

中华人民共和国 网络安全法

发布机构：全国人民代表大会
常务委员会
发布日期：2016 年 11 月 7 日
生效日期：2017 年 6 月 1 日

http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm
中国人权于 2022 年 11 月 17 日
登陆该网页。

第一章 总则

第一条

为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条

在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条

国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设 and 互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

Cybersecurity Law of the People's Republic of China*

Promulgating entity: Standing Committee of the
National People's Congress
Date of promulgation: November 7, 2016
Date of legal effect: June 1, 2017

*English translation based on China Law Translate,
<http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en>, last visited Nov. 16, 2022.

Chapter One: General Provisions

Article 1

This Law is formulated so as to safeguard cybersecurity, to maintain cyberspace sovereignty and national security, and the public interest, to protect the lawful rights and interests of citizens, legal persons, and other organizations, and to promote the healthy development of economic and social informatization.

Purpose

Article 2

This Law is applicable to the construction, operation, maintenance, and usage of networks, and to cybersecurity supervision and management, within the borders of the People's Republic of China.

Scope

Article 3

The state persists in placing equal importance on cybersecurity and informatization development; adheres to the objectives of active use, scientific development, management in accordance with the law, and assurance of security; promotes the construction of network infrastructure and interconnectivity; encourages innovation and application of network technology; supports the cultivation of cybersecurity talent; establishes and

Equal importance of cybersecurity and informatization development

improves systems to safeguard cybersecurity; and raises the capacity for cybersecurity protection.

第四条

国家制定并不断完善网络安全战略，明确保障网络安全的基本要求 and 主要目标，提出重点领域的网络安全政策、工作任务和措施。

Article 4

The state formulates and continuously improves cybersecurity strategies; clarifies the fundamental requirements and primary goals of safeguarding cybersecurity; and puts forward cybersecurity policies, work duties, and measures for key fields.

State's role in formulating cybersecurity policy

第五条

国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

Article 5

The state adopts measures to monitor, prevent, and handle cybersecurity risks and threats originating from both within and outside the borders of the People's Republic of China; protects critical information infrastructure against attacks, intrusions, interference, and damage; punishes unlawful and criminal cyberactivities in accordance with the law; and preserves cyberspace security and order.

State's role in responding to cybersecurity risks

第六条

国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

Article 6

The state advocates honest, trustworthy, healthy, and civilized cyber conduct; promotes dissemination of core socialist values; adopts measures to raise the entire society's awareness and level of cybersecurity; and forms a good environment for the entire society to jointly participate in advancing cybersecurity.

Public's role in promoting civilized cyber conduct

第七条

国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

Article 7

The state actively develops international exchange and cooperation in such areas as cyberspace governance, network technologies research and development and standards formulation, and attacking unlawful and criminal cyberactivities; promotes the construction of a peaceful, secure, open, and cooperative cyberspace; and establishes a multilateral, democratic, and transparent system for cyber governance.

International exchange and cooperation

第八条

国家网信部门负责统筹协调网络安全工作和相关监督管理工

Article 8

The state's cyberspace administration authorities are responsible for the overall planning and

Cyberspace administration authorities

作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

coordination of cybersecurity work and related supervision and management work. The State Council departments for telecommunications, public security, and other relevant organs are responsible for cybersecurity protection, and supervision and management work within the scope of their respective responsibilities, in accordance with the provisions of this Law, relevant laws, and administrative regulations.

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

Cybersecurity protection and supervision and management responsibilities for relevant departments of local people's governments at the county level or above shall be determined in accordance with the relevant state regulations.

Authority of state entities at or above county level

第九条

网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

Article 9

Network operators carrying out business and service activities must comply with laws and administrative regulations, respect social ethics, comply with commercial ethics, be honest and trustworthy, fulfill obligations to protect cybersecurity, accept supervision by the government and society, and bear social responsibility.

Obligations of network operators

第十条

建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

Article 10

The construction and operation of networks, or the provision of services through networks, shall be in accordance with provisions of laws and administrative regulations, and the mandatory requirements of state standards; [with the] adoption of technical measures and other necessary measures to safeguard cybersecurity and operational stability; [with] effective response to cybersecurity incidents; [with] prevention of unlawful and criminal cyberactivities; and [with] maintenance of the integrity, confidentiality, and usability of network data.

Network activity standards

第十一条

网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络

Article 11

Internet-related industry organizations shall, in accordance with their charters, strengthen industry self-discipline, formulate cybersecurity codes of

Industrial organization obligations

安全保护，提高网络安全保护水平，促进行业健康发展。

conduct, guide their members in strengthening cybersecurity protection, raise the level of cybersecurity protection, and promote the healthy development of the industry.

第十二条

国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

Article 12

The state protects the rights of citizens, legal persons, and other organizations to use the Internet, in accordance with the law; promotes the popularization of network access; raises the level of network services, provides secure and convenient network services to society; and safeguards the lawful, orderly, and free circulation of network information.

