

《网络安全法》 (解读)

Cybersecurity Law



深信服官方微信



深信服移动官网

条文解读

责任要求

合规建议

深圳市南山区学苑大道1001号南山智园A1栋

咨询热线 400-806-6868 服务热线 400-630-6430

www.sangfor.com.cn

深信服 · 智安全

专注做实用的安全，

让每个组织的安全建设更有效、更简单！



01

概述

网络安全法是我国第一部网络安全领域的法律，是保障网络安全的基本法，与《国家安全法》、《反恐怖主义法》、《刑法》、《保密法》、《治安管理处罚法》、《计算机信息系统安全保护条例》等现行法律法规共同构成中国关于网络安全管理的法律体系。

责任导读

主管单位	审计监管	第八条：明确网络安全的监管责任
	安全教育	第十九条：开展网络安全宣传教育 第三十条：规范职能，防止权力滥用
	职业保密	第四十五条：执法部门的职业保密要求 第五十条：网络信息安全监管职责
	监测预警通报	第五十二条：建立行业层面的网络安全监测预警和信息通报制度
	应急响应与处置	第五十一条、第五十三条、第五十四条、第五十五条、第五十八条：网络安全事件应急响应与处置

网络运营者层面	制度及责任人	第九条、第二十一条、第二十四条、第二十五条、第二十八条、第四十二条、第四十七条、第五十六条：网络运营者承担的义务
	防病毒和网络入侵	
	网络监测与日志存储	第四十条：用户信息保护
	数据分类、备份与加密	第四十一条：个人信息的收集与保护 第四十条：“删除权”
	网络应急预案	第四十四条：严禁“非法出售” 第四十九条：投诉举报

关键基础设施运营者

- **安全建设** 第三十一条：关键基础设施相关定义
- **安全保护** 第三十二条：安全保护工作
- **安全审查** 第三十三条：建设工作
- **安全审查** 第三十四条：关键信息基础设施运营者的义务
- **保密要求** 第三十五条：相关安全产品的采购
- **境内存储** 第三十六条：采购保密协议
- **检测评估** 第三十七条：重要数据境外输出的安全评估
- **检测评估** 第三十九条：风险评估和信息共享

国家层面

- 第一条：立法目的
- 第五条：国家采取手段处理网络安全风险
- 第六条：构建网络安全良好环境
- 第七条：开展网络空间治理
- 第十三条：未成年人在网络环境中的保护
- 第十五条：促进网络安全人才培养
- 第二十条：促进网络安全人才培养
- 第五十一条：建立网络安全监测预警和信息通报制度

网络产品和服务提供者

- **符合国家标准强制性要求** 第十条：对产品和服务在数据安全方面的要求
- **及时告知漏洞等风险** 第十六条：国家鼓励加大投入、重点扶持、保护知识产权、支持创新项目
- **不得擅自终止维护服务** 第十七条：关于网络安全的认证、检测和风险评估工作
- **专用产品经过检测和认证** 第十八条：开发数据安全保护技术，促进公共数据资源开放
- **专用产品签署保密协议** 第二十二条；第二十七条：网络产品和服务提供者的义务
- **专用产品签署保密协议** 第二十三条：网络安全产品的检测与认证
- **专用产品签署保密协议** 第三十五条：关键信息基础设施运营者的产品和服务的采购
- **专用产品签署保密协议** 第三十六条：保密协议
- **专用产品签署保密协议** 第三十八条：检测评估工作
- **专用产品签署保密协议** 第四十八条：电子信息、软件下载的数据安全

其他

- 第十一条：相关行业组织规范
- 第十二条：个人和组织网络行为规范
- 第十四条：举报维权
- 第二十六条：网络安全认证、检测和风险评估须遵守国家规定
- 第二十九条：情报交换与风险评估

