Chapter I: GENERAL PROVISIONS

Article 1. Scope of regulation

1. This Law provides for the research, development, provision, deployment, and use of artificial intelligence systems (hereinafter referred to as artificial intelligence activities); the rights and obligations of relevant organizations and individuals; and state management of artificial intelligence activities in Vietnam.
2. Artificial intelligence activities serving exclusively for national defense, security, and cipher purposes are not within the scope of regulation of this Law.

Article 2. Subjects of application

This Law applies to Vietnamese agencies, organizations, and individuals, as well as foreign organizations and individuals participating in artificial intelligence activities in Vietnam.

Article 3. Interpretation of terms

In this Law, the following terms shall be understood as follows:

1. **Artificial intelligence** is the electronic implementation of human intellectual capabilities, including learning, reasoning, perception, judgment, and natural language understanding.
2. **Artificial intelligence system** is a machine-based system designed to perform artificial intelligence capabilities with varying levels of autonomy, capable of self-adaptation after deployment; based on clearly defined or implicitly formed objectives, the system infers from input data to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

3. **Developer** is an organization or individual that designs, builds, trains, tests, or fine-tunes all or part of a model, algorithm, or artificial intelligence system and has direct control over technical methods, training data, or model parameters.
4. **Provider** is an organization or individual that brings an artificial intelligence system to the market or puts it into use under their own name, brand, or trademark, regardless of whether that system was developed by them or a third party.
5. **Deployer** is an organization, individual, or state agency that uses an artificial intelligence system under its control in professional, commercial activities or in providing services; excluding cases of personal, non-commercial use.
6. **User** is an organization or individual that directly interacts with an artificial intelligence system or uses the output of that system.
7. **Affected person** is an organization or individual directly or indirectly impacted in terms of legal rights, interests, life, health, property, reputation, or access to services due to the deployment or output of an artificial intelligence system.
8. **Serious incident** is an event occurring during the operation of an artificial intelligence system that causes or risks causing significant damage to human life, health, fundamental rights, property, cybersecurity, public order, the environment, or disrupts the operation of critical information systems for national security.

Article 4. Fundamental principles in artificial intelligence activities

1. Human-centric, ensuring human rights, privacy, national interests, public interests, and national security; complying with the Constitution and the law.
2. Artificial intelligence serves humans and does not replace human authority and responsibility. Ensure the maintenance of human

control and the ability to intervene in every decision and behavior of artificial intelligence systems; system safety, data security, and information confidentiality; the ability to inspect and supervise the development and operation process of the system.

3. Ensure fairness, transparency, non-bias, non-discrimination, and no harm to humans or society; comply with ethical standards and Vietnamese cultural values; perform accountability for the decisions and consequences of the system.
4. Promote green, inclusive, and sustainable artificial intelligence development; encourage the development and application of artificial intelligence technologies toward efficient energy use, resource conservation, and reduction of negative impacts on the environment.

Article 5. State policies on artificial intelligence activities

1. Have policies to develop artificial intelligence into an important driver for growth, innovation, and sustainable development of the country.
2. Encourage controlled technology testing; apply management measures proportionate to the level of risk and encourage voluntary compliance mechanisms.
3. Have policies to ensure the rights and create conditions for organizations and individuals to access, learn, and benefit from artificial intelligence; encourage the development and application of artificial intelligence for social welfare, supporting people with disabilities, the poor, and ethnic minorities to bridge the digital divide; preserve, promote, and maintain national cultural identity.
4. Prioritize investment and mobilization of social resources to develop data infrastructure, computing infrastructure, safe artificial intelligence, high-quality human resources, and shared artificial intelligence platforms of national strategic importance.

5. Prioritize the application of artificial intelligence in management, administration, public service provision, and decision-making support of state agencies to enhance efficiency, transparency, and service quality for citizens and businesses; encourage widespread application in economic and social sectors to improve productivity, service quality, and management efficiency.
6. Encourage organizations, networks, and social initiatives that promote safety, ethics, reliability, and build social trust in artificial intelligence development.
7. Promote the application of artificial intelligence in business activities and key economic and social sectors; develop the startup and innovation ecosystem; encourage public-private partnerships.
8. Proactively integrate and cooperate internationally; participate in building and shaping global governance standards and frameworks; ensure national interests and sovereignty in the field of artificial intelligence.

Article 6. Application of artificial intelligence in sectors and fields

1. The application of artificial intelligence in sectors and fields must comply with risk management principles as prescribed by this Law and relevant laws.
2. For essential sectors with direct impact on human life, health, rights, and legal interests or social order and safety, the application of artificial intelligence must be managed under stricter risk control appropriate to the characteristics of each sector, including:
   a) Healthcare: ensuring patient safety; reliability under actual conditions of use; protection of health data according to legal regulations;
   b) Education: ensuring suitability with the age characteristics and development of learners; preventing risks in assessment,

classification, and impact on learners; ensuring data safety and privacy.

