网络安全等级保护条例

（征求意见稿）

目　录

第一章　总　则

第一条【立法宗旨与依据】为加强网络安全等级保护工作，提高网络安全防范能力和水平，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，依据《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》等法律，制定本条例。

第二条【适用范围】在中华人民共和国境内建设、运营、维护、使用网络，开展网络安全等级保护工作以及监督管理，适用本条例。个人及家庭自建自用的网络除外。

第三条【确立制度】国家实行网络安全等级保护制度，对网络实施分等级保护、分等级监管。

前款所称“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。

第四条【工作原则】网络安全等级保护工作应当按照突出重点、主动防御、综合防控的原则，建立健全网络安全防护体系，重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。

网络运营者在网络建设过程中，应当同步规划、同步建设、同步运行网络安全保护、保密和密码保护措施。

涉密网络应当依据国家保密规定和标准，结合系统实际进行保密防护和保密监管。

第五条【职责分工】中央网络安全和信息化领导机构统一领导网络安全等级保护工作。国家网信部门负责网络安全等级保护工作的统筹协调。

国务院公安部门主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。

国家保密行政管理部门主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理。

国家密码管理部门负责网络安全等级保护工作中有关密码管理工作的监督管理。

国务院其他有关部门依照有关法律法规的规定，在各自职责范围内开展网络安全等级保护相关工作。

县级以上地方人民政府依照本条例和有关法律法规规定，开展网络安全等级保护工作。

第六条【网络运营者责任义务】网络运营者应当依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。

第七条【行业要求】行业主管部门应当组织、指导本行业、本领域落实网络安全等级保护制度。

第二章　支持与保障

第八条【总体保障】国家建立健全网络安全等级保护制度的组织领导体系、技术支持体系和保障体系。

各级人民政府和行业主管部门应当将网络安全等级保护制度实施纳入信息化工作总体规划，统筹推进。

第九条【标准制定】国家建立完善网络安全等级保护标准体系。国务院标准化行政主管部门和国务院公安部门、国家保密行政管理部门、国家密码管理部门根据各自职责，组织制定网络安全等级保护的国家标准、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等级保护国家标准、行业标准的制定。

第十条【投入和保障】各级人民政府鼓励扶持网络安全等级保护重点工程和项目，支持网络安全等级保护技术的研究开发和应用，推广安全可信的网络产品和服务。

第十一条【技术支持】国家建设网络安全等级保护专家队伍和等级测评、安全建设、应急处置等技术支持体系，为网络安全等级保护制度提供支撑。

第十二条【绩效考核】行业主管部门、各级人民政府应当将网络安全等级保护工作纳入绩效考核评价、社会治安综合治理考核等。

第十三条【宣传教育培训】各级人民政府及其有关部门应当加强网络安全等级保护制度的宣传教育，提升社会公众的网

络安全防范意识。

国家鼓励和支持企事业单位、高等院校、研究机构等开展网络安全等级保护制度的教育与培训，加强网络安全等级保护管理和技术人才培养。

第十四条【鼓励创新】国家鼓励利用新技术、新应用开展网络安全等级保护管理和技术防护，采取主动防御、可信计算、人工智能等技术，创新网络安全技术保护措施，提升网络安全防范能力和水平。

国家对网络新技术、新应用的推广，组织开展网络安全风险评估，防范网络新技术、新应用的安全风险。

第三章　网络的安全保护

第十五条【网络等级】根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。

（一）第一级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益的一般网络。

（二）第二级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造

成危害，但不危害国家安全的一般网络。

（三）第三级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。

（四）第四级，一旦受到破坏会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害的特别重要网络。

（五）第五级，一旦受到破坏后会对国家安全造成特别严重危害的极其重要网络。

第十六条【网络定级】网络运营者应当在规划设计阶段确定网络的安全保护等级。

当网络功能、服务范围、服务对象和处理的数据等发生重大变化时，网络运营者应当依法变更网络的安全保护等级。

第十七条【定级评审】对拟定为第二级以上的网络，其运营者应当组织专家评审；有行业主管部门的，应当在评审后报请主管部门核准。

跨省或者全国统一联网运行的网络由行业主管部门统一拟定安全保护等级，统一组织定级评审。

行业主管部门可以依据国家标准规范，结合本行业网络特点制定行业网络安全等级保护定级指导意见。

第十八条【定级备案】第二级以上网络运营者应当在网络的安全保护等级确定后 10 个工作日内，到县级以上公安机关备

案。

因网络撤销或变更调整安全保护等级的，应当在10个工作日内向原受理备案公安机关办理备案撤销或变更手续。

备案的具体办法由国务院公安部门组织制定。

第十九条【备案审核】公安机关应当对网络运营者提交的备案材料进行审核。对定级准确、备案材料符合要求的，应在10个工作日内出具网络安全等级保护备案证明。

第二十条【一般安全保护义务】网络运营者应当依法履行下列安全保护义务，保障网络和信息安全:

（一）确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度;

（二）建立安全管理和技术保护制度，建立人员管理、教育培训、系统安全建设、系统安全运维等制度;

（三）落实机房安全管理、设备和介质安全管理、网络安全管理等制度，制定操作规范和工作流程;

（四）落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施;

（五）落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并按照规定留存六个月以上可追溯网络违法犯罪的相关网络日志;

（六）落实数据分类、重要数据备份和加密等措施;

（七）依法收集、使用、处理个人信息，并落实个人信息保护措施，防止个人信息泄露、损毁、篡改、窃取、丢失和滥

用;

（八）落实违法信息发现、阻断、消除等措施，落实防范违法信息大量传播、违法犯罪证据灭失等措施;

（九）落实联网备案和用户真实身份查验等责任;

（十）对网络中发生的案事件，应当在二十四小时内向属地公安机关报告；泄露国家秘密的，应当同时向属地保密行政管理部门报告。

（十一）法律、行政法规规定的其他网络安全保护义务。

第二十一条【特殊安全保护义务】第三级以上网络的运营者除履行本条例第二十条规定的网络安全保护义务外，还应当履行下列安全保护义务:

（一）确定网络安全管理机构，明确网络安全等级保护的工作职责，对网络变更、网络接入、运维和技术保障单位变更等事项建立逐级审批制度;

（二）制定并落实网络安全总体规划和整体安全防护策略，制定安全建设方案，并经专业技术人员评审通过;

（三）对网络安全管理负责人和关键岗位的人员进行安全背景审查，落实持证上岗制度;

（四）对为其提供网络设计、建设、运维和技术服务的机构和人员进行安全管理;

（五）落实网络安全态势感知监测预警措施，建设网络安全防护管理平台，对网络运行状态、网络流量、用户行为、网

络安全案事件等进行动态监测分析，并与同级公安机关对接;

（六）落实重要网络设备、通信链路、系统的冗余、备份和恢复措施;

（七）建立网络安全等级测评制度，定期开展等级测评，并将测评情况及安全整改措施、整改结果向公安机关和有关部门报告;

（八）法律和行政法规规定的其他网络安全保护义务。

第二十二条【上线检测】新建的第二级网络上线运行前应当按照网络安全等级保护有关标准规范，对网络的安全性进行测试。

新建的第三级以上网络上线运行前应当委托网络安全等级测评机构按照网络安全等级保护有关标准规范进行等级测评，通过等级测评后方可投入运行。

第二十三条【等级测评】第三级以上网络的运营者应当每年开展一次网络安全等级测评，发现并整改安全风险隐患，并每年将开展网络安全等级测评的工作情况及测评结果向备案的公安机关报告。

第二十四条【安全整改】网络运营者应当对等级测评中发现的安全风险隐患，制定整改方案，落实整改措施，消除风险隐患。

第二十五条【自查工作】网络运营者应当每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自

查，发现安全风险隐患及时整改，并向备案的公安机关报告。

第二十六条【测评活动安全管理】网络安全等级测评机构应当为网络运营者提供安全、客观、公正的等级测评服务。

网络安全等级测评机构应当与网络运营者签署服务协议，并对测评人员进行安全保密教育，与其签订安全保密责任书，明确测评人员的安全保密义务和法律责任，组织测评人员参加专业培训。

第二十七条【网络服务机构要求】网络服务提供者为第三级以上网络提供网络建设、运行维护、安全监测、数据分析等网络服务，应当符合国家有关法律法规和技术标准的要求。

网络安全等级测评机构等网络服务提供者应当保守服务过程中知悉的国家秘密、个人信息和重要数据。不得非法使用或擅自发布、披露在提供服务中收集掌握的数据信息和系统漏洞、恶意代码、网络入侵攻击等网络安全信息。

第二十八条【产品服务采购使用的安全要求】网络运营者应当采购、使用符合国家法律法规和有关标准规范要求的网络产品和服务。

第三级以上网络运营者应当采用与其安全保护等级相适应的网络产品和服务；对重要部位使用的网络产品，应当委托专业测评机构进行专项测试，根据测试结果选择符合要求的网络产品；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。

第二十九条【技术维护要求】第三级以上网络应当在境内实施技术维护，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施。实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。

