|  |  |  |
| --- | --- | --- |
| 发文机关Promulgator | ：: | 全国人民代表大会常务委员会The Standing Committee of the National People's Congress |
| 发布日期Date of Issue | ：: | 2016.11.072016.11.07 |
| 生效日期Effective Date | ：: | 2017.06.012017.06.01 |
| 时效性Effectiveness | ：: | 现行有效Current |
| 文号No.  | ：: | 主席令第五十三号Presidential Decree No. 53 |

# 中华人民共和国网络安全法

# Cybersecurity Law of China

中华人民共和国网络安全法

Cybersecurity Law of China

主席令第五十三号

Presidential Decree No. 53

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

The Cyber Security Law of the People's Republic of China, adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on 7 November 2016, is hereby promulgated, effective 1 June 2017.

中华人民共和国主席 习近平

President Xi Jinping

2016年11月7日

November 7, 2016

中华人民共和国网络安全法

Cybersecurity Law of China

（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

(Adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on 7 November 2016)

第一章 总 则

Chapter 1 General Provisions

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。

Article 1 This Law is formulated for the purposes of ensuring cyber security, safeguarding cyberspace sovereignty, national security and public interest, protecting the legitimate rights and interests of citizens, legal persons and other organisations, and promoting healthy development of economic and social informatisation.

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。

Article 2 The Law shall apply to the construction, operation, maintenance and use of the network as well as the supervision and administration over cyber security within the territory of the People's Republic of China.

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和互联互通，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。

Article 3 The State adheres to equal focus on cyber security and information-based development, follows the guidelines of positive use, scientific development, lawful management and security assurance, promotes the construction of cyber infrastructure and its interconnection, encourages the innovation in and application of cyber technologies, supports the cultivation of talents for cyber security, establishes and perfects the cyber security guarantee system and raises the ability to protect cyber security.

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和主要目标，提出重点领域的网络安全政策、工作任务和措施。

Article 4 The State shall formulate and continuously improve cyber security strategies, specify the basic requirements and main objectives for cyber security protection, and propose cyber security policies, work tasks and measures in key areas.

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 shall take measures to monitor, prevent and deal with cyber security risks and threats from both within and outside the territory of the People's Republic of China, to protect key information infrastructure from attacks, intrusions, interference and damage, to punish illegal criminal activities on the network in accordance with the law and to maintain cyberspace security and order.

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 shall advocate honest, faithful, healthy and civilized cyber behaviors, advance the spreading of the core socialist values, and take measures to raise the awareness and level of cyber security of the whole of society, forming a sound environment for promoting cyber security with the participation of all the public.

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 shall actively carry out international exchange and cooperation in terms of cyberspace governance, research and development of cyber technologies, establishment of standards thereof and fighting against illegal crimes committed on the network and other aspects, promote the construction of a peaceful, safe, open and cooperative cyberspace, and establish a multilateral, democratic and transparent system for network governance.

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。

Article 8 The national cyberspace administration authority is responsible for the overall planning and coordination of cyber security work and relevant supervision and management work. The competent telecommunications department, the public security department and other relevant authorities of the State Council shall be responsible for the protection, supervision and administration of cyber security within the scope of their respective duties in accordance with the provisions of the 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。

Responsibilities of relevant departments under local people's governments at or above the county level for protecting, supervising and administering cyber security shall be determined in accordance with relevant provisions of the State.

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, while carrying out business and service activities, shall abide by laws and administrative regulations, respect social moralities, follow business ethics, act in good faith, perform the obligation of cyber security protection, accept supervision by the government and the society, and undertake social responsibilities.

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 For the construction and operation of networks or the provision of services through networks, it is required to, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, take technical measures and other necessary measures to ensure the secure and stable operation of networks, effectively respond to cyber security incidents, prevent illegal crimes committed on the network, and maintain the integrity, confidentiality and availability of network data.