3. The application of artificial intelligence in scientific research activities must ensure compliance with research ethics and scientific integrity, and prevent fraudulent behavior or plagiarism during the research and result publication process.
4. The Government, ministries, and ministerial-level agencies, within the scope of their functions, duties, and powers, shall detail requirements for safety, risk management, and deployment conditions for the application of artificial intelligence in the sectors and fields under their management, ensuring consistency with this Law.

Article 7. Prohibited acts

1. Taking advantage of or misappropriating artificial intelligence systems to commit violations of the law, infringing upon the rights and legal interests of organizations and individuals.
2. Developing, providing, deploying, or using artificial intelligence systems for the following purposes:
   a) Performing acts prohibited by law;
   b) Using fake elements or simulating real people and events to intentionally and systematically deceive or manipulate human perception and behavior, causing serious harm to human rights and legal interests;
   c) Taking advantage of the weaknesses of vulnerable groups, including children, the elderly, people with disabilities, ethnic minorities, or persons lacking civil act capacity, persons with limited civil act capacity, or persons with difficulties in perception and behavior control, to cause harm to themselves or others;
   d) Creating or disseminating fake content capable of causing serious harm to national security, social order, and safety.

3. Collecting, processing, or using data to develop, train, test, or operate artificial intelligence systems contrary to legal regulations on data, personal data protection, intellectual property, and cybersecurity.
4. Obstructing, disabling, or falsifying human supervision, intervention, and control mechanisms over artificial intelligence systems as prescribed by this Law.
5. Concealing information that must be made public, transparent, or accountable; erasing or falsifying mandatory information, labels, or warnings in artificial intelligence activities.
6. Taking advantage of research, testing, evaluation, or verification activities of artificial intelligence systems to commit acts contrary to the law.

Article 8. One-stop electronic portal for artificial intelligence and national database on artificial intelligence systems

1. The one-stop electronic portal for artificial intelligence is a digital platform established to support the receipt and registration of participation in controlled testing; receiving notifications of artificial intelligence system classification results, serious incident reports, and periodic reports; making public information about artificial intelligence systems, conformity assessment results, and violation handling results according to law; and connecting support programs, funds, infrastructure, and shared data.
2. The national database on artificial intelligence systems is built and managed uniformly to serve the management, supervision, and publicizing of information about artificial intelligence systems according to law.
3. The publicization, connection, and sharing of data on the one-stop electronic portal for artificial intelligence and the national database on

artificial intelligence systems must ensure information safety and security; protect state secrets, business secrets, and personal data.

4. The Government details the operation, management, and exploitation mechanism of the one-stop electronic portal for artificial intelligence and the national database on artificial intelligence systems.

Chapter II: CLASSIFICATION AND MANAGEMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS ACCORDING TO RISK

Article 9. Classification of risk levels of artificial intelligence systems

1. Artificial intelligence systems are classified into the following levels:
   a) High-risk artificial intelligence systems are systems that can cause significant damage to the life, health, rights, and legal interests of organizations and individuals, national interests, public interests, and national security;
   b) Medium-risk artificial intelligence systems are systems capable of causing confusion, impacting, or manipulating users because they do not recognize that the interacting entity is an artificial intelligence system or the content is generated by the system;
   c) Low-risk artificial intelligence systems are systems that do not fall under the cases prescribed in points a and b, Clause 1 of this Article.
2. The risk classification of artificial intelligence systems is determined based on criteria regarding the level of impact on human rights, safety, and security; the sector in which the system is used, especially essential sectors or those directly related to public interests; the scope of users and the scale of the system's influence.
3. The Government details this Article.

Article 10. Classification and notification of artificial intelligence systems

1. Providers shall self-classify artificial intelligence systems before putting them into use. Systems classified as medium-risk or high-risk must be accompanied by classification dossiers.
2. Deployers may inherit the classification results from providers and are responsible for ensuring the safety and integrity of the system during use; in case of modification, integration, or change of functions that generate new or higher risks, they shall coordinate with the provider to perform re-classification.
3. For systems classified as medium-risk or high-risk, providers must notify the classification results to the Ministry of Science and Technology through the one-stop electronic portal for artificial intelligence before putting them into use. Organizations and individuals developing low-risk artificial intelligence systems are encouraged to make basic system information public to increase transparency.
4. In cases where the risk level cannot be determined, providers may request the Ministry of Science and Technology for guidance on the classification level based on technical dossiers.
5. Inspection and supervision are carried out according to the risk level of the system:
   a) High-risk systems are inspected periodically or when there are signs of violation;
   b) Medium-risk systems are supervised through reports, sample testing, or evaluation by independent organizations;
   c) Low-risk artificial intelligence systems are monitored and inspected when there are incidents, feedback, or when safety needs to be ensured, without generating unnecessary obligations for organizations and individuals.
6. Based on the inspection and supervision results prescribed in Clause 5 of this Article, when detecting deviations or dishonest declarations,

competent authorities shall require re-classification, dossier supplementation, or temporary suspension of use, while simultaneously handling the matter according to law.