第三十条【监测预警和信息通报】地市级以上人民政府应当建立网络安全监测预警和信息通报制度，开展安全监测、态势感知、通报预警等工作。

第三级以上网络运营者应当建立健全网络安全监测预警和信息通报制度，按照规定向同级公安机关报送网络安全监测预警信息，报告网络安全事件。有行业主管部门的，同时向行业主管部门报送和报告。

行业主管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，按照规定向同级网信部门、公安机关报送网络安全监测预警信息，报告网络安全事件。

第三十一条【数据和信息安全保护】网络运营者应当建立并落实重要数据和个人信息安全保护制度；采取保护措施，保障数据和信息在收集、存储、传输、使用、提供、销毁过程中的安全；建立异地备份恢复等技术措施，保障重要数据的完整性、保密性和可用性。

未经允许或授权，网络运营者不得收集与其提供的服务无关的数据和个人信息；不得违反法律、行政法规规定和双方约

定收集、使用和处理数据和个人信息；不得泄露、篡改、损毁其收集的数据和个人信息；不得非授权访问、使用、提供数据和个人信息。

第三十二条【应急处置要求】第三级以上网络的运营者应当按照国家有关规定，制定网络安全应急预案，定期开展网络安全应急演练。

网络运营者处置网络安全事件应当保护现场，记录并留存相关数据信息，并及时向公安机关和行业主管部门报告。

公安机关和行业主管部门应当向同级网信部门报告重大网络安全事件处置情况。

发生重大网络安全事件时，有关部门应当按照网络安全应急预案要求联合开展应急处置。电信业务经营者、互联网服务提供者应当为重大网络安全事件处置和恢复提供支持和协助。

第三十三条【审计审核要求】网络运营者建设、运营、维护和使用网络，向社会公众提供需取得行政许可的经营活动的，相关主管部门应当将网络安全等级保护制度落实情况纳入审计、审核范围。

第三十四条【新技术新应用风险管控】网络运营者应当按照网络安全等级保护制度要求，采取措施，管控云计算、大数据、人工智能、物联网、工控系统和移动互联网等新技术、新应用带来的安全风险，消除安全隐患。

第四章　涉密网络的安全保护

第三十五条【分级保护】涉密网络按照存储、处理、传输国家秘密的最高密级分为绝密级、机密级和秘密级。

第三十六条【网络定级】涉密网络运营者应当依法确定涉密网络的密级，通过本单位保密委员会（领导小组）的审定，并向同级保密行政管理部门备案。

第三十七条【方案审查论证】涉密网络运营者规划建设涉密网络，应当依据国家保密规定和标准要求，制定分级保护方案，采取身份鉴别、访问控制、安全审计、边界安全防护、信息流转管控、电磁泄漏发射防护、病毒防护、密码保护和保密监管等技术与管理措施。

第三十八条【建设管理】涉密网络运营者委托其他单位承担涉密网络建设的，应当选择具有相应涉密信息系统集成资质的单位，并与建设单位签订保密协议，明确保密责任，采取保密措施。

第三十九条【信息设备、安全保密产品管理】涉密网络中使用的信息设备，应当从国家有关主管部门发布的涉密专用信息设备名录中选择；未纳入名录的，应选择政府采购目录中的产品。确需选用进口产品的，应当进行安全保密检测。

涉密网络运营者不得选用国家保密行政管理部门禁止使用或者政府采购主管部门禁止采购的产品。

涉密网络中使用的安全保密产品，应当通过国家保密行政管理部门设立的检测机构检测。计算机病毒防护产品应当选用取得计算机信息系统安全专用产品销售许可证的可靠产品，密码产品应当选用国家密码管理部门批准的产品。

第四十条【测评审查和风险评估】涉密网络应当由国家保密行政管理部门设立或者授权的保密测评机构进行检测评估，并经设区的市级以上保密行政管理部门审查合格，方可投入使用。

涉密网络运营者在涉密网络投入使用后，应定期开展安全保密检查和风险自评估，并接受保密行政管理部门组织的安全保密风险评估。绝密级网络每年至少进行一次，机密级和秘密级网络每两年至少进行一次。

公安机关、国家安全机关涉密网络投入使用的管理，依照国家保密行政管理部门会同公安机关、国家安全机关制定的有关规定执行。

第四十一条【涉密网络使用管理总体要求】涉密网络运营者应当制定安全保密管理制度，组建相应管理机构，设置安全保密管理人员，落实安全保密责任。

第四十二条【涉密网络预警通报要求】涉密网络运营者应建立健全本单位涉密网络安全保密监测预警和信息通报制度，发现安全风险隐患的，应及时采取应急处置措施，并向保密行政管理部门报告。