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，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

Article 11 Cyber-related industrial organizations shall, in accordance with their regulations, intensify industrial self-discipline, formulate regulations on cyber security behaviors, instruct their members to strengthen cyber security protection, enhance the level of cyber security protection and promote the healthy development of relevant industries.

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 networks according to the law, promotes the popularity of network access, and raises the level of network services, so as to provide the public with secure and convenient network services and guarantee the orderly and free flow of network information in accordance with the law.

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 individual and organization using the network shall comply with the Constitution and laws, follow the public order and respect social morals, and shall neither endanger cyber security, nor engage in activities by making use of the network that endanger national security, honor and interests, incite to subvert the State power and overthrow the socialist system, incite to split the country and undermine national unity, advocate terrorism and extremism, ethnic hatred and discrimination, spread violent and pornographic information, fabricate and disseminate false information to disturb the economic and social order, or infringe upon the reputation, privacy, intellectual property and other legitimate rights and interests of others.

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 research and development of network products and services that are favorable to minors' healthy growth, and punishes activities endangering minors' physical and mental health by virtue of the network according to the law, in a bid to provide minors with a safe and healthy network environment.

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、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。

Article 14 Any individual or organization shall have the right to report the behaviors that endanger cyber security to cyberspace administration authorities, telecommunication departments, public security departments, etc. The department receiving a report shall promptly handle it according to law; if the case does not fall within the scope of its duties, it shall timely transfer the case to the department which has the authority to handle it.

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。

The relevant authorities shall keep confidentiality of the relevant information of informants, and protect the legitimate rights and interests of informants.

第二章 网络安全支持与促进

Chapter II Support and Promotion of Cyber Security

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 system of cyber security standards. The competent standardization administrative department under the State Council and other relevant departments under the State Council shall, in accordance with their respective responsibilities, organize the formulation of relevant national and industrial standards for cyber security administration and the security of network products, services and operations and make revisions at appropriate time.

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 industrial organizations to participate in the formulation of national and industrial standards for cyber security.

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、研究机构和高等学校等参与国家网络安全技术创新项目。

Article 16 The State Council and the people's governments of provinces, autonomous regions and municipalities directly under the Central Government shall make the overall planning, increase the input, support key cyber security technology industries and projects, support the research, development and application of cyber security technologies, promote safe and reliable network products and services, protect the intellectual property rights of network technologies and support enterprises, research institutes, institutions of higher learning to participate in national innovation projects related to cyber security technologies.

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 shall boost the construction of a socialized service system for cyber security, encourage enterprises and institutions concerned to provide such security services as the authentication, detection and risk assessment of cyber security.

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 shall encourage the development of technologies for protecting and using network data, promote the availability of public data resources and propel technological innovation and social and economic development.

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 cyber security administration methods and the application of new network technologies to improve the level of cyber security protection.

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 relevant departments thereof shall organize and conduct regular publicity and education on cyber security, and guide, supervise and urge relevant entities to effectively conduct the publicity and education on cyber security.

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 give publicity and education on cyber security targeted at the public specifically.

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 learning, vocational schools and other education training institutions to carry out cyber security-related education and training, adopt multiple methods to cultivate talents for cyber security, and promote the exchange of talents for cyber security.

第三章 网络运行安全

Chapter III Network Operation Security

第一节 一般规定

Section 1 General 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：

Article 21 The State implements the classified protection system for cyber security. Network operators shall fulfill the following security protection obligations according to the requirements of the classified protection system for cyber security to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified:

（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；

1. formulate internal security management systems and operating procedures, determine the persons responsible for cyber security, and implement the responsibility of cyber security protection;

（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；

(II) take technical measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cyber security;

（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；

(III) Take technological measures to monitor and record the network operation status and cyber security incidents, and preserve relevant web logs for no less than six months as per provisions;

（四）采取数据分类、重要数据备份和加密等措施；

(IV) take measures such as data classification, and backup and encryption of important data; and

（五）法律、行政法规规定的其他义务。

(V) Other obligations stipulated by laws and administrative regulations.