7. The Government details the content to be notified, orders, procedures for notification, and technical guidance on risk classification.

Article 11. Transparency responsibilities

1. Providers shall ensure that artificial intelligence systems interacting directly with humans are designed and operated so that users recognize they are interacting with the system, except where otherwise provided by law.
2. Providers shall ensure that audio, image, and video content generated by artificial intelligence systems are marked in machine-readable formats according to Government regulations.
3. Deployers are responsible for clearly notifying when providing the public with text, audio, images, or videos generated or edited by artificial intelligence systems if such content is capable of causing confusion about the authenticity of events or characters, except where otherwise provided by law.
4. Deployers are responsible for ensuring that audio, images, and videos generated or edited by artificial intelligence systems to simulate or emulate the appearance or voice of real people or recreate real events must be attached with recognizable labels to distinguish them from real content. For products that are cinematographic, artistic, or creative works, the labeling prescribed in this Clause shall be performed in an appropriate manner, ensuring it does not obstruct the display, performance, or enjoyment of the work.
5. Providers and deployers are responsible for maintaining transparent information as prescribed in this Article throughout the process of providing the system, product, or content to users.

6. The Government details the forms of notification and labeling.

Article 12. Responsibility for management and handling of artificial intelligence incidents

1. Developers, providers, deployers, and users of artificial intelligence systems have the responsibility to ensure safety, security, and reliability, and to promptly detect and remedy incidents capable of causing harm to people, property, data, or social order.
2. When a serious incident occurs in an artificial intelligence system, developers, providers, deployers, and users have the following responsibilities:
   a) Developers and providers must urgently apply technical measures to remedy, temporarily suspend, or recall the system, and simultaneously notify competent authorities;
   b) Deployers and users have the obligation to record and promptly notify the incident and coordinate during the remedy process.
3. Competent state management agencies shall receive, verify, and guide the handling of incidents; when necessary, they have the right to request temporary suspension, recall, or re-evaluation of the system.
4. Reporting and handling of incidents are carried out via the one-stop electronic portal for artificial intelligence.
5. The Government regulates the reporting and responsibilities of relevant agencies, organizations, and individuals, appropriate to the severity of the incident and the scope of influence of the artificial intelligence system.

Article 13. Conformity assessment for high-risk artificial intelligence systems

1. High-risk artificial intelligence systems must undergo conformity assessment according to the provisions of this Law before being put

into use or when there are significant changes during use. In cases where there are standards or technical regulations on artificial intelligence systems, conformity assessment must also be performed according to the law on standards and technical regulations.

2. Conformity assessment is the confirmation that an artificial intelligence system meets the requirements in Article 14 of this Law and is performed as follows:

   a) For high-risk artificial intelligence systems on the List requiring conformity certification before use: the assessment is performed by a conformity assessment organization that has been registered or recognized according to law;

   b) For other high-risk artificial intelligence systems: the provider self-assesses conformity or hires a conformity assessment organization that has been registered or recognized according to law.
3. Conformity assessment results are a condition for high-risk artificial intelligence systems to be permitted for use; organizations and individuals with assessed systems are responsible for maintaining conformity and making information public according to Government regulations; and serve as a basis for performing inspection and supervision of compliance with Article 10 of this Law.
4. The Prime Minister stipulates the List of high-risk artificial intelligence systems, including the list of systems requiring conformity certification before being put into use.
5. Organizations performing conformity assessment or verification of artificial intelligence systems must ensure independence, possess sufficient technical capacity according to regulations, and be subject to periodic supervision by competent state agencies.
6. The Government details this Article.

Article 14. Management of high-risk artificial intelligence systems

1. Providers of high-risk artificial intelligence systems have the responsibility to:
   a) Establish and maintain risk management measures and regularly review them when the system has significant changes or new risks arise;
   b) Manage training, testing, and operational data ensuring quality within technical capabilities and appropriate to the system's intended purpose;
   c) Establish, update, and store technical dossiers and activity logs to the extent necessary for conformity assessment and post-use inspection; provide this information to competent state agencies according to the principles of necessity and proportionality to the inspection purpose, without disclosing business secrets;
   d) Design the system to ensure human supervision and intervention capabilities;
   e) Perform transparency obligations and incident handling according to Articles 11 and 12 of this Law;
   f) Perform accountability to competent state agencies regarding the purpose of use, operational principles at a functional description level, main types of input data, risk management and control measures, and necessary contents for inspection and examination; simultaneously provide public information to users and affected persons at a functional description level, operating methods, and risk warnings to ensure safety in use; accountability and information provision shall not require disclosure of source code, detailed algorithms, parameter sets, or information belonging to business or technological secrets;
   g) Coordinate with competent state agencies and deployers in inspection, evaluation, post-inspection, and incident remedy related to the system.