02

条文解读

目录 | CONTENTS

第一章 总则	02
第二章 网络安全支持与促进	06
第三章 网络运行安全	08
• 一般规定	08
• 关键信息基础设施的运行安全	12
第四章 网络信息安全	15
第五章 监测预警与应急处置	18
第六章 法律责任	21
第七章 附则	27

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。

解读：本条指明网络安全法的制定目的。

第二条 在中华人民共和国境内建设、运营、维护和和使用网络，以及网络安全的监督管理，适用本法。

解读：本条指明了网络法的适用范围。

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。

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。

解读：未来国家可能会出台网络安全战略，网络安全上升到国家战略层面。

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。

解读：全民普及并提升安全意识。企业和组织管理好网络并规范好上网行为，净化网络；个人依法上网，加强自我防范意识。

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。

解读：表明国家在网络安全领域开放合作的立场。本条款说明将来国家会有配套的制度、标准出台。

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。

解读：这一条明确了网络安全的监管责任。目前在国家层面主要是中央网信办网络安全协调局负责统筹协调，工信部网络安全管理局负责网络安全相关管理工作，公安部网络安全保障局负责安全保障工作。

第九条 网络运营者开展经营活动和服务活动，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。

解读：表明了网络运营者要承担的一般性义务。

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。

解读：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、保密性和可用性都是网络运营者要做的工作。

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。

解读：明确了行业组织的责任义务。

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。

解读：点明了哪些事情不可为。即时通讯、搜索、网络社区等存在较多言论行为的网络服务注意信息审计，净化网络环境。

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。

解读：本条文明确了在未成年人保护方面的要求。教育行业重点关注，规范青少年上网行为，营造安全、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。

解读：在遇到网络安全危害行为等有举报维权的权利和权益。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。

解读：国家在网络安全标准制定方面的总体规定。企业、研究机构、高校、网络相关行业可参与国家标准和行业标准的制定。

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 and 高等学校等参与国家网络安全技术创新项目。

解读：加大国家课题研究、创新项目等方式的投入，企业和高校等可积极参与。

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向社会进行网络安全宣传教育。

解读：政府及相关部门应积极组织开展网络安全宣传教育活动。

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。

解读：高校等开展网络安全教育培训活动，培养网络安全人才。

第三章 网络运行安全

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。

解读：1· 国家实行网络安全等级保护制度，不做等保相当于不合法。
2· 网络安全法要求明确责任人，出现安全事故，直接负责人需要承担责任并且接受法律处罚。
3· 网络中应有防范病毒入侵、网络攻击的能力。
4· 网络日志不仅仅是要保存，而且需要存储不少于6个月。
5· 做好数据的分类、备份和加密。