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。

Article 22 Network products and services shall comply with the compulsory requirements of the relevant national standards. Providers of network products and services shall not install malwares; upon discovery of risks such as security defects or bugs etc of their network products or services, the provider shall forthwith adopt remedial measures, promptly notify users pursuant to the provisions, and report to the relevant authorities.

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。

Providers of network products and services shall provide security maintenance for their products and services; and shall not terminate the provision of security maintenance within the stipulated period or the period agreed by the parties concerned.

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。

Where network products and services have the function of collecting users' information, the providers shall clearly notify their users and obtain their consent. In the case of involving users' personal information, the providers shall also comply with the provisions regarding the protection of personal information as stipulated by this Law, relevant laws and administrative regulations.

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。

Article 23 Critical network equipment and specialized cyber security products shall, pursuant to the compulsory requirements of the relevant national standards, pass the security certification by qualified institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration authority shall, in concert with relevant departments under the State Council, formulate and release the catalog of critical network equipment and specialized cyber security products, and promote the mutual recognition of security certification and security detection results, so as to avoid repeated certifications and detections.

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。

Article 24 When network operators handle network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information publication services, instant messaging services and other services, they shall require users to provide real identity information at the time of signing agreements with users or confirming the provision of services. Network operators shall not provide services for users who fail to provide their real identity information.

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 of trusted identities in cyberspace, supports the research and development of secure and convenient technologies for electronic identity authentication, and promotes the mutual recognition among different electronic identity authentications.

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 contingency plans for cyber security incidents, and promptly dispose of system bugs, computer viruses, network attacks and intrusions and other security risks; when any incident endangering cyber security occurs, network operators shall immediately initiate contingency plans, take corresponding remedial measures, and report the same to the relevant competent departments in accordance with the provisions.

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 Carrying out such activities as cyber security authentication, detection and risk evaluation, and releasing cyber security information like system bugs, computer viruses, network attacks and intrusions to society shall comply with the relevant regulations of the State.

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，不得为其提供技术支持、广告推广、支付结算等帮助。

Article 27 Any individual or organization shall neither engage in activities endangering cyber security, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data, nor provide programs or tools specifically used for activities endangering cyber security, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data; if such individual or organization knows that a person engages in activities jeopardizing cyber security, it shall not provide technical support, advertising promotion, payment and settlement services or other types of assistance to such person or organization.

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。

Article 28 Network operators shall provide technical support and assistance to the public security organs and state security organs in lawfully safeguarding national security and investigating crimes.

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。

Article 29 The State supports the cooperation among network operators in areas such as collection, analysis and reporting of cyber security information and emergency disposal, so as to improve the ability of network operators to safeguard the security.

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。

Relevant industrial organizations shall establish and perfect cyber security protection regulations and coordination mechanisms for their own industry, strengthen the analysis and evaluation of cyber security risks, regularly give risk warnings to their members, and support and assist members in handling cyber security risks.

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。

Article 30 The information acquired by cyberspace administration authorities and relevant departments in the course of their fulfillment of responsibilities for protecting cyber security shall be used exclusively for the need of cyber security protection but not for any other purpose.

第二节 关键信息基础设施的运行安全

Section 2. Security of operations of the Key Information Infrastructure

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。

Article 31 The State shall, based on the classified protection system for cyber security, be focused on protecting the important industries and fields such as public communications and information service, energy, transport, water conservancy, finance, public service and e-government, as well as other key information infrastructure that may seriously endanger the national security, national economy and people's livelihood and public interests if they are destroyed, have lost their functions or are subject to data leakage. The specific scope and measures for security protection for key information infrastructure shall be formulated by the State Council.

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 other than key information infrastructure to participate in the protective system of key information infrastructure on a voluntary basis.