2. Deployers of high-risk artificial intelligence systems have the responsibility to:
   a) Operate and supervise the system according to the purpose, scope, and risk level as classified, without generating new or higher risks;
   b) Ensure data safety, security, and human intervention capabilities during use;
   c) Maintain compliance with standards and technical regulations on artificial intelligence during system operation;
   d) Perform transparency obligations and incident handling according to Articles 11 and 12 of this Law;
   e) Perform accountability to competent state agencies regarding system operation, risk control measures, incident handling, and necessary contents for inspection and examination; simultaneously provide public information to users and affected persons at a functional description level, operating methods, and risk warnings to ensure safety in use;
   f) Coordinate with providers and competent state agencies in inspection, evaluation, post-inspection, and incident remedy.
3. Users of high-risk artificial intelligence systems have the responsibility to comply with operating procedures, technical instructions, and safety measures; not to interfere illegally to change system features and to promptly notify incidents to the deployer.
4. Accountability must be appropriate to the technical capabilities of the system and not disclose business secrets according to law.
5. Encourage providers and deployers to participate in civil liability insurance or apply other appropriate obligation guarantee measures to promptly remedy incidents and compensate for damages.
6. Foreign providers having high-risk artificial intelligence systems provided in Vietnam must have a legal contact point in Vietnam; in cases where the system requires mandatory conformity certification

before use, they must have a commercial presence or an authorized representative in Vietnam.

7. The Government details this Article.

Article 15. Management of medium-risk and low-risk artificial intelligence systems

1. Medium-risk artificial intelligence systems are managed as follows:
   a) Providers and deployers must ensure transparency as prescribed in Article 11 of this Law;
   b) Providers are responsible for accountability regarding the purpose of use, operational principles at a functional description level, main input data, and risk management and safety measures of the system upon request by state agencies during inspection and examination or when there are signs of risk or incidents; accountability does not require disclosure of source code, detailed algorithms, parameter sets, or business or technological secrets;
   c) Deployers are responsible for accountability regarding the operation, risk control, incident handling, and protection of the rights and legal interests of organizations and individuals upon request by competent state agencies during inspection, examination, or incident handling;
   d) Users are responsible for complying with regulations on notification and labeling of the system.
2. Low-risk artificial intelligence systems are managed as follows:
   a) Providers are responsible for accountability upon request by competent state agencies in cases where there are signs of law violation or impact on the rights and legal interests of organizations and individuals;
   b) Deployers are responsible for accountability upon request by competent state agencies in cases where there are signs of law

violation or impact on the rights and legal interests of organizations and individuals;

c) Users have the right to exploit and use the system for legal purposes and are solely responsible before the law for their usage activities.

3. The State encourages organizations and individuals deploying medium-risk and low-risk artificial intelligence systems to apply technical standards on artificial intelligence.

Chapter III: DEVELOPMENT OF INFRASTRUCTURE AND ASSURANCE OF NATIONAL ARTIFICIAL INTELLIGENCE SOVEREIGNTY

Article 16. National artificial intelligence infrastructure

1. National artificial intelligence infrastructure is strategic infrastructure, including infrastructure invested in by the State, enterprises, and social organizations; it is developed as a unified, open, safe ecosystem with the capability for connection, sharing, and expansion, ensuring it meets the requirements for the development and application of artificial intelligence.
2. The State holds the role of directing, coordinating, and ensuring infrastructure capacity to serve national artificial intelligence development; encourages enterprises, research institutes, universities, and social organizations to invest in, build, and share infrastructure; and strengthens public-private partnerships in developing artificial intelligence infrastructure.
3. The State invests in, builds, and operates artificial intelligence infrastructure provided as a public service, serving research, development, state management, and supporting innovative startup enterprises, including: computing capacity and shared data; training platforms, testing and experimental environments; foundational models, general-purpose artificial intelligence models, large language

models for Vietnamese and ethnic minority languages; and other infrastructure components.

4. National artificial intelligence infrastructure invested in by the State, enterprises, and social organizations shall be connected, shared, and exploited according to technical standards, regulations, and requirements for safety, security, and data protection.
5. Important artificial intelligence applications in essential sectors according to the list issued by the Prime Minister must be deployed on national artificial intelligence infrastructure to ensure safety, security, and control capability.
6. The Government shall stipulate in detail the mechanism for coordination, sharing, incentives, and measures to promote the development of national artificial intelligence infrastructure, appropriate for each stage and the requirements for ensuring national safety and security.

Article 17. Databases serving artificial intelligence

1. Databases serving artificial intelligence are important components of the national artificial intelligence infrastructure, including national databases, databases of ministries, ministerial-level agencies, agencies under the Government, People's Committees at all levels, and databases of organizations and individuals; they are created, managed, and exploited to serve training, testing, evaluation, and development of artificial intelligence applications according to the provisions of law on data, personal data protection, and intellectual property.
2. National databases on artificial intelligence invested in, built, and operated by the State at the National Data Center shall be organized as open, safe, and controlled, meeting requirements for quality,

connectivity, and exploitation; including open data, conditional open data, and commercial data according to the provisions of law.

