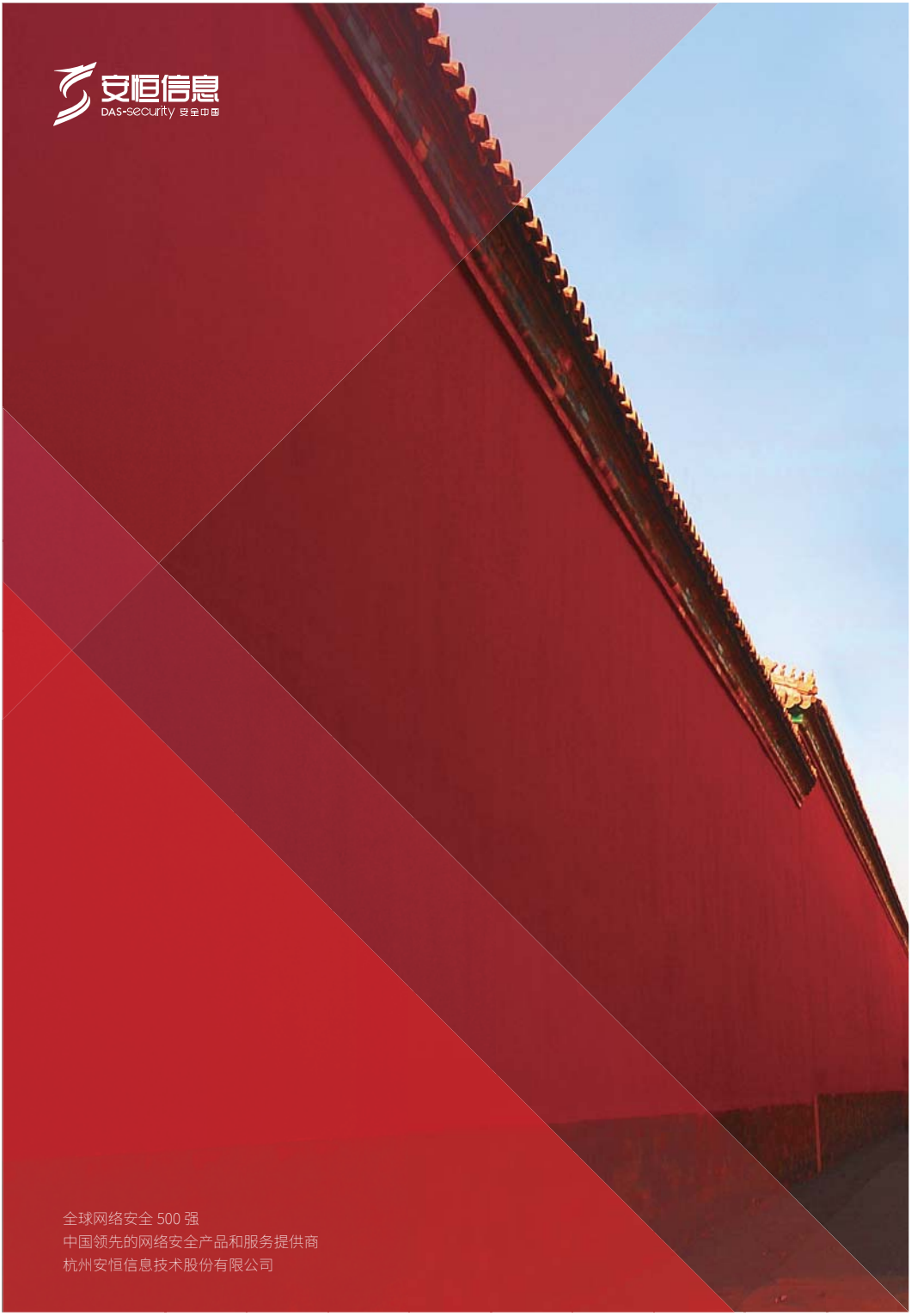
中华人民共和国网络安全法读本

杭州安恒信息技术股份有限公司
WWW.DBAPPSECURITY.COM.CN



安恒信息
DAS-security 安全中国

全球网络安全 500 强
中国领先的网络安全产品和服务提供商
杭州安恒信息技术股份有限公司

目 录
CONTENTS

第一部分 《中华人民共和国网络安全法》

中华人民共和国主席令

第五十三号

《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。

中华人民共和国主席 习近平

2016年11月7日

中华人民共和国网络安全法

PEOPLE'S REPUBLIC OF CHINA NETWORK SECURITY LAW

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，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。