State obligations

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

Any person and organization using a network shall comply with the Constitution and laws, comply with public order, and respect social ethics; must not endanger cybersecurity; and must not use the network to engage in such activities that endanger the security, honor, and interests of the nation, that incite subversion of state power or the overthrow of the socialist system, that incite separatism or damage national unity, that propagate terrorism or extremism, that propagate ethnic hatred or ethnic discrimination, that disseminate violent, obscene, or pornographic information, that fabricate or disseminate false information to disrupt the economic or social order, and that infringe on another's reputation, privacy, intellectual property, or other legitimate rights and interests.

Individual and organizational obligations

第十三条

国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

Article 13

The state supports the research and development of network products and services conducive to the healthy growth of minors; punishes in accordance with the law the exploitation of networks to engage in activities that endanger the physical and mental health of minors; and provides a safe and healthy cyber environment for minors.

Protection of juveniles

第十四条

任何个人和组织有权对危害网络安全的行为向网信、电信、

Article 14

Any individuals and organizations have the right to report acts endangering cybersecurity to the

Reporting cybersecurity threats

公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

departments of cyberspace administration, telecommunications, public security, and so forth. Departments receiving reports shall promptly process them in accordance with the law. If the reports do not fall within the responsibilities of that department, they shall be promptly transferred to departments with the authority to handle them.

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

Relevant departments shall preserve the confidentiality of the informant's information and protect the informant's lawful rights and interests.

Protecting reporter's confidentiality

第二章 网络安全支持与促进

Chapter Two: Support for and Promotion of Cybersecurity

第十五条

国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

Article 15

The state establishes and improves the cybersecurity standards system. The State Council administrative department for standardization and other relevant State Council departments, on the basis of their respective responsibilities, organize the formulation and timely revision of relevant national and industry standards for cybersecurity management as well as for the security of network products, services, and operations.

Cybersecurity standards system

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

The state supports enterprises, research institutions, institutions of higher education, and network-related industry organizations to participate in the formulation of national and industry standards for cybersecurity.

Role of non-state entities in formulating cybersecurity standards

第十六条

国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参

Article 16

The State Council and people's governments of provinces, autonomous regions, and directly-administered municipalities shall handle overall planning; expand their input; support key cybersecurity technology industries and projects; support cybersecurity technology research and development, and application; promote safe and trustworthy network products and services; protect

Role of state entities

与国家网络安全技术创新项目。

the intellectual property rights of network technologies; and support the participation of enterprises, research institutions, institutions of higher education, and others in state cybersecurity technology innovation projects.

第十七条

国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

Article 17

The state promotes the construction of cybersecurity service systems for society and encourages relevant enterprises and institutions to develop cybersecurity certification, testing, risk assessment, and other such security services.

Cybersecurity service systems

第十八条

国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

Article 18

The state encourages the development of network data security protection and utilization technologies, advances the opening of public data resources, and promotes technological innovation and economic and social development.

Encouraging network technology innovation

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

The state supports the innovation of cybersecurity management methods, and the application of new network technologies, to raise the level of cybersecurity protections.

Encouraging cybersecurity management innovation

第十九条

各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

Article 19

People's governments at all levels and their relevant departments shall organize and carry out regular cybersecurity public education, and guide and urge relevant units in thoroughly doing cybersecurity public education work.

Cybersecurity publicity and education

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

The mass media shall conduct targeted cybersecurity public education aimed at society.

Role of mass media in publicity and education

第二十条

国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

Article 20

The state supports enterprises, institutions of higher education, vocational schools, and other educational training institutions to carry out cybersecurity-related education and training, employ diverse methods to cultivate cybersecurity talent, and promote the exchange of cybersecurity talent.

Role of educational institutions in carrying out cybersecurity education and training

第三章 网络运行安全

Chapter Three: Network Operations Security

第一节 一般规定

Section One: Ordinary Provisions

第二十一条

国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条

网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风

Article 21

The state implements a tiered cybersecurity protection system. Network operators shall fulfill the following security protection obligations according to the requirements of the tiered cybersecurity protection system to safeguard the network from interference, damage, or unauthorized visits, and prevent network data leaks, theft, or tampering:

(1) formulate internal security management systems and operating rules, assign persons responsible for cybersecurity, and carry out cybersecurity protection responsibilities;

(2) adopt technological measures to prevent computer viruses, cyberattacks, cyber intrusions, and other acts that endanger cybersecurity;

(3) adopt technological measures for monitoring and recording network operational status and cybersecurity incidents, and keep relevant network logs for at least six months in accordance with the provisions;

(4) adopt measures such as data classification and backup and encryption of important data; and

(5) [fulfill] other obligations as specified by laws or administrative regulations.

Article 22

Network products and services shall comply with the mandatory requirements of the relevant national standards. Providers of network products and services must not install malware; upon discovery that their network products and services have security flaws, vulnerabilities, or other such

Obligations of network operators under a tiered cybersecurity system

Internal security management systems

Defensive technological measures

Monitoring and recording network operational status

Data management

Other obligations

Obligations of providers of network products and services

险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条

网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条

网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应

risks, they shall immediately adopt remedial measures, and promptly inform users and report to the relevant competent departments in accordance with the provisions.