3. Databases serving artificial intelligence of ministries, ministerial-level agencies, agencies under the Government, and People's Committees at all levels shall be built, updated, and connected uniformly with the national database on artificial intelligence; ensuring technical standards, regulations, data quality, and information safety.
4. Databases of organizations and individuals serving artificial intelligence are encouraged to be shared with state agencies and other organizations and individuals according to an agreement mechanism; the sharing must comply with the law on data, personal data protection, and intellectual property, ensuring the rights and legal interests of the parties involved.
5. The Prime Minister shall issue a List of datasets serving the development of artificial intelligence in essential sectors, prioritizing cultural data, Vietnamese and ethnic minority language data, administrative procedure data, healthcare, education, agriculture, environment, transportation, socio-economics, and other important sectors.
6. The Government shall stipulate in detail the principles of connection, mechanisms for sharing, exploitation, and data safety assurance in databases serving artificial intelligence.

Article 18. Mastery of artificial intelligence technology

1. The State prioritizes the development and mastery of core artificial intelligence technologies; prioritizes resources for research and development of general-purpose artificial intelligence models, large language models for Vietnamese and ethnic minority languages, Vietnamese knowledge processing technology, computing capacity, and high-performance training technology, hardware, and

semiconductors serving artificial intelligence; promotes the development and application of open source to enhance technological autonomy, safety, and national sovereignty in the digital environment.

2. The State promotes research, development, perfection, and application of domestic artificial intelligence technology; supports organizations and individuals in developing models, algorithms, software, hardware, and foundational technologies; encourages solutions that save resources, are easy to deploy, and are suitable for Vietnam's conditions; develops national endogenous capacity and the innovation ecosystem for artificial intelligence; strengthens public-private cooperation to master technology.
3. Organizations and individuals researching, developing, and mastering core artificial intelligence technologies are entitled to preferential policies and specific support according to the provisions of law.
4. The State promotes the application of artificial intelligence serving research, analysis, and scientific simulation, technology design and testing, automation of research, development, and innovation processes to enhance national scientific and technological capacity; creates conditions to form the capacity to create and master the entire lifecycle of artificial intelligence technology.
5. The Government shall stipulate in detail the mechanisms, criteria, and measures to promote the mastery of artificial intelligence technology, appropriate for each development stage and the requirements for ensuring national safety and security.

Chapter IV: ARTIFICIAL INTELLIGENCE APPLICATION, DEVELOPMENT OF INNOVATION ECOSYSTEM AND HUMAN RESOURCES

Article 19. National Strategy on Artificial Intelligence

1. The Prime Minister shall issue the National Strategy on Artificial Intelligence, and shall review, evaluate, and update it periodically at least every 03 years or when there are major changes in technology or the market. Ministries, ministerial-level agencies, agencies under the Government, and People's Committees at all levels have the responsibility to integrate the goals and tasks of the Strategy into their sector, field, and local development strategies and plans and ensure resources for implementation.
2. The National Strategy on Artificial Intelligence is built on the basis of development orientations for technology, infrastructure, data, and human resources; promotes research, mastery, and application of artificial intelligence in priority sectors; ensures safety, innovation, and national sovereignty in the digital environment. The Strategy must stipulate a system of indicators, methods, and measurement mechanisms to evaluate the level of national artificial intelligence development.
3. The State encourages the development of groups of artificial intelligence technologies suitable for Vietnam's conditions, with the potential to create added value, be environmentally friendly, easily applicable on a wide scale, and contribute to ensuring national sovereignty in the digital environment.

Article 20. Development of the artificial intelligence ecosystem and market

1. Organizations and individuals operating in the field of artificial intelligence are entitled to the highest incentives and support according to the provisions of law on science and technology, investment, digital technology industry, high technology, digital transformation, and other relevant laws; are created with conditions to access infrastructure, data, and testing environments serving

research, production, and commercialization of artificial intelligence products and services.

2. The State supports the development of the artificial intelligence ecosystem and market, including:
   a) Prioritizing the use of artificial intelligence products and services according to the provisions of law on bidding;
   b) Developing the market for artificial intelligence products and services, including technology transaction floors and supply-demand connection platforms;
   c) Ensuring fair and transparent access to computing infrastructure, data, and controlled testing environments;
   d) Applying preferential policies on tax, investment, and finance according to the principle of encouraging research, production, and commercialization of artificial intelligence products and services.
3. The State encourages the development and application of next-generation artificial intelligence, promoting innovation, enhancing management capacity, production, business, and public service provision.
4. Organizations, individuals, enterprises, research facilities, and state agencies are encouraged to exploit, share, and reuse data in the national database on artificial intelligence for research, training, testing, and innovation, ensuring compliance with laws on data, cybersecurity, and intellectual property.
5. Small and medium-sized enterprises and innovative startup enterprises in artificial intelligence are prioritized for access to technical infrastructure, data, and testing environments, and are entitled to support in costs, training, and market connection for the development of artificial intelligence products and services.