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。

解读：本条指明了网络产品、服务提供者的义务和责任，企业可对网络厂商提出合法要求。

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。

解读：目前网信办已经公布了一部分网络关键设备和网络安全专用产品目录，在目录内的产品，都需要经过专门的认证和或者检测方可销售或提供。

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。

解读：本条的核心是实名认证。这也是网络运营者的需要承担的义务。

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。

解读：本条的核心是应急响应。这是网络运营者要承担的义务。

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。

解读：对外发布网络安全信息应谨慎，严格遵守相关规定。

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。

解读：应配合公安机关进行网络安全事件调查等相关工作，做好审计工作，用于事后调查取证。

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。

解读：国家支持网络运营者之间进行信息收集、分析、通报。同时做好网络监测和应急响应机制，来提升威胁发现能力和响应处置能力。

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。

解读：规范了执法者的行为，防范执法机关权力滥用。

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。

解读：定义了什么是关键基础设施。

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。

解读：会有专门负责关键设施安全保护工作的部门。

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。

解读：建设关键信息基础设施应满足三同步：同步规划、同步建设、同步使用，并保证业务稳定性。

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。

解读：本条文从制度、培训、灾备、应急等方面对关键基础设施运营者提出了进一步要求。

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。

解读：本条的关键词是“采购”“保密协议”。

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。

解读：个人信息和重要信息需境内存储。外企和有海外业务的国内企业应重点关注。

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。

解读：每年至少一次的网络安全检测和风险评估。

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。

解读：有关部门会对关键信息基础设施的安全风险进行抽查检测，因此，关键信息基础设施运营者一定要做好网络安全相关工作。

第四章 网络信息安全

第四十条 网络运营者应当建立健全用户信息保护制度，对其收集的用户信息必须严格保密。

解读：进行用户信息保护。用户信息主要是指：用户使用产品或服务过程中收集的信息构成用户信息，包括IP地址、用户名和密码、上网时间、Cookie信息等。

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。

解读：进行个人信息保护。个人信息指：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。

解读：网络运营者应做好信息防泄露、防篡改等工作，未经同意，不得向他人提供个人信息。

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。

解读：本条主要讲了公民个人信息的删除权和更正权制度。

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。

解读：本条主要是个人信息保护，非法获取、非法出售、非法提供个人信息均

不可为。

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。

解读：对执法部门和人员的职业保密提出了要求。

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。

解读：主要讲了网络犯罪。任何个人和组织不得进行网络诈骗等违法犯罪活动。

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。

解读：内容审查是网络运营者需要承担的义务。

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。

解读：对软件开发商、电子信息发送服务提供者、应用下载服务提供者提出了要求。

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。

解读：本条的重点是举报制度，是网络运营者的义务，也是公众举报投诉的权利。

第五章 监测预警与应急处置

解读：本章节用了整个章节来描述监测预警和应急处置，可见其重要性。

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。

解读：本条的重点在于“约谈”，建议网络运营者要承担相关责任义务，做好网络安全工作。

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；情节严重的，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。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；情节严重的，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。电子信息发送服务提供者、应用程序下载服务提供者，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，处五十万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、删除等处置措施的；
- （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，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。

03

网络建设合法合规建议

网络运营者

- 建立安全责任制度，明确责任人。
- 制度及责任人** 开展等级保护工作，落实网络安全等级保护制度。
- 防病毒和网络入侵** 通过防火墙等网络安全防护设备防范病毒入侵，保障网络安全、稳定运行。
- 网络监测与日志存储** 建立审核监控制度，如通过审计产品或态势感知等有效监控网络系统，及时发现漏洞和信息泄露等风险。
- 数据分类、备份与加密** 通过建设日志存储中心来满足日志存储六个月的要求。
可用VPN做数据加密跟隔离，做好个人信息保护；同时也可用SSL 进行身份认证，落实网络实名制制度。
- 网络应急预案** 使用具备持续检测与快速响应能力的安全产品，实现网络安全事件应急响应。
- 个人信息保护** 建议使用具备可视化能力产品，便于建立报告制度，及时报告系统漏洞、信息泄露等风险事件。

关键信息基础设施运营者

- 关键基础设施运营者进行网络建设同样需承担网络运营者的全部责任，可参考网络运营者建设方法。
- 规划、建设、使用三同步** 安全技术措施同步规划、同步建设、同步使用，确保业务运行做好可靠，建议加强病毒防御的同时做好冗余负载。
- 安全保护** 做好系统和数据的容灾备份，如采用云备份。
- 安全审查** 设立专岗，责任明确，定期进行网络安全教育培训与考核。
- 保密要求** 定期进行网络应急响应演练，建议参考其他同行业演练方案。
- 境内存储** 境内设置数据存储中心，所有重要数据均在境内存储。
采购安全产品时关注网络服务提供商提供产品是否符合法规，并签署保密协议。
- 检测评估** 每年定期进行安全检测评估，建议与等保工作一起开展，确保合规。
使用具备持续检测与快速响应能力的安全产品，实现网络安全事件应急响应。
建议使用具备可视化能力产品，便于建立报告制度，及时报告系统漏洞、信息泄露等风险事件。