Providers of network products and services shall continuously provide security maintenance for their products and services; and must not terminate the provision of security maintenance during either the specified time period or the time period agreed upon with clients.

Where network products and services have the capacity to collect user information, their providers shall make this clear to users and obtain consent; where users' personal information is involved, [providers] shall also abide by provisions of this Law and relevant laws and administrative regulations concerning personal information protection.

Article 23

Critical network equipment and dedicated cybersecurity products shall only be sold or provided after a qualified institution approves their security certifications or deems they meet the requirements of a security inspection in accordance with the mandatory requirements of national standards. The state's cyberspace administration departments, together with the relevant departments of the State Council, will formulate and publish a catalog of critical network equipment and dedicated cybersecurity products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24

Network operators handling network access and domain name registration services for users, handling network access procedures for landline or mobile phones, or providing users with information distribution or instant messaging services, shall require users to provide real identity

Ongoing security maintenance of products and services

Notification of user information collection and protection of user information

Selling or provision of critical network equipment and dedicated cybersecurity products

Obligation to require users' real identity information

当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

information when signing agreements with users or confirming provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

The state implements the strategy for trusted network identity, supports the research and development of secure and convenient technology for digital identification authentication, and promotes the reciprocal recognition among different digital identification authentications.

Trusted network identity and digital identification authentication

第二十五条

网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

Article 25

Network operators shall formulate emergency response plans for cybersecurity incidents, promptly address system vulnerabilities, computer viruses, cyberattacks, cyber intrusions, and other such security risks; and, when an incident that endangers cybersecurity occurs, immediately activate the emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with provisions.

Cybersecurity incident emergency response plans

第二十六条

开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

Article 26

Those carrying out cybersecurity certification, inspection, risk assessment, or other such activities, and publishing cybersecurity information such as system vulnerabilities, computer viruses, cyber-attacks, or cyber intrusions to society, shall comply with the relevant national provisions.

Publishing information on cybersecurity incidents

第二十七条

任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不

Article 27

No individuals or organizations may engage in activities that endanger cybersecurity, such as illegally intruding into others' networks, interfering with the normal functions of others' networks, or stealing network data; provide programs or tools that are specifically used to engage in cyber intrusions, interfere with the normal functions and preventive measures of the networks, steal network data or other activities that

Prohibitions against activities that endanger cybersecurity, or support such activities

得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条

网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条

国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条

网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的 运行安全

第三十一条

国家对公共通信和信息服务、能源、交通、水利、金融、公

endanger cybersecurity; or, when clearly knowing that others will engage in activities endangering cybersecurity, provide them with help such as technological support, advertisements and promotion, or payment services.

Article 28

Network operators shall provide technical support and assistance to public security organs and national security organs in their activities to maintain national security and investigate crimes in accordance with the law.

Obligation of network operators to assist public and national security organs

Article 29

The state supports cooperation among network operators in areas such as cybersecurity information collection, analysis, circulation, and emergency response handling, so as to raise the network operators' security assurance capacities.

Cooperation between network operators

Relevant industry organizations are to establish and improve cybersecurity protection codes and cooperation mechanisms for their industry, strengthen analysis and assessment of cybersecurity risks, and regularly provide risk alerts to members, and support and assist members in responding to cybersecurity risks.

Cybersecurity protection measures

Article 30

Information obtained by cyberspace administration departments and relevant departments in the course of fulfilling cybersecurity protection obligations can only be used for the needs of maintaining cybersecurity, and must not be used in other ways.

Use of information obtained by cyberspace administration authorities

Section Two: Operational Security for Critical Information Infrastructure

Article 31

The state implements, on the basis of the tiered cybersecurity protection system, key protection of important industries and sectors, such as public

Scope of the state's protection of critical

共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

communication and information services, energy sources, public transportation services, water resources, financial services, public services, e-government affairs, and other critical information infrastructure, that once subjected to damage, loss of function, or data leaks, could seriously endanger national security, the national economy and the people's livelihood, and the public interest. The specific scope of and security protection measures for critical information infrastructure are formulated by the State Council.

information infrastructure

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

The state encourages network operators outside the scope of critical information infrastructure to voluntarily participate in the system for protecting critical information infrastructure.

Voluntary participation in system for protecting critical information infrastructure

第三十二条

按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

Article 32

In accordance with the obligations and division of labor specified by the State Council, departments responsible for the work of protecting the security of critical information infrastructure shall each compile and organize the implementation of its critical information infrastructure security plan for its respective industry or sector, and guide and supervise the security protection work for the operation of critical information infrastructure.

Role of State departments in protecting critical information infrastructure

第三十三条

建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

Article 33

The construction of critical information infrastructure shall ensure that it has the properties of supporting stable and continuous operation, and ensure that security technical measures are planned, constructed, and used concurrently.