6. The Government shall stipulate in detail the mechanisms, conditions, and procedures for implementing measures to support the development of the artificial intelligence ecosystem and market.

Article 21. Controlled testing mechanism for artificial intelligence

1. The controlled testing mechanism for artificial intelligence is implemented according to the provisions of law on science, technology, and innovation and the provisions in Clauses 2, 3, and 4 of this Article.
2. Controlled testing results are the basis for competent state agencies to consider:
   a) Recognizing conformity assessment results according to the provisions of this Law;
   b) Exempting, reducing, or adjusting corresponding compliance obligations of this Law.
3. Competent state agencies shall preside over and coordinate with relevant agencies to receive, appraise, and process dossiers according to a fast appraisal and feedback process; supervise the testing process and decide to temporarily suspend or terminate testing when there are risks affecting safety, security, or the rights and legal interests of organizations and individuals.
4. The Government shall stipulate in detail this Article.

Article 22. National Artificial Intelligence Development Fund

1. The National Artificial Intelligence Development Fund is an extra-budgetary state financial fund, operating not for profit, established by the Government to mobilize, coordinate, and allocate resources to promote the research, development, application, and management of artificial intelligence serving socio-economic

development, national defense, security, and enhancing national competitive capacity.

2. Financial sources of the Fund include sources allocated from the state budget; contributions, aid, and sponsorship from domestic and foreign organizations and individuals; and other legal sources according to the provisions of law.
3. The Fund is applied a specific financial mechanism, accepting risks in science, technology, and innovation; allocates capital flexibly according to progress and implementation requirements, regardless of the fiscal year; is applied shortened sequences and procedures for tasks of a strategic nature or requiring rapid deployment. The Fund is prioritized for investment, sponsorship, and support for:
   a) Development of artificial intelligence infrastructure;
   b) Research, development, and mastery of core artificial intelligence technologies;
   c) Development of artificial intelligence enterprises;
   d) Training, fostering, and attracting artificial intelligence human resources;
   dd) Other investment and support tasks serving artificial intelligence development goals as stipulated by the Government.
4. The Fund operates on the principles of openness, transparency, efficiency, and correct purpose; ensuring coordination and no duplication with other state financial funds.
5. The Government shall stipulate in detail the specific financial mechanism, organization, management, use, and supervision of the Fund.

Article 23. Development of artificial intelligence human resources

1. The State develops artificial intelligence human resources in a comprehensive and interconnected manner across educational levels

and training degrees, ensuring the formation of a high-quality human resource team serving research, development, application, and management of artificial intelligence.

2. General education integrates basic content on artificial intelligence, computational thinking, digital skills, and technology ethics into the mandatory curriculum; encourages experiential activities, research, and creativity in the field of artificial intelligence.
3. Vocational education institutions and higher education institutions are encouraged to build training programs on artificial intelligence, data science, and related specialties; are encouraged to cooperate with enterprises, research institutes, and international organizations in training, internship, research, and technology transfer.
4. The State implements the National Program for the Development of Artificial Intelligence Human Resources, including policies on training, scholarships, attracting and utilizing experts, developing a team of lecturers, scientists, and management human resources in the field of artificial intelligence.
5. Organizations, training facilities, research institutes, and enterprises participating in the development of artificial intelligence human resources are entitled to incentive mechanisms and preferences according to the provisions of law, and at the same time have the responsibility to coordinate in training, applied research, and professional practice, linking training with practical needs.
6. Higher education institutions, research institutes, and innovation centers have the responsibility to cooperate, share knowledge, and participate in national and international networks on training, research, and development of artificial intelligence human resources.
7. The Ministry of Education and Training shall preside over building and submitting to the Prime Minister for issuance the National Program on Developing Artificial Intelligence Human Resources,

which stipulates standards, recognition of training programs, mechanisms for mobilizing resources, and preferential policies for participating organizations and individuals.

Article 24. Development of artificial intelligence clusters

1. An artificial intelligence cluster is a cooperation network between enterprises, research institutes, universities, and related organizations, organized toward strengthening links in functions, artificial intelligence infrastructure, and physical space to promote innovation, artificial intelligence development, and enhance competitive capacity.
2. The State encourages the development of artificial intelligence clusters according to a model combining concentrated physical space and digital linkage networks; forming cluster centers at high-tech zones, concentrated digital technology zones, and innovation centers; attracting organizations and individuals to invest in building technical infrastructure serving the operations of the cluster, including laboratories, testing centers, verification centers, and other support facilities meeting national and international standards.
3. Organizations and individuals that are members of recognized artificial intelligence clusters are entitled to the following preferential policies:
   a) Priority access to and use of national artificial intelligence infrastructure, shared data, and testing platforms at preferential costs;
   b) Support to participate in human resource training programs, trade promotion, and key scientific and technological tasks.
4. The Government shall stipulate in detail the criteria, sequence, procedures for recognition, operating mechanisms of artificial intelligence clusters, and preferential policies in Clause 3 of this Article.

