中华人民共和国网络安全法

目　　录

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，鼓励网络技术创新和应用，建立健全网络安全保障体系，提高网络安全保护能力。

第四条 国家倡导诚实守信、健康文明的网络行为，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。

第五条 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。

第六条 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。国务院工业和信息化、公安部门和其他有关部门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。

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。

第七条 建设、运营网络或者通过网络提供服务，应当依照法律、法规的规定和国家标准、行业标准的强制性要求，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，防范违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第八条 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，指导会员依法加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第九条 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。

任何个人和组织使用网络应当遵守宪法和法律，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、宣扬恐怖主义和极端主义、宣扬民族仇恨和民族歧视、传播淫秽色情信息、侮辱诽谤他人、扰乱社会秩序、损害公共利益、侵害他人知识产权和其他合法权益等活动。

第十条 任何个人和组织都有权对危害网络安全的行为向网信、工业和信息化、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。

第二章 网络安全战略、规划与促进

第十一条 国家制定网络安全战略，明确保障网络安全的基本要求和主要目标，提出完善网络安全保障体系、提高网络安全保护能力、促进网络安全技术和产业发展、推进全社会共同参与维护网络安全的政策措施等。

第十二条 国务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门应当依据国家网络安全战略，编制关系国家安全、国计民生的重点行业、重要领域的网络安全规划，并组织实施。

第十三条 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。

国家支持企业参与网络安全国家标准、行业标准的制定，并鼓励企业制定严于国家标准、行业标准的企业标准。

第十四条 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、应用和推广，保护网络技术知识产权，支持科研机构、高等院校和企业参与国家网络安全技术创新项目。

第十五条 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。

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。

第十六条 国家支持企业和高等院校、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技术人才，促进网络安全技术人才交流。

第三章 网络运行安全

第一节 一般规定

第十七条 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、网络入侵等危害网络安全行为的技术措施；

（三）采取记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并按照规定留存网络日志；

（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。

网络安全等级保护的具体办法由国务院规定。

第十八条 网络产品、服务应当符合相关国家标准、行业标准。网络产品、服务的提供者不得设置恶意程序；其产品、服务具有收集用户信息功能的，应当向用户明示并取得同意；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当及时向用户告知并采取补救措施。

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间内，不得终止提供安全维护。

第十九条 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、行业标准的强制性要求，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。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服务，应当在与用户签订协议或者确认提供服务时，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。

国家支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证技术之间的互认、通用。

第二十一条 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、网络入侵、网络攻击等安全风险；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。

第二十二条 任何个人和组织不得从事入侵他人网络、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；不得提供从事入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的工具和制作方法；不得为他人实施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。

第二十三条 为国家安全和侦查犯罪的需要，侦查机关依照法律规定，可以要求网络运营者提供必要的支持与协助。

第二十四条 国家支持网络运营者之间开展网络安全信息收集、分析、通报和应急处置等方面的合作，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。

第二节　关键信息基础设施的运行安全

第二十五条　国家对提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或者管理的网络和系统（以下称关键信息基础设施），实行重点保护。关键信息基础设施安全保护办法由国务院制定。

第二十六条　国务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门（以下称负责关键信息基础设施安全保护工作的部门）按照国务院规定的职责，分别负责指导和监督关键信息基础设施运行安全保护工作。

第二十七条　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。

第二十八条　除本法第十七条的规定外，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：

（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；

（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；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期组织演练；

（五）法律、行政法规规定的其他义务。

第二十九条 关键信息基础设施的运营者采购网络产品和服务，应当与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十条 关键信息基础设施的运营者采购网络产品或者服务，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安全审查。具体办法由国务院规定。

第三十一条 关键信息基础设施的运营者应当在中华人民共和国境内存储在运营中收集和产生的公民个人信息等重要数据；因业务需要，确需在境外存储或者向境外的组织或者个人提供的，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从其规定。

第三十二条 关键信息基础设施的运营者应当自行或者委托专业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，并对检测评估情况及采取的改进措施提出网络安全报告，报送相关负责关键信息基础设施安全保护工作的部门。

第三十三条 国家网信部门应当统筹协调有关部门，建立协作机制。对关键信息基础设施的安全保护可以采取下列措施：

（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，必要时可以委托专业检验检测机构对网络存在的安全风险进行检测评估；

（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，提高关键信息基础设施应对网络安全事件的水平和协同配合能力；

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

（四）对网络安全事件的应急处置与恢复等，提供技术支持与协助。

第四章 网络信息安全

第三十四条 网络运营者应当建立健全用户信息保护制度，加强对用户个人信息、隐私和商业秘密的保护。

第三十五条 网络运营者收集、使用公民个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的公民个人信息，不得违反法律、行政法规的规定和双方的约定收