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 The departments in charge of protecting key information infrastructure security shall, as per the division of duties stipulated by the State Council, respectively prepare and organize the implementation of key information infrastructure security plans for their own industry and field, guide and supervise the protection of operation security of key 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 To construct the key information infrastructure, it shall be ensured that the key information infrastructure has properties for supporting the stable and continuous operation of the business, and that technical security measures are planned, established and used concurrently.

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 Article 21 herein, key information infrastructure operators shall also fulfill the following obligations of security protection,

（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 special security management institutions and persons in charge of security management, and conduct security background review on the said persons and personnel on key positions;

（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；

(II) periodically conduct cyber security education, technical training and skill assessment for practitioners;

（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;

（四）制定网络安全事件应急预案，并定期进行演练；

(IV) formulate contingency plans for cyber security incidents, and regularly conduct drills; and

（五）法律、行政法规规定的其他义务。

(V) Other obligations stipulated by laws and 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 Where key information infrastructure operators purchase network products and services, which may influence national security, they shall go through a security review organized by the national cyberspace administration authority in concert with relevant departments under the State Council.

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 To purchase network products and services, key information infrastructure operators shall enter into security confidentiality agreements with the providers in accordance with the provisions, in which obligations and responsibilities in terms of security and confidentiality shall be clarified.

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评估；法律、行政法规另有规定的，依照其规定。

Article 37 Key information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administrative regulations have other provisions, those provisions shall prevail.

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 Key information infrastructure operators shall conduct by themselves, or entrust cyber security service institutions to conduct, the detection and assessment of their cyber security and any potential risk at least once a year; and submit the detection and assessment situations as well as improvement measures to the relevant departments responsible for the security protection of key 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 national cyberspace administration authority shall coordinate with relevant departments in an overall way to take the following measures with respect to the security protection of key 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 random detection on security risks related to key information infrastructure, and propose improvement measures; if necessary, may entrust cyber security service institutions to carry out the detection and evaluation of any potential security risks related to the network;

（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；

(II) periodically organize key information infrastructure operators to conduct emergency cyber security drills, and enhance the level and ability of coordination and cooperation to respond to cyber security incidents; and

（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；

(III) Promoting cyber security information sharing among relevant departments, key information infrastructure operators, relevant research institutions and cyber security service institutions; and

（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。

(IV) Provide technical support and assistance for emergency disposal of cyber security incidents and recovery of network functions.

第四章 网络信息安全

Chapter 4 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 strictly keep confidential the user information that they have collected, and establish and improve the system for user information protection.

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 To collect and use personal information, network operators shall follow the principles of legitimacy, rightfulness and necessity, make public the rules for collection and use, clearly express the purposes, methods and scope of collection and use of information, and obtain the consent of the persons whose data is gathered.

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 shall neither gather personal information unrelated to the services they provide, nor gather or use personal information in violation of the provisions of laws and administrative regulations or the agreements arrived at; and shall dispose of personal information they have saved in accordance with the provisions of laws and administrative regulations and agreements reached with users.

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 shall not divulge, tamper with or damage the personal information they have collected, and shall not provide personal information to others without the consent of the persons whose data is collected. However, the circumstance where the information has been processed and cannot be recovered and thus it is impossible to identify specific individuals is an exception.

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 take technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent such information from being divulged, damaged or lost. If personal information has been or may be divulged, damaged or lost, it is necessary to take remedial measures immediately, inform users in time according to the provisions and report to the relevant competent departments.

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 gather or use their personal information in violation of the provisions of laws and administrative regulations or the agreements arrived, they have the right to request the network operators to delete their personal information; where they find that their personal information gathered or stored by network operators has any error, they have the right to request the network operators to make corrections. Network operators shall take measures to delete or correct the said 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 Any individual or organization may neither acquire personal information by stealing or through other illegal ways, nor illegally sell or provide personal information to others.