Article 25. Support for enterprises in the field of artificial intelligence

1. Innovative startup enterprises and small and medium-sized enterprises are supported with the costs of conformity assessment as prescribed by this Law; are provided for free with sample dossiers, self-assessment tools, training, and consulting; and are prioritized for support from the National Artificial Intelligence Development Fund.
2. Innovative startup enterprises, small and medium-sized enterprises, scientific and technological organizations, and research groups with feasible innovation projects are supported through support vouchers to use computing infrastructure, shared datasets, large language models for Vietnamese and ethnic minority languages, training platforms, testing, and technical consulting services serving research, development, and deployment of artificial intelligence applications.
3. Enterprises with capacity for research, development, and innovation in the field of artificial intelligence are prioritized to participate in national-level scientific and technological tasks, tasks for high-technology development prioritized for investment, strategic technologies, and key digital technology products; are supported to develop core technologies, foundational models, hardware, and high-performance training technology according to national artificial intelligence capacity development orientations.
4. Enterprises participating in artificial intelligence testing under the controlled testing mechanism are supported with technical consulting, risk assessment, safety testing, and connection with testing and verification facilities according to the provisions of law.
5. Enterprises that share data, models, tools, or research results serving artificial intelligence development are entitled to incentives or support according to the provisions of law, ensuring compliance with law on data, personal data protection, and intellectual property.

6. The State encourages cooperation between enterprises, research institutes, universities, and innovation centers to develop artificial intelligence technology, commercialize research results, and expand innovation capacity; encourages enterprises to invest long-term in artificial intelligence research and development.
7. The Government shall stipulate in detail the mechanisms, conditions, and procedures for implementing policies to support enterprises in the field of artificial intelligence.

Chapter V: ETHICS AND RESPONSIBILITY IN ARTIFICIAL INTELLIGENCE ACTIVITIES

Article 26. National Artificial Intelligence Ethical Framework

1. The National Artificial Intelligence Ethical Framework is issued based on the following principles:
   a) Ensuring safety, reliability, and no harm to human life, health, honor, dignity, and spiritual life;
   b) Respecting human rights and citizen rights, ensuring fairness, transparency, and non-discrimination in the development and use of artificial intelligence;
   c) Promoting happiness, prosperity, and the sustainable development of humans, communities, and society;
   d) Encouraging creativity, innovation, and social responsibility in research, development, and application of artificial intelligence.
2. The National Artificial Intelligence Ethical Framework is reviewed and updated periodically or when there are major changes in technology, law, and management practices.
3. The National Artificial Intelligence Ethical Framework is the basis for directing the construction of technical standards, regulations,

specialized guidelines, and policies to encourage safe, reliable, and responsible artificial intelligence development.

4. The State encourages organizations and individuals to apply the National Artificial Intelligence Ethical Framework in the process of design, development, deployment, and use of artificial intelligence systems to ensure transparency, fairness, safety, and respect for human rights.
5. The Minister of Science and Technology shall issue the National Artificial Intelligence Ethical Framework based on the provisions in Clause 1 of this Article.

Article 27. Ethical responsibility and impact assessment when applying artificial intelligence in state management and public service provision

1. The use of artificial intelligence systems in state management and public service provision must ensure openness, transparency, and the responsibility to comply with the National Artificial Intelligence Ethical Framework.
2. Artificial intelligence systems do not replace the authority and decision-making responsibility of decision-makers according to the provisions of law. Decision-makers are responsible for reviewing and using results provided by artificial intelligence systems.
3. Agencies operating artificial intelligence systems belonging to the high-risk group or having a significant impact on human rights, social fairness, or public interests must prepare an impact assessment report on the use of the system; the report includes the identification of risks, control measures, and assurance of human supervision and intervention capabilities.
4. The agency preparing the report is responsible for the content, truthfulness, and completeness of the report; the report is made

public according to the provisions of law, except for content belonging to state secrets, business secrets, or personal data.

5. The Government shall stipulate in detail the content, process, and responsibility for impact assessment, risk management, and supervision of the use of artificial intelligence systems in the state sector.

Chapter VI: INSPECTION, EXAMINATION AND HANDLING OF VIOLATIONS

Article 28. Inspection and examination

1. Inspection activities in the field of artificial intelligence are carried out according to the provisions of law on inspection.
2. Agencies and organizations assigned to perform state management functions over artificial intelligence have the responsibility to examine the compliance with the law by organizations and individuals in artificial intelligence activities.
3. In the process of inspection and examination, relevant organizations and individuals have the obligation to provide technical dossiers, trace logs, training data, and other necessary information to determine the cause of violations or incidents or to allocate responsibility; the provision of information must comply with the provisions of law on the protection of state secrets, data, personal data protection, and intellectual property.
4. Inspection and examination conclusions and decisions on administrative violation handling must be made public according to the provisions of law.

