H3C
新IT解决方案领导者

《中华人民共和国网络安全法》全文与解读

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

本法则自 2017 年 6 月 1 日起执行

> 企业战略要匹配国家战略，
> 新华三要扛起国家信息安全产业
> 自主可控的重任。

新华三集团

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

北京总部
北京市朝阳区广顺南大街 8 号院
利星行中心 1 号楼
邮编：100102
www.h3c.com

目录

《中华人民共和国网络安全法》全文

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。

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。

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。

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。

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。

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。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，府和社会的监督，承担社会责任。

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。

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。

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。

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。

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。

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。

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。

第二章 网络安全支持与促进

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。

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。

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。

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。

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。

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。

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。

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。

第三章 网络运行安全

第一节 一般规定

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，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。

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。

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。

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。

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。

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。

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。

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。

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：

（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，并定期进行演练；
（五）法律、行政法规规定的其他义务。

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。

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。

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。

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。

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：

（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；
（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；
（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；
（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。

第四章 网络信息安全

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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：

（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；

（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；

（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。

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。

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。

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。

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。

第六章 法律责任

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。

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。

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。

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。

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。

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。

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：

（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；
（二）拒绝、阻碍有关部门依法实施的监督检查的；
（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

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。

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。

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。

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。

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。

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。
（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。
（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）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。