第四十三条【涉密网络重大变化的处置】有下列情形之一的，涉密网络运营者应当按照国家保密规定及时向保密行政管理部门报告并采取相应措施:

（一）密级发生变化的;

（二）连接范围、终端数量超出审查通过的范围、数量的;

（三）所处物理环境或者安全保密设施变化可能导致新的安全保密风险的;

（四）新增应用系统的，或者应用系统变更、减少可能导致新的安全保密风险的。

对前款所列情形，保密行政管理部门应当及时作出是否对涉密网络重新进行检测评估和审查的决定。

第四十四条【涉密网络废止的处理】涉密网络不再使用的，涉密网络运营者应当及时向保密行政管理部门报告，并按照国家保密规定和标准对涉密信息设备、产品、涉密载体等进行处理。

第五章　密码管理

第四十五条【确定密码要求】国家密码管理部门根据网络的安全保护等级、涉密网络的密级和保护等级，确定密码的配备、使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。

第四十六条【涉密网络密码保护】涉密网络及传输的国家秘密信息，应当依法采用密码保护。

密码产品应当经过密码管理部门批准，采用密码技术的软件系统、硬件设备等产品，应当通过密码检测。

密码的检测、装备、采购和使用等，由密码管理部门统一管理；系统设计、运行维护、日常管理和密码评估，应当按照国家密码管理相关法规和标准执行。

第四十七条【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

第四十八条【密码安全管理责任】网络运营者应当按照国家密码管理法规和相关管理要求，履行密码安全管理职责，加强密码安全制度建设，完善密码安全管理措施，规范密码使用行为。

任何单位和个人不得利用密码从事危害国家安全、社会公共利益的活动，或者从事其他违法犯罪活动。

第六章　监督管理

第四十九条【安全监督管理】县级以上公安机关对网络运营者依照国家法律法规规定和相关标准规范要求，落实网络安全等级保护制度，开展网络安全防范、网络安全事件应急处置、重大活动网络安全保护等工作，实行监督管理；对第三级以上网络运营者按照网络安全等级保护制度落实网络基础设施安全、网络运行安全和数据安全保护责任义务，实行重点监督管理。

县级以上公安机关对同级行业主管部门依照国家法律法规规定和相关标准规范要求，组织督促本行业、本领域落实网络安全等级保护制度，开展网络安全防范、网络安全事件应急处置、重大活动网络安全保护等工作情况，进行监督、检查、指导。

地市级以上公安机关每年将网络安全等级保护工作情况通报同级网信部门。

第五十条【安全检查】县级以上公安机关对网络运营者开展下列网络安全工作情况进行监督检查:

（一）日常网络安全防范工作;

（二）重大网络安全风险隐患整改情况;

（三）重大网络安全事件应急处置和恢复工作;

（四）重大活动网络安全保护工作落实情况;

（五）其他网络安全保护工作情况。

公安机关对第三级以上网络运营者每年至少开展一次安全检查。涉及相关行业的可以会同其行业主管部门开展安全检查。必要时，公安机关可以委托社会力量提供技术支持。

公安机关依法实施监督检查，网络运营者应当协助、配合，并按照公安机关要求如实提供相关数据信息。

第五十一条【检查处置】公安机关在监督检查中发现网络安全风险隐患的，应当责令网络运营者采取措施立即消除；不能立即消除的，应当责令其限期整改。

公安机关发现第三级以上网络存在重大安全风险隐患的，应当及时通报行业主管部门，并向同级网信部门通报。

第五十二条【重大隐患处置】公安机关在监督检查中发现重要行业或本地区存在严重威胁国家安全、公共安全和社会公共利益的重大网络安全风险隐患的，应报告同级人民政府、网信部门和上级公安机关。

第五十三条【对测评机构和安全建设机构的监管】国家对网络安全等级测评机构和安全建设机构实行推荐目录管理，指导网络安全等级测评机构和安全建设机构建立行业自律组织，制定行业自律规范，加强自律管理。

非涉密网络安全等级测评机构和安全建设机构具体管理办法，由国务院公安部门制定。保密科技测评机构管理办法由国家保密行政管理部门制定。

第五十四条【关键人员管理】第三级以上网络运营者的关键岗位人员以及为第三级以上网络提供安全服务的人员，不得擅

自参加境外组织的网络攻防活动。

第五十五条【事件调查】公安机关应当根据有关规定处置网络安全事件，开展事件调查，认定事件责任，依法查处危害网络安全的违法犯罪活动。必要时，可以责令网络运营者采取阻断信息传输、暂停网络运行、备份相关数据等紧急措施。

