective date may continue in use if they meet compliance requirements within 12 months.





DEPARTMENT OF CYBER SECURITY AND
HIGH-TECH CRIME PREVENTION - MINISTRY OF PUBLIC SECURITY

CYBERSECURITY LAW HANDBOOK

ENABLING DEVELOPMENT IN THE DIGITAL ERA

SAFEGUARDING CYBERSECURITY SOVEREIGNTY



UNDERSTANDING THE LAW



RAISING AWARENESS



PREVENTING PROACTIVELY



PENALIZING VIOLATIONS



Scan the QR

Cybersecurity Law No.
116/2025/QH15