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。

第七十八条

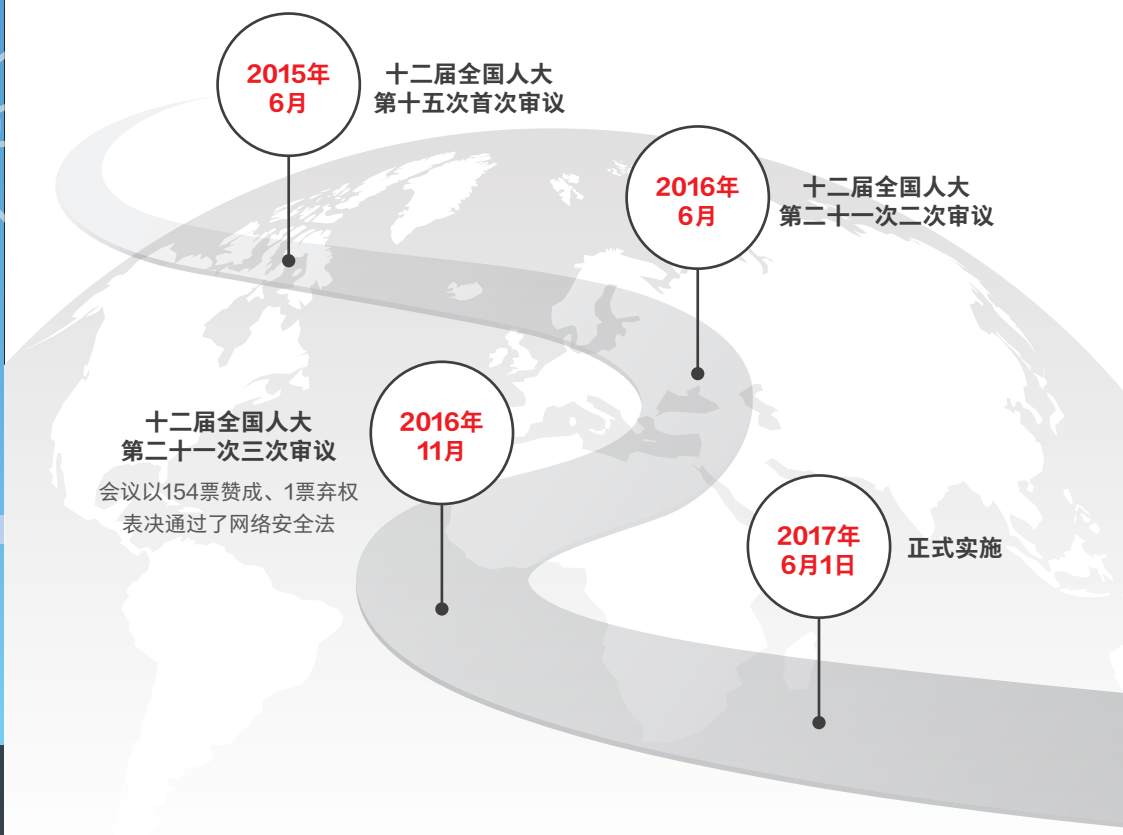
军事网络的安全保护，由中央军事委员会另行规定。

第七十九条

本法自 2017 年 6 月 1 日起施行。

《网络安全法》解读

《网络安全法》的出台



我国网络领域的基础性法律，

明确加强对个人信息保护，打击网络诈骗。

网络安全的关键控制节点

1. 网络安全等级保护
2. 关键信息基础设施安全保护
3. 网络安全监测预警和信息通报
4. 用户信息保护
5. 网络信息安全投诉举报等制度
6. 网络关键设备和网络安全专用产品认证
7. 关键信息基础设施运营者网络产品和服务采购的安全审查
8. 关键信息基础设施运营者信息/数据境内存储
9. 关键信息基础设施运营者信息/数据境外提供安全评估
10. 关键信息基础设施运营者年度风险检测评估
11. 网络可信身份管理
12. 建设运营网络或服务的网络安全保障
13. 网络安全事件应急预案/处置
14. 漏洞等网络安全信息发布
15. 网络信息内容管理
16. 网络安全人员背景审查和从业禁止
17. 网络安全教育和培训
18. 数据留存和协助执法等制度

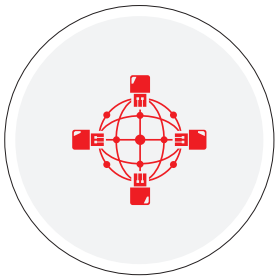
《网络安全法》概要

7 章 79 条

- 第一章 总则（十四条）
- 第二章 网络安全支持与促进（六条）
- 第三章 网络运行安全（十九条）
- 第四章 网络信息安全（十一条）
- 第五章 监测预警与应急处置（八条）
- 第六章 法律责任（十七条）
- 第七章 附则（四条）

- 明确了网络空间主权的原则
- 明确了网络产品和服务提供者的安全义务
- 明确了网络运营者的安全义务
- 进一步完善了个人信息保护规则
- 建立了关键信息基础设施安全保护制度
- 确立了关键信息基础设施重要数据跨境传输的规则

《网络安全法》的基本原则



网络空间主权原则

第1条 立法目的：明确规定要维护我国网络空间主权。

第2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。

网络安全与信息化发展并重原则

第3条 国家坚持网络安全与信息化发展并重，做到“双轮驱动、两翼齐飞”。

共同治理原则

第6条 采取措施鼓励全社会共同参与，政府部门、网络建设者、网络运营者、网络服务提供者、网络行业相关组织、高等院校、职业学校、社会公众等都应根据各自的角色参与网络安全治理工作。

《网络安全法》与等级保护

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：

1. 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；
2. 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；
3. 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；
4. 采取数据分类、重要数据备份和加密等措施；
5. 法律、行政法规规定的其他义务。

《网络安全法》与网络产品和服务提供者

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。
- 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。

2017年3月7日

关于Apache　Struts2存在S2-045远程代码执行漏洞的安全公告

2017年5月12日

新型“蠕虫”式勒索软件 “WannaCry”全面爆发

2017年6月1日

开始实施网络产品和服务安全审查办法（试行）

《网络安全法》与网络运营者

第9条

网络运营者开展经营和服务活动必须接受社会监督

第14条

任何个人和组织有权对危害网络安全的行为进行举报

第43条

发现个人信息被冒用有权要求网络运营者删除

第49条

网络运营者应当建立举报制度、公布举报方式、及时受理举报

《网络安全法》与网络诈骗

精准诈骗

- 不法分子
- XX高考网上报名信息系统
- 植入木马病毒
- 大量考生报名信息糟泄露
- 学生被骗学费近万元

01	02	03	04
焦点1	焦点2	焦点3	焦点4
第40条、第41条	第42条、第44条、第46条	第42条	第64条
如何规范个人信息收集行为? 保护用户权益并确立边界。	如何斩断信息买卖利益链? 未经同意提供、出售个人信息违法。	个人信息泄露如何补救? 运营者要告知并报告。	如何对网络诈骗溯源追责? 重罚甚至吊销执照。