Properties of construction of critical information infrastructure

第三十四条

除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

Article 34

In addition to the provisions of Art. 21 of this Law, critical information infrastructure operators shall also fulfill the following security protection obligations:

Obligations of critical information infrastructure operators

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

(1) set up specialized security management bodies and appoint a person responsible for security management; and conduct security background checks on such responsible person and personnel in key positions;

Security management bodies

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

(2) regularly conduct cybersecurity education and technical training for employees and evaluate their technical abilities;

Employee education and training

（三）对重要系统和数据库进行容灾备份；

(3) make disaster recovery backups of important systems and databases;

Disaster recovery backups

（四）制定网络安全事件应急预案，并定期进行演练；

(4) formulate emergency response plans for cybersecurity incidents and regularly conduct drills; and

Emergency response plans

（五）法律、行政法规规定的其他义务。

(5) [fulfill] other obligations as specified by laws or administrative regulations.

第三十五条

关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

Article 35

The purchase of network products and services by critical information infrastructure operators which could affect national security shall undergo a national security review organized by the state's cyberspace administration departments and relevant State Council departments.

National security review of critical information infrastructure purchases and services

第三十六条

关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

Article 36

Critical information infrastructure operators purchasing network products and services shall, in accordance with provisions, sign a security and confidentiality agreement with the provider, clarifying obligations and responsibilities for security and confidentiality.

Security and confidentiality agreements for critical information infrastructure purchases and services

第三十七条

关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全

Article 37

Personal information and other important data collected or generated by critical information infrastructure operators during operations within the borders of the People's Republic of China shall be stored within its borders. If, for business needs, they truly need to be provided to a party outside the borders, a security evaluation shall be

Storage and sharing of personal and important data collected by critical information infrastructure operators

评估；法律、行政法规另有规定的，依照其规定。

conducted in accordance with the methods formulated by the state's cyberspace administration departments and relevant State Council departments. Where laws or administrative regulations provide otherwise, those provisions shall be followed.

第三十八条

关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

Article 38

Critical information infrastructure operators shall themselves conduct, or entrust cybersecurity service institutions to conduct, inspection and assessment of the security of and potential risks existing in their networks at least once a year, and report the outcome of the inspection and evaluation and improvement measures to the relevant departments responsible for critical information infrastructure security protection work.

Annual inspection and assessment of critical information infrastructure

第三十九条

国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

Article 39

The state's cyberspace administration departments shall handle overall planning and coordinate with relevant departments in adopting the following measures for critical information infrastructure security protection:

Role of cyberspace administration authorities for protection of critical information infrastructure:

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

(1) conduct spot inspections of critical information infrastructure security risks, put forward improvement measures, and, when necessary, may entrust a cybersecurity service institution to conduct inspection and assessment of the security risks existing in the networks;

Spot inspections of critical information infrastructure

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

(2) regularly organize critical information infrastructure operators to conduct cybersecurity emergency response drills, so as to improve their level of response to cybersecurity incidents and their collaboration and cooperation capacity;

Cybersecurity emergency response drills

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

(3) promote sharing of cybersecurity information among [entities such as] relevant departments, critical information infrastructure operators and relevant research institutions, and cybersecurity service institutions; and

Sharing cybersecurity information

(四) 对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

(4) provide technical support and assistance for [actions such as] emergency response handling of cybersecurity incidents and restoration of network functions.

Provide technical support and assistance

第四章 网络信息安全

Chapter Four: Network Information Security

第四十条

网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

Article 40

Network operators shall keep user information they collect strictly confidential, and establish and improve user information protection systems.

Confidentiality and protection of user information

第四十一条

网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

Article 41

In collecting and using personal information, network operators shall abide by the principles of legality, legitimacy, and necessity; make public the rules for collection and use; explicitly state the purpose, means, and scope of the information collection and use; and obtain the consent of the persons whose data are collected.

Principles of use of user information

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

Network operators must not collect personal information unrelated to the services they provide; must not collect or use personal information in violation of the provisions of laws, administrative regulations, or agreements between the parties; and shall follow the provisions of laws, administrative regulations, and agreements with users in processing the personal information they have stored.

Prohibitions on collection and use of user information

第四十二条

网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

Article 42

Network operators must not leak, tamper with, or destroy the personal information they collect; and, without the consent of the person whose information was collected, must not provide personal information to others. But information that has been processed in which specific

Additional prohibitions and exceptions for anonymous user data

individuals are not discernable and which cannot be restored to its original state is excepted.

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

Network operators shall adopt technological measures and other necessary measures to ensure the security of personal information they collect, and prevent information leaks, damage, or loss. When leaks, damage, or loss of personal information occurs, or may occur, they shall immediately adopt remedial measures, and promptly inform users and report to the relevant competent departments in accordance with provisions.

Protection of personal information

第四十三条

个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

Article 43

Where individuals discover that network operators have violated provisions of laws, administrative regulations, or agreements between the parties to collect or use their personal information, they have the right to require the network operators to delete their personal information; where they find that their personal information collected or stored by network operators contains errors, they have the right to require the network operators to make corrections. Network operators shall adopt measures for deletions and corrections.