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。

玄武盾

安全态势感知与云防护一体化平台

点面可控，坚实防护，私有云专属安全管家

云平台安全解决方案：提供云平台安全能力，保障租户系统的安全性与高可用性。
弹性集群架构：提供集群冗余部署方式，灵活调整防护平台引擎与性能。
平台集中管理：管理员集中管控防护平台，各租户自定义防御体系。

《网站安全云防护平台技术要求》起草单位，G20峰会官网防护产品！

安恒助力安全中国

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

AiLPHA大数据智能安全平台

智能 | 态势 | 融合 | 大数据分析

有效提升事件调查效率**300%↑** 降低告警误报率**600%↓**

One Solution to Rule Them ALL

安恒助力安全中国

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。

第二部分　网络安全法解读

1、网络安全法概要

章　节	条目数	概要说明
第一章总则	14 条规定	简述法律目的、范围、总则、部门职责，总体要求等
第二章网络安全支持与促进	6 条规定	政府在推动网络安全工作上的职责定义国家直属部门
第三章网络运行安全	19 条规定	定义网络运营者与关键信息基础设施的 运行安全规定
第一节一般规定 第二节关键信息基础设施的运行安全	10 条规定 9 条规定	针对网络运营者的网络运行安全要求与 职责规定 针对关键信息基础设施的安全规定与保 护措施要求
第四章网络信息安全	11 条规定	定义个人信息保护的保护规定
第五章监测预警与应急处置	8 条规定	定义国家网络安全监测预警与汇报机制
第六章法律责任	17 条规定	定义处罚规定
第七章附则	4 条规定	相关名词释义与其他附则

2、所涉及的关键相关方和职责

1 **国家：**完善国家网络安全战略和方针、鼓励网络 安全技术创新和应用，支持培养网络安全 人才，建立保障体系，提高保护能力 推进国际交流合作。

2 **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。

3 **行业组织：**健全行业的网络安全保护规范和机制，加强 对网络风险的分析评估，定期进行风险警示， 协助应对安全风险 加强行业自律，促进行业健康发展。

4 **电信主管部门：**职责范围内负责网络安全保护和 监督管理工作。

5 **网络运营者：**接受政府和社会监督，承担社会责任按照等保要求，履行安全保护义务，防止网络 数据泄露或者被窃取、篡改，维护网络数据的完整性、保密性和可用性提供对犯罪活动调查的技术支持和协助。

6 **标准化行政主管部门：**负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。

7 **公安部门：**各自职责范围内负责网络安全保护和监督管理工作处罚权。

技术+金融完美结合，守护您网络信息的安全

网络信息安全综合保险

赔付不是重点，风控才是关键

金融赔付实现风险转移

数据丢失赔偿、数据泄露赔偿
营业中断赔偿、法律费用赔偿
危机公关费用赔偿、第三方责任赔偿
网络勒索赔偿

评估、加固、监测、预警
防护、应急、处置、恢复、取证

安全服务、保驾护航

安恒助力安全中国

3、网络安全八大要点

❶ 要点一：网络安全等级保护制度

根据《网络安全法》第二十一条规定，国家实行网络安全等级保护制度。网络运营者承担的实施网络安全等级保护制度相关的安全保护义务包括：

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。

❷ 要点二、关键信息基础设施

《网络安全法》第三十一条对关键信息基础设施进行了规定，法律公布后，社会的关注热点是如何准确地理解关键信息基础设施的范围。

按照《国家网络安全检查操作指南》的规定，“关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括网站类，如党政机关网站、企事业单位网站、新闻网站等；平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等”。从以上定义可以看出，《国家网络安全检查操作指南》下关键信息基础设施的范围是比较广泛的，比如即时通信系统和电商平台都有可能成为关键信息基础设施，其对我们理解《网络安全法》下关键信息