《网络安全法》与个人信息保护

个人信息安全面临严峻挑战

- 信息泄漏事件频频发生
- 个人信息过度收集屡禁不止
- 个人信息非法买卖日益猖獗
- 个人信息滥用助长恶意违法行为

《网络安全法》重点解决个人信息保护的痛点问题

1、规范了相关网络安全监管部门的责权范围

中央网信办、国务院电信主管部门、公安部门等

2、明确了个人信息保护相关主体的法律责任

建立健全用户信息保护制度、对收集信息的安全保密原则、公民信息境内存放原则、泄露报告制度等

3、提高了个人对隐私信息的管控程度

通过引入了删除权和更正制度，进一步提高了个人对隐私信息的管控程度

4、增强了针对侵犯个人信息权益行为的威慑

罚款、停业整顿、关闭网站、撤销相关业务许可或吊销营业执照的处罚

傅莹 | 十二届全国人大新闻发言人

今年将开展网络安全法执法检查重点关注个人信息保护

中央网信办

正制定个人信息收集规范标准

《网络安全法》与关键信息基础设施

419网络安全和信息化工作座谈会

“树立正确的网络安全观，加快构建关键信息基础设施安全保障体系”

“全天候全方位感知网络安全生态，增强网络安全防御能力和威慑能力”

2016年7月8日

《全国范围关键信息基础设施网络安全检查工作启动》“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”（检查时间至12月底。）

基本制度

关键信息基础设施安全保护制度确立为国家网络空间基本制度保护办法由由国务院制定

设施范畴

网络安全法规定了原则性范围：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

责任追责

从国家、行业、运营者三个层面，分别规定了国家职能部门、行业主管部门及运营企业等各相关方的责任与义务，同时对境外的个人或者组织破坏关键信息基础设施提供法律依据

制度框架

关键信息基础设施运营者采购网络产品、服务的安全审查制度；加强国家的网络安全监测预警和应急制度建设，提高网络安全保障能力；尽快出台《国家关键信息基础设施安全保护条例》

新华三大安全

切合已经开始执行的《网络安全法》，以及根据中央网信办、公安部、工信部等相关的云计算安全指导文件及标准要求，新华三集团提供完整的安全产品、解决方案及安全专业服务，帮助客户满足国家有关监管部门的监督，满足合规性要求。

新华三大安全

新华三安全产品

新华三安全产品线专注于网络安全以及应用安全，为用户提供融合网络和应用的产品与解决方案。为保持在业界领先的产品技术和解决方案优势，新华三安全每年将销售额的15%以上作为研发投入。经过多年的持续投入，新华三已开发出自主知识产权高性能业务处理芯片与专用核心软件操作系统，申请200件以上的网络安全相关专利，同时与微软、卡巴斯基、CVE、Commtouch、ICSA等国际安全组织和知名厂商保持长期深度合作，确保安全产品持续的应用层防护能力。

目前，新华三安全产品覆盖网络层安全、应用层安全以及安全管理三个层面，包括防火墙、VPN、UTM、IPS、ACG、负载均衡、安全管理中心等近百余款产品，型号涵盖百兆、千兆、万兆和超万兆应用环境，具备了2～7层全业务安全防护能力，满足未来云计算、IPv6、Web2.0等新业务、新应用的时代需求。