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 The departments and their staff members responsible for the supervision and management over cyber security in accordance with the law shall strictly keep confidentiality of personal information, privacy and trade secrets known thereby in fulfilling their duties, and shall not divulge, sell or illegally provide the same to others.

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 individual or organization is responsible for his/its use of network, and shall neither establish any website or communication group for the purpose of committing fraud, teaching others about criminal methods, making or selling prohibited or controlled items, or carrying out other illegal and criminal activities, nor utilize the network to release information involving such illegal and criminal activities as committing fraud, making or selling prohibited or controlled items.

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 the management over the information published by their users, and upon discovery of the information whose publication or transmission is prohibited by the laws and administrative regulations, they shall immediately stop the transmission of such information, take disposal measures such as deletion to prevent the information from spreading, save relevant records, and report the same to the relevant competent departments.

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 The electronic information sent by and application software provided by any individual or organization shall neither be installed with malwares, nor contain any information whose publication or transmission is prohibited by laws and administrative regulations.

电子信息发送服务提供者和应用软件下载服务提供者，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 messaging service providers and application software download service providers shall fulfill security administration duties; and where the said providers learn that their users have committed the acts prescribed in the preceding paragraph, they shall stop the provision of services, take disposal measures such as deletion, keep relevant records and report the same to the relevant competent departments.

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。

Article 49 Network operators shall set up complaint and reporting systems for network information security, disclose the ways of complaint and reporting and other information, and promptly accept and handle complaints and reports related to network information security.

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。

Network operators shall cooperate with the supervision and inspection carried out by cyberspace administration authorities and relevant departments in accordance with the law.

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，采取消除等处置措施，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。

Article 50 The national cyberspace administration authority and relevant departments shall fulfill their obligations of supervising and managing cyber security information in accordance with the law, and upon discovery of any information whose publication or transmission is prohibited by the laws and administrative regulations, they shall request the network operators to stop the transmission, take disposal measures such as deletion, and keep relevant records; for the above information sourced from outside the territory of the People's Republic of China, they shall notify the relevant organizations to take technical measures and other necessary measures to block the transmission.

第五章 监测预警与应急处置

Chapter 5 Monitoring, Early Warning and Emergency Disposal

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 51 The State shall establish cyber security monitoring and early warning and information notification systems. The national cyberspace administration authority shall coordinate with the relevant departments to strengthen the work on collection, analysis and notification of cyber security information under an overall plan, and shall uniformly release cyber security monitoring and early warning information in accordance with regulations.

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。

Article 52 The departments responsible for protecting key information infrastructure security shall establish and perfect the cyber security monitoring and early warning and information notification system for their respective industry or field, and submit the cyber security monitoring and early warning and information notification in accordance with the relevant provisions.

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 national cyberspace administration authority shall coordinate with relevant departments to establish and perfect the cyber security risk assessment and emergency work mechanism, make contingency plans for cyber security incidents and organize drills periodically.

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。

The departments responsible for protecting key information infrastructure security shall formulate contingency plans for cyber security incidents for their respective industry or field, and periodically organize drills.

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。

In cyber security incident emergency plans, the cyber security incidents shall be graded based on such factors as the degree of harm and the scope of influence after the incidents occur, and the corresponding emergency disposal measures shall be prescribed.

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 probability of causing cyber security incidents increases, relevant departments of the people's governments at provincial level or above shall, in accordance with the authorization and procedures stipulated, take the following measures according to the characteristics of and possible harm from the cyber security 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 timely collect and report the relevant information, and strengthen the monitoring over cyber security risks;

（二）组织有关部门、机构和专业人员，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；

(II) organize relevant departments, institutions and professionals to analyze and assess cyber security risk information and predict the likelihood of occurrence of, scope of influence of and degree of harm from the incidents; or

（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。

(III) Release an early warning about cyber security risks to the public and take measures to avoid and mitigate harm therefrom.