Deleting and correcting personal information

第四十四条

任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

Article 44

No individuals or organizations may steal or use other illegal methods to acquire personal information, or unlawfully sell or unlawfully provide others with personal information.

Prohibitions on acquisition of personal information

第四十五条

依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

Article 45

Departments that bear cybersecurity supervision and management responsibilities in accordance with the law and their staff must maintain the strict confidentiality of personal information, private information, and commercial secrets that they learn of in fulfilling their responsibilities, and must not leak, sell, or unlawfully provide it to others.

Obligations of state departments in handling confidential information

第四十六条

任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

Article 46

Any individuals and organizations shall be responsible for their conduct in using a network and must not establish websites or communication groups used for illegal or criminal activities, such as committing fraud, imparting criminal methods, or producing or selling banned or controlled items; [any individuals and organizations] must not use a network to distribute information involving the commission of fraud, the production or sale of banned or controlled items, or other illegal or criminal activities.

Prohibitions in establishing websites and communication groups

第四十七条

网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

Article 47

Network operators shall strengthen their management of information distributed by their users, and, upon discovering information whose distribution or transmission is prohibited by laws or administrative regulations, shall immediately stop transmission of that information, adopt handling measures such as deletion to prevent the information from spreading, keep relevant records, and report to the relevant competent departments.

Obligation of network operators to manage information published by users

第四十八条

任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

Article 48

Electronic information sent or application software provided by any individuals and organizations must not install malware, and must not contain information whose distribution or transmission is prohibited by laws or administrative regulations.

Prohibitions on content of electronic information or application software sent by individuals and organizations

电子信息发送服务提供者和应用程序下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

Electronic information distribution service providers, and application software download service providers, shall fulfill security management obligations, and, upon knowing that their users have committed acts as set forth in the preceding paragraph, shall stop providing services, adopt handling measures such as deletion, keep relevant records, and report to the relevant competent departments.

Obligations of distributors to monitor information and application content

第四十九条

网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条

国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取删除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条

国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

Article 49

Network operators shall establish network information security complaint and reporting systems, make public information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports related to network information security.

Network operators shall cooperate with the lawful implementation of supervision and inspection by cyberspace administration departments and relevant departments.

Article 50

The state's cyberspace administration departments and relevant departments fulfill network information security supervision and management responsibilities in accordance with the law; upon discovering information whose distribution or transmission is prohibited by laws or administrative regulations, they shall require the network operators to stop transmission, adopt handling measures such as deletion, and keep relevant records; as for information described above which comes from outside the borders of the People's Republic of China, they shall notify the relevant organs to adopt technological measures and other necessary measures to block its dissemination.

Chapter Five: Monitoring, Early Warnings, and Emergency Response Handling

Article 51

The state establishes a system for cybersecurity monitoring, early warnings, and information notifications. The state's cyberspace administration departments shall handle the overall planning and coordination of the work of relevant departments in strengthening cybersecurity information collection, analysis, and notification and, in accordance with provisions, centrally issue

Network information security complaint and reporting systems

Cooperation with cyberspace administration authorities

Blocking transmission of domestic and extraterritorial illegal content

Cybersecurity monitoring, warning, and notification system

第五十二条

负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

cybersecurity monitoring and early warning information.

Article 52

Departments responsible for the work of critical information infrastructure security protection shall establish and improve a system for cybersecurity monitoring, early warning, and information notification for their own industry and sector, and submit cybersecurity monitoring and early warning information in accordance with provisions.

Cybersecurity monitoring system for critical information infrastructure

第五十三条

国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

Article 53

The state's cyberspace administration departments coordinate with relevant departments to establish and improve mechanisms for cybersecurity risk assessment and emergency response work, formulate cybersecurity incident emergency response plans, and regularly organize drills.

Role of cyberspace administration authorities in establishing cybersecurity monitoring system

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

Departments responsible for the work of critical information infrastructure security protection shall formulate cybersecurity incident emergency response plans for their own industry and sector, and regularly organize drills.

Cybersecurity incident emergency response plans for critical information infrastructure

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

Cybersecurity incident emergency response plans shall rank cybersecurity incidents on the basis of factors such as the degree of harm after the incident occurs and the scope of the impact, and specify the corresponding emergency response handling measures.

Criteria for emergency response plans

第五十四条

网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

Article 54

When the risk of the occurrence of cybersecurity incidents increases, the relevant departments of people's governments at the provincial level and above shall adopt the following measures, according to the specified scope of authority and procedures and based on the features of the cybersecurity risk and the harm it may cause:

State role in responding to increased cybersecurity risks

(一) 要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

(1) require the relevant departments, institutions, and personnel to promptly collect and report relevant information, and strengthen the monitoring of cybersecurity risks;

Collect and report information

(二) 组织有关部门、机构和专业技术人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

(2) organize relevant departments, institutions, and specialist personnel to conduct analysis and assessment of information on cybersecurity risks, and forecast the likelihood of an incident's occurrence, the scope of its impact, and its level of harm; and

Conduct analysis and assessment

(三) 向社会发布网络安全风险预警，发布避免、减轻危害的措施。

(3) distribute cybersecurity risk warnings to society, and distribute measures for avoiding or mitigating harm.