安全管理

安全管理中心（SSM）

云安全监测中心

漏洞扫描

终端安全管理（EAD）

应用层安全

入侵防御系统

T1000/5000/9000系列

应用控制

ACG1000/2000/8000系列

负载均衡

L1000/5000/9000系列

Web防火墙

W1000/2000系列

网闸

堡垒机

网页防篡改

数据库审计

安全刀片

SecBladelite/III/IV

NFV虚拟化安全

VMSG虚拟化安全网关

M9000多业务网关

网络层安全

下一代防火墙/UTM/VPN系列

U200系列

F100系列

F1000系列

F10X0系列

F50X0系列

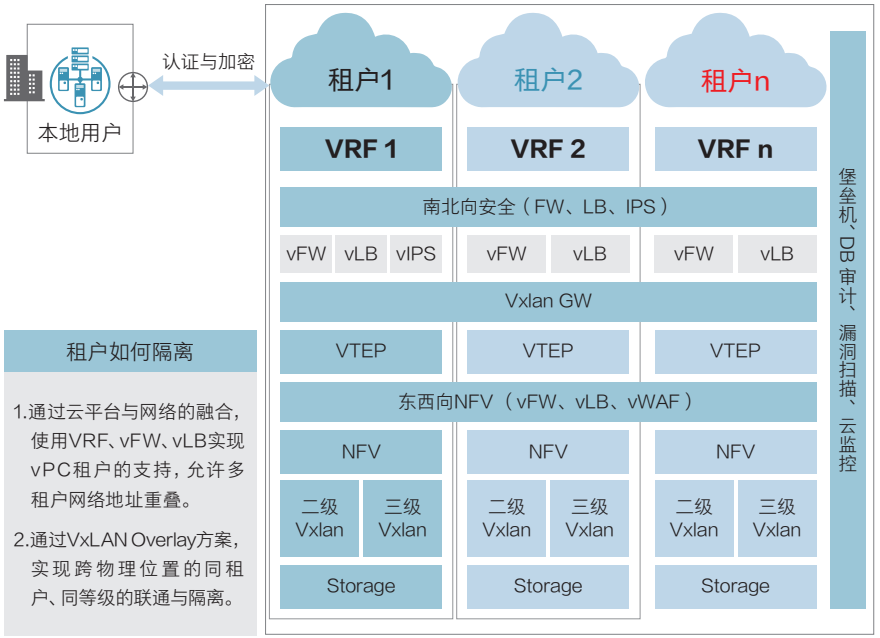
华三天机系统

新华三安全解决方案

通过全面普及云计算、虚拟化、SDN(软件定义网络)等技术，在带来高效、灵活、可靠的IT环境同时，基于路径的传统防护措施针对虚拟化环境的安全需求已经捉襟见肘，并且在全面融合SDN技术方面也存在技术缺陷。基于SDN和NFV的云安全防护体系能够满足环境多样化的需求，该体系在客户侧大规模部署建设是公认的技术发展方向，也是必经之路。为此，新华三推出云安全2.0解决方案。

云安全2.0解决方案架构

新华三云安全2.0解决方案是以整网的高速转发性能为基础，以平台防护为前提，满足基于等级保护的防护设计，同时以安全资源池化为手段，通过VPC技术实现多租户和多业务的南北向隔离，同时利用安全服务链技术和NFV技术满足不同安全区域的资源安全交互，实现云上业务丰富的服务目录，最终实现在新一代业务架构下的安全交付。



云安全2.0 整体架构

利用VPC的思路，有效利用VRF和Vxlan等技术，构建基于私有云IaaS类型的云化管理环境，在物理网络上构建虚拟的overlay网络层，通过新一代防火墙、IPS和负载均衡产品的SOP技术，实现网络的云化应用，为每个租户分配独立非共享的安全防护资源。

不同系统可能分布在不同的Vxlan或网段中，利用SDN控制器通过网络服务虚拟化技术，将承载层物理网络服务资源进行归一化的切片和抽象，建立虚拟网络服务节点。虚拟网络服务节点可以涵盖虚拟防火墙节点、虚拟LB节点、虚拟IPS节点等多种类型。一旦虚拟网络服务节点完成定义，SDN控制器会将这些虚拟资源和承载层网元自动映射，当不同应用的数据跨安全级别流动时，通过服务链技术对访问流量进行东西向的安全检测，最终将清洗后的流量注入到目标地址当中。

安全的按需交付

一旦多业务网络架构设计完毕，其他安全控制手段就可以分平台分区实现。控制包括集中式认证，IPS，网络准入，云安全监控，网络行为审计，漏洞和补丁管理。这些控制手段便于为每个区域进行性能优化和效率的调整。

云安全2.0解决方案特点

- 节省成本

有了云技术及及云安全2.0解决方案的协助，可以有效地提高运营能力而不需要花费更多的资金、人力成本，也不用添置服务器、网络及安全设备。由于在云环境中，计算、存储和安全都是按需提供的，不同业务部门只需要为自己使用的资源按需申请即可，不需要按传统方式前期购置大量的软硬件设备。

- 安全合规

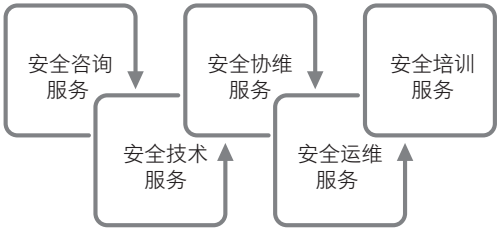
云安全2.0解决方案以云网融合为基础，能够实现无边界网络和云计算环境下的安全防护需求，充分满足国家监管部门对于虚拟化和云计算环境下的政策法规要求。