基础设施的范围具有一定的借鉴意义。

一旦被认定为关键信息基础设施，设施运营者将会承担相应的网络安全保护法定义务，包括：

1）关键信息基础设施的建设要求（第三十三条）；
2）关键信息基础设施运营者的安全保护义务（第三十四条）；
3）采购关键信息基础设施产品和服务的国家安全审查要求（第三十五条）；
4）采购关键信息基础设施产品和服务的保密要求（第三十六条）；
5）个人信息和重要数据的本地化要求（第三十七条）；
6）关键信息基础设施的网络安全年度检测评估（第三十八条）。

3 要点三：数据保护

《网络安全法》对于数据的保护包括个人信息保护、用户信息保护和商业秘密保护。

《网络安全法》引入了“用户信息”的概念，第二十二条规定，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；并在第四十条中要求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。“用户信息”，就是在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、用户身份、上网时间、Cookie 信息等。如果用户信息具备身份识别的功能或，则构成用户的个人信息。可见，用户信息的范围相比个人信息更广泛一些。

《网络安全法》建立了关于关键信息基础设施产品和服务采购的国家安全审查制度（第三十五条）、数据跨境传输的安全评估制度（第三十七条）等，这些制度的实施，都需要网络运营者和其它主体向有权机关提交相应的审查内容，其中可能包括受知识产权保护的软件代码、加密算法、商业计划和商业秘密等。

4 要点四：数据本地化

依照《网络安全法》第三十七条规定，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。数据本地化要求包括个人信息和重要数据。

对数据本地化的法律规制，除了《网络安全法》的规定，以下的数据（或设施）亦明确有本地化的法律要求。

天池

天池云安全管理平台

针对云安全的一站式专业解决方案

聚能天池 共护云端

弹性的云安全资源

云安全资源按需分配
自动化部署
弹性扩容

统一的云安全管理平台

云安全能力统一认证
自助选购
统一运维

完善的云安全能力

一键按需获取综合漏洞扫描
云WEB应用防火墙
网页防篡改、下一代云防火墙
IPS、IDS、防病毒、EDR
云数据库审计、云堡垒机
云综合日志审计
大数据分析、玄武盾
态势感知等安全能力

丰富的云安全套餐服务

提供符合用户各个应用场景的云安全解决方案,一键满足业务安全需求

安恒助力安全中国

5 要点五：网络实名制

再一次确立了网络实名制在中国的实施，第二十四条规定，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。

6 要点六：网络运营者的企业制度建设要求

《网络安全法》对网络运营者设定了一系列的法定义务，有些义务需要网络运营者建立企业的管理制度和操作规程，以满足法律合规性的要求，避免法律风险，主要包括如下：

（1）与实施网络安全等级保护制度相关的义务和制度建设，包括制定内部安全管理制度和操作规程，确定网络安全负责人等（第二十一条）；

（2）健全用户信息保护制度（第二十二条和第四十条）；

（3）落实网络实名制（第二十四条）；

（4）网络安全事件应急预案（第二十五条）；

（5）关键信息基础设施的安全保护义务，包括：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；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务（第三十四条）；

（6）采购关键信息基础设施产品和服务的保密制度（第三十六条）；

（7）关键信息基础设施安全性的年度评估（第三十六条）；

（8）个人信息的收集和利用规则及制度（第四十一条和第四十二条）；

（9）个人信息泄露事件的报告制度（第四十二条）；

（10）违法使用个人信息删除和错误个人信息更正制度（第四十三条）；

（11）网络运营者对用户非法信息传播的监管（第四十七条）；

（12）网络信息安全投诉、举报制度（第四十九条）。

7 要点七：法律责任

《网络安全法》第六章规定了详尽的法律责任。对网络运营者，根据违法行为的情形，主要的法律责任承担形式包括责令改正、警告、罚款，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