Publish risk warnings and measures

第五十五条

发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

Article 55

When a cybersecurity incident occurs, the cybersecurity incident emergency response plan shall be immediately activated; an investigation and evaluation of the cybersecurity incident shall be conducted; network operators shall be required to adopt technological and other necessary measures to eliminate the latent security risks and prevent harm from spreading; and warning information relevant to the public shall be promptly distributed to society.

Cybersecurity incident emergency response plan activation

第五十六条

省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

Article 56

When relevant departments of people's governments at the provincial level or above discover, in the course of fulfilling their cybersecurity supervision and management responsibilities, that the network has a relatively major security risk or that a security incident has occurred, they may, according to the specified scope of authority and procedures, summon the legal representative or main person in charge of the network operator for a chat. Network operators shall follow requirements to adopt measures to carry out corrections, and eliminate latent risks.

State investigation of cybersecurity risks and incidents

第五十七条

因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

Article 57

Emergencies or production safety accidents that occur as the result of cybersecurity incidents shall be handled in accordance with the provisions of relevant laws and administrative regulations, such as the *Emergency Response Law of the People's Republic of China* and the *Production Safety Law of the People's Republic of China*.

Applicable laws governing emergencies resulting from cybersecurity incidents

第五十八条

因维护国家和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

Article 58

In order to maintain national security and social public order and as is required for handling major sudden social security incidents, temporary measures such as restricting network communications in a specific region may be adopted, following a decision or approval by the State Council.

Region-specific restriction of network communication

第六章 法律责任

Chapter Six: Legal Liability

第五十九条

网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

Article 59

Network operators who do not fulfill the cybersecurity protection obligations specified in the provisions of Art. 21 or Art. 25 of this Law will be ordered to make corrections and given warnings by the relevant competent departments; those who refuse to make rectifications or cause such consequences as the endangerment of cybersecurity will be fined not less than RMB10,000 and not more than RMB100,000; the directly responsible person in charge will be fined not less than RMB5,000 and not more than RMB50,000.

Network operator liability

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚

Critical information infrastructure operators who do not fulfill the cybersecurity protection obligations specified in the provisions of Art. 33, Art. 34, Art. 36, or Art. 38 of this Law will be ordered to make corrections and given warnings by the relevant competent departments; those who refuse to make rectifications or cause such consequences as the endangerment of

Critical information infrastructure operator liability

款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条

违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条

网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业

cybersecurity will be fined not less than RMB100,000 and not more than RMB1 million; the directly responsible person in charge will be fined not less than RMB10,000 and not more than RMB100,000.

Article 60

Those who violate the provisions of Art. 22, para. 1 or 2 or Art. 48, para. 1 of this Law, by committing any of the acts listed below, will be ordered to make corrections and given warnings by the relevant competent departments; those who refuse to make rectifications or cause such consequences as the endangerment of cybersecurity will be fined not less than RMB50,000 and not more than RMB500,000; the directly responsible person in charge will be fined not less than RMB10,000 and not more than RMB100,000:

(1) installing malware;

(2) failing to immediately adopt remedial measures to address such risks as security flaws or vulnerabilities that exist in their products or services, or failing to promptly inform users and report to the relevant competent departments in accordance with the provisions; or

(3) ending the provision of security maintenance for their products or services without authorization.

Article 61

Network operators who violate the provisions of Art. 24, para. 1 of this Law, by failing to require users to provide true identity information or providing relevant services to users who do not provide true identity information, will be ordered to make corrections by the relevant competent departments; those who refuse to make rectifications or whose circumstances are serious will be fined not less than RMB50,000 and not more than RMB500,000, and the relevant

Liability for violating Art. 22, Art. 48, and other specific infractions

Installing malware

Failing to address risks

Ending ongoing security maintenance

Liability of network operators who fail to require users to submit identity information in violation of Art. 24

整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条

违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条

违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上

competent departments may order them to temporarily suspend the relevant business, suspend operations and undergo rectification, shut down the website, or revoke the relevant business permit or operating license; and the directly responsible person in charge and other directly responsible persons will be fined not less than RMB10,000 and not more than RMB100,000.

Article 62

Those who violate the provisions of Art. 26 of this Law, in carrying out activities such as cybersecurity certifications or inspection or risk assessments, or distributing to society cybersecurity information such as system vulnerabilities, computer viruses, cyberattacks, or cyber intrusions, will be ordered to make corrections and given warnings by the relevant competent departments; those who refuse to make rectifications or whose circumstances are serious will be fined not less than RMB10,000 and not more than RMB100,000, and the relevant competent departments may order them to temporarily suspend the relevant business, suspend operations and undergo rectification, shut down the website, or revoke the relevant business permit or operating license; the directly responsible management person in charge and other directly responsible persons will be fined not less than RMB5,000 and not more than RMB50,000.