- 安全即服务

云安全2.0解决方案以软件定义安全为核心，结合安全服务链技术，将安全服务化，可以根据业务的安全策略需求，自定义安全访问路径，将传统的围防式安全变为塔防式安全，以适应云计算环境下的安全边界模糊、多租户安全策略冲突等问题。

新华三安全专业服务

结合多年专注信息安全、努力服务客户的经验，新华三推出五大类安全专业服务产品，几乎能够覆盖客户的所有服务需求，为客户提供信息系统全生命周期安全服务。



信息安全保障服务体系

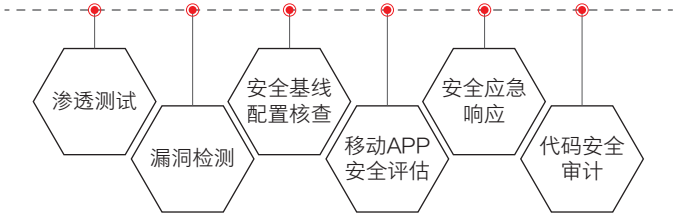
•安全咨询服务

基于对国家信息安全标准理解，对IT风险管理实践认识，新华三提出安全咨询服务，内容涉及等级保护合规咨询服务、信息安全风险评估服务、信息安全规划咨询服务（云安全合规咨询服务和云安全架构划设计服务），通过安全咨询服务，满足客户安全需求，为客户构建信息安全防护体系。

•安全技术服务

随着企业业务的快速发展以及应用系统的复杂性和多样性，系统漏洞层出不穷，病毒木马在网络中肆虐，黑客入侵和网站篡改等安全事件频繁发生。新华三经过技术积累和应用实践，对国内外安全技术进行详尽搜集、分析和研究，为客户应用系统提供全局、深度、颗粒化的安全技术服务。

安全技术服务包括：



•安全协维/运维服务

经过多年的信息化建设，大多数企业已建立了比较完整的信息系统。但是，在安全运维及应急响应方面缺少一套完整的运维和应急体系来保障各类紧急事件的处理。

新华三基于客户安全需求，提供5*8、7*24小时安全协维服务和安全运维服务，在服务过程中，重视事件管理流程和配置管理流程以及经验积累和共享，形成能持续完善、自我优化的安全运维体系和安全管理体系，提高客户信息系统的整体安全等级，为保证业务的健康发展和提升核心竞争力提供坚实的基础保障。

•安全培训服务

新华三注重知识库的积累和共享，为客户提供了丰富的安全培训内容，包括：安全产品培训、安全技术培训、安全管理培训、客户定制化培训，通过培训加强客户技术人员安全意识，强化岗位技能，提高技术水平。

新华三安全服务优势

新华三具备丰富的行业实战经验、全面的安全服务资质、强大的安全专业服务团队以及完善的服务交付流程，为客户提供基于行业最佳实践的安全专业服务，保障客户业务的持续运营。

•丰富的行业实战经验

新华三在安全领域拥有超过13年的服务案例积累，曾为北京奥运会、上海世博会、世界互联网大会、十八大、APEC峰会、杭州G20等重大活动提供安全保障，服务于百行百业，具备丰富的行业实战经验。

结合自身云计算、大数据和大互联的优势，提供最契合客户业务的服务体验。

•全面的安全服务资质

新华三是国内综合类网络安全厂商中唯一具备等级保护建设能力资质的企业；

新华三是国家信息安全漏洞库CNNVD最高级别支撑单位，同时是国家信息安全漏洞共享平台CNVD技术组单位。

新华三具备安全工程类一级、信息安全风险评估二级服务资质，ISO9001/TL9000质量体系证书，信息安全管理体系(ISO27001)和信息技术服务管理体系（ISO20000）等资质证书。

•强大的安全专业服务团队

新华三服务团队采用总部安全服务专家+驻外服务工程师的模式，拥有39个驻外服务机构，1000多人的区域服务工程师，拥有50余名总部安全服务专家，多人拥有CISP、CISSP、CISA、ISO20000、ISO27001、H3CIE、计算机信息系统集成项目经理、PMP认证等证书。