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 For the occurrence of cyber security incidents, it is necessary to activate contingency plans for cyber security incidents immediately, investigate and assess such incidents, require network operators to take technical measures and other necessary measures to eliminate potential security hazards, prevent expansion of the harm, and promptly issue warning information in relation to the public to society.

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 Relevant departments of the people's governments at provincial level or above may have an interview with the legal representatives or principals of the network operators in accordance with prescribed authorities and procedures upon discovery of relatively high security risks or security incidents on the network. Network operators shall take measures to effect rectification and eliminate hidden dangers as required.

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 Emergency incidents or work safety accidents caused by cyber security incidents shall be handled in accordance with the Emergency Response Law of the People's Republic of China, the Work Safety Law of the People's Republic of China and other relevant laws and administrative regulations.

第五十八条   因维护国家安全和社会公共秩序，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 the case of demands to protect the national security and social public order, and respond to major social emergent security incidents, upon the decision or approval by the State Council, the competent departments may take restriction and other temporary measures on network communications within specific regions.

第六章 法律责任

Chapter 6 Legal Liabilities

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 fail to perform the obligation of protecting the cyber security as stipulated by Article 21 or Article 25 of this Law, shall be ordered to make rectification and be warned by relevant competent departments. Where they refuse to make rectification, or such consequences as endangering cyber security are caused, a fine of no less than CNY10,000 but no more than CNY100 ,000 shall be imposed; as for persons directly in charge, a fine of no less than CNY5,000 but no more than CNY50,000 shall be imposed.

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款，对直接负责的主管人员处一万元以上十万元以下罚款。

Where an operator of critical information infrastructure fails to fulfill obligation of cybersecurity protection set out in Articles 33, 34, 36 and 38 hereof, the competent authority shall warn such operator and order it to make rectifications. A fine ranging from 100,000 yuan to 1 million yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.

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：

Article 60 Where Paragraph 1 and Paragraph 2 of Article 22 and Paragraph 1 of Article 48 of this Law are violated by any of the following acts, the competent authority shall order it to make corrections and give it a warning. If it refuses to make corrections or causes consequences that endanger cybersecurity, it shall be fined not less than CNY50,000 but not more than CNY500,000, and the person directly in charge shall be fined not less than CNY10,000 but not more than CNY100 ,000:

（一）设置恶意程序的；

1. setting up malicious programs;

（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；

2. failing to take remedial measures immediately against such risks as security defects and bugs of their products and services, or failing to promptly inform users of such risks and report the same to the relevant competent departments in accordance with the relevant provisions; or

（三）擅自终止为其产品、服务提供安全维护的。

(III) arbitrarily terminating the provision of security maintenance for their products and services.

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 61 Network operators, who, in violation of the provisions of Paragraph 1, Article 24 hereof, fail to require users to provide real identity information, or provide services to users who fail to provide real identity information, shall be ordered by relevant competent departments to make rectifications. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or of severe circumstance, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be imposed by relevant competent departments. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.

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。

Article 62 Where a network operator, in violation of Article 26 hereof, carries out cybersecurity authentication, detection, risk assessment and other activities, or releases cybersecurity information such as system bug, computer virus, network attack and intrusion, the competent authority shall warn such operator and order it to make rectifications. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed in case of refusal to make rectifications or severe circumstance, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be imposed by the competent authority. A fine ranging from 5,000 yuan to 50,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.

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，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

Article 63 For persons who violate the provisions of Article 27 of this Law in engaging in activities which compromise cyber security, or providing procedures and tools for activities which compromise cyber security, or providing technical support, advertising and promotion, payment and settlement assistance etc for others to engage in activities which compromise cyber security but the case does not constitute a criminal offence, the public security authorities shall confiscate the illegal income, detain the offender for not more than five days, and may impose a fine ranging from RMB50,000 to RMB500,000; in relatively serious cases, the offender shall be subject to a detention of five to 15 days, and may be subject to a fine ranging from RMB100,000 to RMB1 million.