集、使用公民个人信息，并应当依照法律、行政法规的规定或者与用户的约定，处理其保存的公民个人信息。

网络运营者收集、使用公民个人信息，应当公开其收集、使用规则。

第三十六条 网络运营者对其收集的公民个人信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。

网络运营者应当采取技术措施和其他必要措施，确保公民个人信息安全，防止其收集的公民个人信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施，告知可能受到影响的用户，并按照规定向有关主管部门报告。

第三十七条 公民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。

第三十八条 任何个人和组织不得窃取或者以其他非法方式获取公民个人信息，不得出售或者非法向他人提供公民个人信息。

第三十九条 依法负有网络安全监督管理职责的部门，必须对在履行职责中知悉的公民个人信息、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。

第四十条 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。

第四十一条 电子信息发送者发送的电子信息，应用软件提供者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。

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，发现电子信息发送者、应用软件提供者有前款规定行为的，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。

第四十二条 网络运营者应当建立网络信息安全投诉、举报平台，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。

第四十三条 国家网信部门和有关部门依法履行网络安全监督管理职责，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信息传播。

第五章 监测预警与应急处置

第四十四条 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。

第四十五条 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。

第四十六条 国家网信部门协调有关部门建立健全网络安全应急工作机制，制定网络安全事件应急预案，并定期组织演练。

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。

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。

第四十七条 网络安全事件即将发生或者发生的可能性增大时，县级以上人民政府有关部门应当依照有关法律、行政法规和国务院规定的权限和程序，发布相应级别的预警信息，并根据即将发生的事件的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全事件发生、发展情况的监测；

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

（三）向社会发布与公众有关的预测信息和分析评估结果；

（四）按照规定向社会发布可能受到网络安全事件危害的警告，发布避免、减轻危害的措施。

第四十八条 发生网络安全事件，县级以上人民政府有关部门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。

第四十九条 因网络安全事件，发生突发事件或者安全生产事故的，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》等有关法律的规定处置。

第五十条 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，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施。

第六章 法律责任

第五十一条 网络运营者不履行本法第十七条、第二十一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。

关键信息基础设施的运营者不履行本法第二十七条至第二十九条、第三十二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。

第五十二条 网络产品、服务的提供者，电子信息发送者，应用软件提供者违反本法规定，有下列行为之一的，由有关主管部门责令改正，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）其产品、服务具有收集用户信息功能，未向用户明示并取得同意的；

（三）对其产品、服务存在的安全缺陷、漏洞等风险未及时向用户告知并采取补救措施的；

（四）擅自终止为其产品、服务提供安全维护的。

第五十三条 网络运营者违反本法规定，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、撤销相关业务许可或者吊销营业执照；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。

第五十四条 网络运营者违反本法规定，侵害公民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，处五十万元以下罚款；情节严重的，可以责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；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。

违反本法规定，窃取或者以其他方式非法获取、出售或者非法向他人提供公民个人信息，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，处五十万元以下罚款。

第五十五条 关键信息基础设施的运营者违反本法第三十条规定，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。

第五十六条 关键信息基础设施的运营者违反本法规定，在境外存储网络数据，或者未经安全评估向境外的组织或者个人提供网络数据的，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、撤销相关业务许可或者吊销营业执照；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。

第五十七条 网络运营者违反本法规定，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、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处二万元以上二十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，未履行本法规定的安全义务的，依照前款规定处罚。

第五十八条 发布或者传输法律、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。

第五十九条 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：

（一）未将网络安全风险、网络安全事件向有关主管部门报告的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不提供必要的支持与协助的。

第六十条 有本法第二十二条规定的危害网络安全的行为，尚不构成犯罪的，或者有其他违反本法规定的行为，构成违反治安管理行为的，依法给予治安管理处罚。

第六十一条 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。

第六十二条 依法负有网络安全监督管理职责的部门的工作人员，玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予行政处分。

第六十三条 违反本法规定，给他人造成损害的，依法承担民事责任。

第六十四条 违反本法规定，构成犯罪的，依法追究刑事责任。

第七章 附 则

第六十五条 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、处理的网络和系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、入侵、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，以及保障网络存储、传输、处理信息的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供

者，包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等。

（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。

（五）公民个人信息，是指以电子或者其他方式记录的公民的姓名、出生日期、身份证件号码、个人生物识别信息、职业、住址、电话号码等个人身份信息，以及其他能够单独或者与其他信息结合能够识别公民个人身份的各种信息。

第六十六条 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。

第六十七条 军事网络和信息安全保护办法，由中央军事委员会制定。

第六十八条 本法自 2017 年 06 月 01 日起施行。