Liability of those violating provisions regarding cybersecurity assessments in violation of Art. 26

Article 63

Those who violate the provisions of Art. 27 of this Law, by engaging in activities endangering cybersecurity, or providing programs or tools specifically used for engaging in activities endangering cybersecurity, or providing others engaging in activities endangering cybersecurity with help such as technological support, advertisements and promotion, or payment services, where a crime is not constituted, will have their unlawful gains confiscated and be detained for up to five days by public security organs, and may also be fined not less than

Liability for those endangering cybersecurity in violation of Art. 27

十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条

网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

RMB50,000 and not more than RMB500,000; those whose circumstances are serious will be detained for not less than five days and not more than 15 days, and may also be fined not less than RMB100,000 and not more than RMB1 million.

Units committing acts listed in the preceding paragraph will have their unlawful gains confiscated by public security organs, be fined not less than RMB100,000 and not more than RMB1 million; the directly responsible person in charge and other directly responsible persons will be punished in accordance with the provisions in the preceding paragraph.

Persons who receive public security administrative punishments for violation of the provisions of Art. 27 of this Law must not engage in the work of cybersecurity management or key positions in network operation for five years; persons who receive criminal punishments must not engage in the work of cybersecurity management or key positions in network operation for life.

Article 64

Network operators and network product or service providers who violate the provisions of Art. 22, para. 3 and Arts. 41-43 of this Law, by infringing the right of lawful protection of personal information, will be ordered to make corrections by the relevant competent departments; depending on the circumstances, they may be, singly or in combination, given warnings, have their unlawful gains confiscated, or be fined not less than the equivalent of and no more than 10 times the amount of the unlawful gains; where there are no unlawful gains, they will be fined up to RMB1 million, with the directly responsible person in charge and other directly responsible persons receiving fines not less than RMB10,000 and not more than RMB100,000; where the circumstances are serious, they may be ordered to temporarily suspend the relevant business, suspend operation and undergo rectification, shut down the website,

Prohibitions on future employment for certain violations

Liability of network operators and network product or service providers violating personal information protection

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条

关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条

关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

and have the relevant business permit or operating license revoked.

Those who violate the provisions of Art. 44 of this Law, by stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, where a crime is not constituted, will have their unlawful gains confiscated by public security organs, and fined not less than the equivalent of and no more than 10 times the amount of the unlawful gains; and where there are no unlawful gains, they will be fined up to RMB1 million.

Article 65

Critical information infrastructure operators who violate the provisions of Art. 35 of this Law, by using network products or services that have not undergone security review or did not pass security review, will be ordered by the relevant competent departments to stop such usage and fined not less than the equivalent of and not more than 10 times the purchase price; and the directly responsible person in charge and other directly responsible persons will be fined not less than RMB10,000 and not more than RMB100,000.

Liability of critical information infrastructure operators bypassing security reviews in violation of Art. 35

Article 66

Critical information infrastructure operators who violate the provisions of Art. 37 of this Law, by storing network data outside the borders [of the People's Republic of China], or providing network data to those who are outside the borders, will be ordered to make corrections and given warnings by the relevant competent departments, will have their unlawful gains confiscated, and will be fined not less than RMB50,000 and not more than RMB500,000, and may be ordered to temporarily suspend the relevant business, suspend operation and undergo rectification, shut down the website, or have the relevant business permit or operating license revoked; the directly responsible person in charge and other directly responsible persons will

Liability of critical information infrastructure operators who store data outside the country in violation of Art. 37

be fined not less than RMB10,000 and not more than RMB100,000.

第六十七条

违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条

网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取删除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

Article 67

Those who violate the provisions of Art. 46 of this Law, by establishing a website or communication group used to carry out illegal or criminal activities, or by using a network to distribute information involving carrying out illegal or criminal activities, where a crime is not constituted, will be detained for up to five days by public security organs, and may be fined not less than RMB10,000 and not more than RMB100,000; those whose circumstances are serious will be detained for not less than five days and not more than 15 days, and may also be fined not less than RMB50,000 and not more than RMB500,000. The website or communication group used to carry out the illegal or criminal activities will be shut down.

Units committing acts listed in the preceding paragraph will be fined not less than RMB100,000 and not more than RMB500,000 by public security organs; the directly responsible person in charge and other directly responsible persons will be punished in accordance with the provisions in the preceding paragraph.

Article 68

Network operators who violate the provisions of Art. 47 of this Law, by failing to stop the transmission of information whose distribution or transmission is prohibited by laws or administrative regulations, adopt handling measures such as deletion, and keep relevant records will be ordered to make corrections, given warnings, and have their unlawful gains confiscated by the relevant competent departments; those who refuse to make rectifications or whose circumstances are serious will be fined not less than RMB100,000 and not more than RMB500,000, and may be ordered to temporarily suspend the relevant business, suspend operation and undergo rectification, shut down the

Liability of those establishing a website or communication group to commit illegal activities in violation of Art. 46

Liability of network operators failing to stop transmission of illegal information in violation of Art. 47

website, or have the relevant business permit or operating license revoked; and the directly responsible person in charge and other directly responsible persons will be fined not less than RMB10,000 and not more than RMB100,000.