Article 29. Violation handling and responsibility for compensation for damage

1. Organizations and individuals that commit violations of the provisions of this Law and other relevant legal provisions related to artificial intelligence shall, depending on the nature, level, and consequences of the violation, be administratively sanctioned or prosecuted for criminal liability; if they cause damage, they must compensate according to the provisions of civil law.
2. In cases where high-risk artificial intelligence systems are managed, operated, and used correctly according to regulations but damage still occurs, the deployer must bear the responsibility for compensating the victim. After compensation, the deployer shall request the provider, developer, or related parties to reimburse the compensation amount if there is an agreement between the parties.
3. Responsibility for compensation for damage as prescribed in Clause 2 of this Article is exempted in the following cases:
   a) The damage occurs entirely due to the intentional fault of the victim;
   b) The damage occurs in cases of force majeure or states of emergency, except where otherwise provided by law.
4. In cases where an artificial intelligence system is intruded upon, seized control of, or illegally intervened in by a third party, the third party must bear the responsibility for compensating for damage. In cases where the deployer or provider is at fault for allowing the system to be intruded upon, seized control of, or illegally intervened in, they must be jointly liable for compensation according to the provisions of civil law.
5. The Government shall stipulate in detail administrative sanctions for violations caused by artificial intelligence systems.

Chapter VII: STATE MANAGEMENT OF ARTIFICIAL INTELLIGENCE

Article 30. Content and responsibility of state management of artificial intelligence

1. Content of state management of artificial intelligence includes:
   a) Building, issuing, and organizing the implementation of strategies, policies, programs, and legal normative documents on artificial intelligence;
   b) Issuing and organizing the implementation of technical standards and regulations on artificial intelligence;
   c) Managing, coordinating, and developing national artificial intelligence infrastructure;
   d) Managing and supervising artificial intelligence activities;
   dd) Propagating and disseminating policies and laws; statistics, reporting, scientific research, and international cooperation on artificial intelligence;
   e) Inspecting, examining, handling violations, and resolving disputes, complaints, and denunciations regarding artificial intelligence.
2. Responsibility for state management of artificial intelligence:
   a) The Government uniformly performs state management of artificial intelligence;
   b) The Ministry of Science and Technology is the focal agency, responsible before the Government for performing state management of artificial intelligence nationwide;
   c) Ministries and ministerial-level agencies, within the scope of their functions, duties, and powers, shall coordinate with the Ministry of Science and Technology to perform state management of artificial intelligence;
   d) People's Committees of provinces shall perform state management of artificial intelligence in their localities.

Would you like me to translate the final section (Articles 31 to 35) as well?

Article 31. Principles for providing information and data for state management

1. Competent state agencies, organizations, and individuals assigned to perform state management activities under the provisions of this Law are responsible for ensuring the confidentiality of information and data, as well as business secrets provided during the performance of their duties, including technical dossiers, training data, source code, and algorithms according to the provisions of law.
2. Requests for organizations and individuals to provide information and data must ensure necessity, balance, and reasonableness with the scope, purpose, and content of state management activities.
3. Information and data provided must be ensured for safety and security according to the provisions of law.

Article 32. International cooperation

1. International cooperation in the field of artificial intelligence shall be carried out according to the provisions of law on science and technology, law on technology transfer, other relevant legal provisions, and international treaties to which the Socialist Republic of Vietnam is a member.
2. The State encourages international cooperation in sharing high-performance computing infrastructure, data, human resources, scientific research, and the recognition of conformity assessment results according to the provisions of this Law.

Chapter VIII: IMPLEMENTATION PROVISIONS

Article 33. Repealing a number of chapters, articles, clauses, and points of the Law on Digital Technology Industry No. 71/2025/QH15 Repeal Clause 9 of Article 3; Clause 7 of Article 4; Clause 6 of Article 12; Point dd,

Clause 2 of Article 34; and Chapter IV on artificial intelligence of the Law on Digital Technology Industry.

Article 35. Transitional provisions

1. For artificial intelligence systems that have been put into operation before the date this Law takes effect, providers and deployers are responsible for performing compliance obligations according to the provisions of this Law within the following time limits:
    a. 18 months from the date this Law takes effect for artificial intelligence systems in the fields of healthcare, education, and finance;
    b. 12 months from the date this Law takes effect for artificial intelligence systems not falling under the cases prescribed in Point a of this Clause.
2. During the time limits prescribed in Clause 1 of this Article, the artificial intelligence system may continue to operate, except where the state management agency for artificial intelligence determines the system has a risk of causing serious damage, in which case it has the right to request temporary suspension or termination of operations.