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。

Where an entity commits any of the violations stipulated in the preceding paragraph, public security organs shall confiscate its illegal gains, impose a fine of no less than CNY100 ,000 but no more than CNY1,000,000, and punish the persons directly in charge and the other directly responsible persons in accordance with the provisions of the preceding paragraph.

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。

Any person who violates Article 27 hereof and receives public security administrative punishment shall be prohibited from taking up key posts of cybersecurity and network operation for five years; and any such person who receives criminal punishment shall be prohibited from taking up key posts of cybersecurity and network operation for life.

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。

Article 64 Network operators or providers of network products or services who, in violation of the provisions of Paragraph 3 of Article 22 hereof and Articles 41 through 43 hereof, infringe upon the protection of personal information in accordance with the law, shall be ordered by relevant competent departments to make rectifications and may be subject to one or several of such penalties as a warning, confiscation of illegal earnings, imposition of a fine equivalent to more than one but less than ten times the illegal earnings or, if there is no illegal earnings, a fine of less than CNY1, 000, 000 and a fine of more than CNY10, 000 but less than CNY100, 000 on the supervisor directly in charge and other directly liable persons; in case of a serious violation, may also be ordered to suspend relevant business, stop doing business for internal rectification, close down the website, revoke the business license or revoke the business license.

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。

Where the operators violate Article 44 hereof by stealing, acquiring by other illegal means, or illegally selling or providing personal information to others but do not constitute a crime, public security organs shall confiscate the illegal gains, and impose a fine of no less than one but no more than ten times the illegal gains; if there is no illegal gain, a fine of no more than CNY1 million shall be imposed.

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。

Article 65 Where operators of key information infrastructures, in violation of Article 35 hereof, use network products or services that have neither been examined for security nor passed the security examination, they shall be ordered by relevant competent departments to stop using such products or services, and a fine of no less than one time but no more than ten times the purchase amount shall be imposed; as for persons directly in charge or other directly responsible persons, a fine of no less than CNY 10,000 but no more than CNY 100,000 shall be imposed.

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。

Article 66 Operators of key information infrastructure which violate the provisions of Article 37 of this Law in storing network data overseas or providing network data to overseas parties shall be ordered by the relevant authorities to make correction and be subject to a warning, illegal income shall be confiscated, and a fine ranging from RMB50,000 to RMB500,000 shall be imposed, and may be ordered to suspend the relevant businesses, suspend operation for correction, close down the website, revoke the relevant business permit or revoke the business licence; the directly accountable person (s) -in-charge and other directly accountable personnel shall be subject to a fine ranging from RMB10,000 to 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。

Article 67 Where Article 46 hereof is violated by establishing a website or a communication group for the purpose of committing criminal activities, or using a network to release information involving the commission of criminal activities, which does not constitute a crime, the public security organ shall detain the offender for not more than five days and may concurrently impose a fine of not less than CNY10,000 but not more than CNY100 ,000; if the circumstances are relatively serious, the public security organ shall detain the offender for not less than five days but not more than 15 days and may concurrently impose a fine of not less than CNY50,000 but not more than CNY500,000. Websites and communication groups used for conducting illegal and criminal activities shall be closed down.

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。

Organisations which commit the act in the preceding paragraph shall be subject to a fine ranging from RMB100,000 to RMB500,000 imposed by the public security authorities, and the person-in-charge directly accountable and other directly accountable personnel shall be punished pursuant to the provisions of the preceding paragraph.

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、采取消除等处置措施、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 68 Where a network operator, in violation of Article 47 hereof, fails to take such measures as ceasing transmission or elimination of such information prohibited by laws and administrative regulations, or keep relevant records, the competent authority shall warn such operator and order it to make rectifications, and confiscate its illegal gains. A fine of ranging from 100,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or of severe circumstance, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.