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

Electronic information distribution service providers and application software download service providers who do not fulfill the security management obligations specified in the provisions of Art. 48, para. 2 of this Law will be punished in accordance with the provisions in the preceding paragraph.

第六十九条

网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

Article 69

Network operators who violate the provisions of this Law by any of the acts listed below will be ordered to make corrections by the relevant competent departments; those who refuse to make rectifications or whose circumstances are serious will be fined not less than RMB50,000 and not more than RMB500,000; and the directly responsible person in charge and other directly responsible persons will be fined not less than RMB10,000 and not more than RMB100,000:

Liability of network operators for specified infractions

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

(1) not following the requirements of relevant departments to adopt handling measures on information whose distribution or transmission is prohibited by laws or administrative regulations, such as stopping the transmission or deleting the information;

Failing to properly handle transmission of illegal information

（二）拒绝、阻碍有关部门依法实施的监督检查的；

(2) refusing or obstructing the supervision and inspection by relevant departments in accordance with the law; or

Refusing to collaborate with authorities

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

(3) refusing to provide technical support and assistance to public security organs or state security organs.

Refusing to provide technical support to authorities

第七十条

发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

Article 70

Those who distribute or transmit information whose distribution or transmission is prohibited by Art. 12, para. 2 of this Law or other laws or administrative regulations will be punished in accordance with the provisions of relevant laws or administrative regulations.

Liability of those transmitting illegal information Art. 12

第七十一条

有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

Article 71

Illegal acts as specified in the provisions of this Law will be recorded in the credit file and made public in accordance with relevant laws and administrative regulations.

Credit file records and publication of transgressions

第七十二条

国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

Article 72

Operators of state organs' government affairs networks who do not fulfill the cybersecurity protection obligations specified in the provisions of this Law will be ordered to make corrections by the organs at the next higher level or relevant organs; and the directly responsible person in charge and other directly responsible persons will be given punishment in accordance with the law.

Liability of state actors failing in cybersecurity protection obligations

第七十三条

网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

Article 73

Cyberspace administration departments and relevant departments that violate the provisions of Art. 30 of this Law, by using information obtained for other purposes when fulfilling cybersecurity protection responsibilities, will have the directly responsible person in charge and other directly responsible persons punished in accordance with the law.

Liability of cyberspace administration departments misusing information obtained in the course of their duties Art. 30

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

Staff members of cyberspace administration departments and other relevant departments who are derelict in their duties, abuse their functions and powers, or commit fraud for personal gain, where a crime is not constituted, will be given punishment in accordance with the law.

General liability of cyberspace administration departments derelict in their duties

第七十四条

违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条

境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附则

第七十六条

本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法

Article 74

Those who violate the provisions of this Law and cause harm to others will bear civil liability in accordance with the law.

Those who violate the provisions of this Law through acts that constitute violations of public security administration will be given public security administrative punishments in accordance with the law; where a crime is constituted, criminal liability will be pursued in accordance with the law.

Article 75

Institutions, organizations, or individuals outside the borders [of the People's Republic of China] who engage in activities that endanger the critical information infrastructure of the People's Republic of China, such as attack, intrusion, interference, or damage, and cause serious consequences, will be investigated for legal responsibility in accordance with the law; State Council public security departments and relevant departments may also decide to freeze the assets of such institutions, organizations, or individuals, or adopt other necessary punitive measures against them.

Chapter Seven: Supplementary Provisions

Article 76

In this Law, the terms listed below have the following meanings:

(1) "Networks" refers to systems comprising computers or other information terminals and related equipment that collect, store, transmit, exchange, or process information in accordance with fixed rules and procedures.

(2) "Cybersecurity" refers to the ability, through adopting necessary measures, to prevent network attacks, intrusions, interference, damage, and

Scope of civil liability

Scope of administrative and criminal liability

Foreign or extraterritorial infractions

Definitions

"Networks"

"Cyber-security"

使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

unlawful use, as well as accidents; to enable the networks to be in a state of stable and reliable operation; as well as to safeguard the integrity, confidentiality, and usability of network data.

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

(3) “Network operators” refers to network owners, managers, and network service providers.

“Network operators”

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

(4) “Network data” refers to various types of electronic data collected, stored, transmitted, processed, and produced through a network.

“Network data”

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

(5) “Personal information” refers to various types of information, recorded electronically or through other means, that, individually or in combination with other information, can identify a natural person’s identity, including, but not limited to, a natural person’s full name, birth date, identity document number, personal biometric information, address, or telephone number.

“Personal information”

第七十七条

存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

Article 77

Security protection of network operations that involve storing and processing state secrets information shall, in addition to complying with this Law, also comply with laws and administrative regulations on guarding secrets.

Network operation involving state secrets

第七十八条

军事网络的安全保护，由中央军事委员会另行规定。

Article 78

Security protection for military networks is specified by the Central Military Commission separately.

Military networks

第七十九条

本法自 2017 年 6 月 1 日起施行。

Article 79

This law takes effect on June 1, 2017.

Effective date