天鉴态势感知

关键信息基础设施安全防护管理平台

态然自若 / 势事洞明 / 感知威胁 / 知己知彼

从感知、研判、通报、追踪到溯源，安全态势监管全生命周期数据*0*丢失

- 智能大数据分析
- 贴合监管场景
- 威胁感知可视化
- 监管业务可量化

安恒助力安全中国

人员等进行罚款等；并且，有关机关还可以把违法行为记录到信用档案。对于违反法律第二十七条的人员，法律还建立了职业禁入的制度。

除了以上的行政处罚外，网络运营者还应当关注违法行为所导致的民事责任和刑事责任。网络运营者如果因违法《网络安全法》的行为给他人造成损失的，该行为具有民事上的可诉性，网络运营者应当承担相应的民事责任。《刑法修正案（九）》规定的拒不履行信息网络安全管理义务罪，指网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，具有法律规定的情形之一的，构成本罪。《网络安全法》为网络运营者设定了诸多的网络安全保护义务（比如网络安全等级保护和关键信息基础设施保护等），如果由于不履行法律的规定而导致严重后果的，可能会受到刑事的追诉，从而承担拒不履行信息网络安全管理义务罪的后果。

8 要点八：将监测预警与应急处置措施制度化、法制化

《网络安全法》第五章将监测预警与应急处置工作制度化、法制化，明确国家建立网络安全监测预警和信息通报制度，建立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演练。这为建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制提供了法律依据，为深化网络安全防护体系，实现全天候全方位感知网络安全态势提供了法律保障。

关于安恒

杭州安恒信息技术股份有限公司，是2007 年5 月由“国家千人计划”特聘专家范渊先生创办的国家级高新技术企业，中国领先的网络安全产品和服务提供商。国内总部设在杭州，并在北京、上海、南京、广州、深圳、成都、重庆、济南、西安等三十多个城市设有分支机构，服务客户包括政府、公安、企业、教育、金融、运营商、媒体、医疗、能源等多个行业。目前已是享誉国内外的网络安全品牌，于2015 年成功跻身“全球网络安全500 强中国区榜首”。

安恒信息始终秉承“安恒助力安全中国”的使命，截至2018年7 月，公司已有员工1300 余人，其中研发团队人数超过65%，，拥有数百位国际一线的核心安全专家和自主知识产权的明鉴、天鉴、明御、风暴中心等知名品牌，以及大数据态势感知、玄武盾、安全数据大脑、天池云安全管理平台、AiLPHA 大数据智能分析平台等创新产品，并在涉众经济犯罪、金融风险监控等新型网络空间安全领域不断创新。

自2008 年参与奥运会网站安全保障服务开始，安恒信息就和国家级重大活动的安全保障服务结下了不解之缘，建国60 周年全国网站安全大检查、上海世博会、广州亚运会、深圳大运会、中国共产党第十八次全国代表大会、公安部全国网站安全大检查、历届世界互联网大会、抗战胜利70 周年、G20 杭州峰会、厦门金砖峰会、中国共产党第十九次全国代表大会、“一带一路高峰论坛”、上合组织青岛峰会等重大活动都由安恒信息参与安全保障并在其中多个活动中承担了核心的中坚力量。

安恒信息将坚持践行安恒文化，坚守“成就客户、责任至上、开放创新、以人为本、共同成长”核心价值观，力争成为中国网络安全行业第一品牌，实现与国家网络安全息息相关的中国梦。

安恒信息
DAS-Security 安全中家

杭州安恒信息技术股份有限公司 | DBAPPSecurity Co.,Ltd.

安恒官网：www.dbappsecurity.com.cn
E-mail：info@dbappsecurity.com.cn
客服热线：400-6059-110
地址：杭州市滨江区通和路68号中财大厦15楼（310051）
座机：0571-28860999　28895668
传真：0571-28863666

安恒官方微信

E安全