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 messaging service providers or application software download service providers who fail to fulfill their security management obligations stipulated in Paragraph 2 of Article 48 hereof, shall be punished in accordance with 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, in violation of the provisions hereof, have any of the following acts shall be ordered to correct by the competent departments; where they refuse to correct, or the circumstances are serious, a fine of not less than CNY50,000 but not more than CNY500,000 shall be imposed; as for the directly responsible supervisors and other directly responsible persons, a fine of not less than CNY10,000 but not more than CNY100 ,000 shall be imposed:

（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. Fail to take disposal measures such as stopping transmission or removing information whose publication or transmission is prohibited by the laws or administrative regulations as required by the relevant departments.

（二）拒绝、阻碍有关部门依法实施的监督检查的；

(II) refusing or impeding the supervision and inspection carried out by relevant departments according to the law; or

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

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

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 Releasing or transmitting the information whose publication or transmission is prohibited by Paragraph 2 of Article 12 hereof, or by other laws or administrative regulations, shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

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 Any violation as stipulated in this Law shall be recorded in the credit files in accordance with the provisions of the relevant laws and administrative regulations and be publicized.

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 Where operators of government affairs networks for state organs fail to perform their obligation of cyber security protection as stipulated in this Law, their administrations at the next higher level or relevant administrations shall order them to effect rectification and give sanctions to persons directly in charge and other directly responsible persons.

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 Where cyberspace administration and relevant departments, in violation of Article 30 hereof, use the information accessed in performing their duties of cyber security protection for any other purpose, sanctions shall be imposed on the persons directly in charge and other directly liable persons.

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。

Where the functionaries from the cyberspace administration and relevant departments neglect their duties, abuse their power, play favoritism and commit irregularities, but no crime is constituted, sanctions shall be imposed according to the law.

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。

Article 74 Persons who violate the provisions of this Law and cause others to suffer from damages shall bear civil liability pursuant to the law.

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。

For violations of the provisions of this Law which constitute a violation of public security administration, the offender shall be subject to public security administration punishment pursuant to the law; where the case constitutes a criminal offence, criminal liability shall be pursued in accordance with the law.

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。

Article 75 Where any overseas institution, organization or individual attacks, intrudes, disturbs, damages or otherwise jeopardizes critical information infrastructure of the People's Republic of China, causing serious consequences, it/he shall be investigated for legal liability according to the law; the public security authority and relevant departments under the State Council may decide to freeze properties of such institution, organization or individual or take any other necessary sanction measure.

第七章 附 则

Chapter 7 Supplementary Provisions

第七十六条   本法下列用语的含义：

Article 76 Terms used in this Law are defined as follows:

（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。

1. Network, refers to the system that is constituted by computers or other information terminals and related equipment to collect, save, transmit, exchange, and process information.

（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。

(II) Cyber security refers to through taking necessary measures to prevent attacks, intrusions, interference, sabotage on the network, illicit use of network, and accidents, to make sure the network is in stable and reliable operation conditions, and the capabilities for ensuring the integrity, confidentiality and availability of the 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。

(III) Network operators refer to owners, administrators of networks and network service providers.

（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。

(IV) Network data refers to all kinds of electronic data collected, saved, transmitted, processed and generated through the network.

（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。

(V) Personal information refers to all kinds of information recorded by electronic or otherwise that can be used to independently identify or be combined with other information to identify natural persons' personal information including but not limited to: natural persons' names, dates of birth, ID numbers, biologically identified personal information, addresses and telephone numbers, etc.

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 For the protection of the operation security of the network saving or processing information involving state secrets, provisions of laws and administrative regulations concerning confidentiality shall be complied with in addition to this Law.

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 The security protection of military networks shall be separately formulated by the Central Military Commission.

第七十九条   本法自2017年6月1日起施行。

Article 79 The Law shall come into force as of June 1, 2017.