网络运营者应当配合、支持公安机关和有关部门开展事件调查和处置工作。

第五十六条【紧急情况断网措施】网络存在的安全风险隐患严重威胁国家安全、社会秩序和公共利益的，紧急情况下公安机关可以责令其停止联网、停机整顿。

第五十七条【保密监督管理】保密行政管理部门负责对涉密网络的安全保护工作进行监督管理，负责对非涉密网络的失泄密行为的监管。发现存在安全隐患，违反保密法律法规，或者不符合保密标准保密的，按照《中华人民共和国保守国家秘密法》和国家保密相关规定处理。

第五十八条【密码监督管理】密码管理部门负责对网络安全等级保护工作中的密码管理进行监督管理，监督检查网络运营者对网络的密码配备、使用、管理和密码评估情况。其中重要涉密信息系统每两年至少开展一次监督检查。监督检查中发现存在安全隐患，或者违反密码管理相关规定，或者不符合密码相关标准规范要求的，按照国家密码管理相关规定予以处理。

第五十九条【行业监督管理】行业主管部门应当组织制定

本行业、本领域网络安全等级保护工作规划和标准规范，掌握网络基本情况、定级备案情况和安全保护状况；监督管理本行业、本领域网络运营者开展网络定级备案、等级测评、安全建设整改、安全自查等工作。

行业主管部门应当监督管理本行业、本领域网络运营者依照网络安全等级保护制度和相关标准规范要求，落实网络安全管理和技术保护措施，组织开展网络安全防范、网络安全事件应急处置、重大活动网络安全保护等工作。

第六十条【监督管理责任】网络安全等级保护监督管理部门及其工作人员应当对在履行职责中知悉的国家秘密、个人信息和重要数据严格保密，不得泄露、出售或者非法向他人提供。

第六十一条【执法协助】网络运营者和技术支持单位应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供支持和协助。

第六十二条【网络安全约谈制度】省级以上人民政府公安部门、保密行政管理部门、密码管理部门在履行网络安全等级保护监督管理职责中，发现网络存在较大安全风险隐患或者发生安全事件的，可以约谈网络运营者的法定代表人、主要负责人及其行业主管部门。

第七章　法律责任

第六十三条【违反安全保护义务】网络运营者不履行本条例第十六条，第十七条第一款，第十八条第一款、第二款，第二十条、第二十二条第一款，第二十四条，第二十五条，第二十八条第一款，第三十一条第一款，第三十二条第二款规定的网络安全保护义务的，由公安机关责令改正，依照《中华人民共和国网络安全法》第五十九条第一款的规定处罚。

第三级以上网络运营者违反本条例第二十一条、第二十二条第二款、第二十三条规定、第二十八条第二款，第三十条第二款，第三十二条第一款规定的，按照前款规定从重处罚。

第六十四条【违反技术维护要求】网络运营者违反本条例第二十九条规定，对第三级以上网络实施境外远程技术维护，未进行网络安全评估、未采取风险管控措施、未记录并留存技术维护日志的，由公安机关和相关行业主管部门依据各自职责责令改正，依照《中华人民共和国网络安全法》第五十九条第一款的规定处罚。

第六十五条【违反数据安全和个人信息保护要求】网络运营者违反本条例第三十一条第二款规定，擅自收集、使用、提供数据和个人信息的，由网信部门、公安机关依据各自职责责令改正，依照《中华人民共和国网络安全法》第六十四条第一款的规定处罚。

第六十六条【网络安全服务责任】违反本条例第二十六条

第三款，第二十七条第二款规定的，由公安机关责令改正，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，直至通知发证机关吊销相关业务许可证或者吊销营业执照。

违反本条例第二十七条第二款规定，泄露、非法出售或者向他人提供个人信息的，依照《中华人民共和国网络安全法》第六十四条第二款的规定处罚。

第六十七条【违反执法协助义务】网络运营者违反本条例规定，有下列行为之一的，由公安机关、保密行政管理部门、密码管理部门、行业主管部门和有关部门依据各自职责责令改正；拒不改正或者情节严重的，依照《中华人民共和国网络安全法》第六十九条的规定处罚。

（一）拒绝、阻碍有关部门依法实施的监督检查的；

（二）拒不如实提供有关网络安全保护的数据信息的；

（三）在应急处置中拒不服从有关主管部门统一指挥调度的；

（四）拒不向公安机关、国家安全机关提供技术支持和协助的；

（五）电信业务经营者、互联网服务提供者在重大网络安全事件处置和恢复中未按照本条例规定提供支持和协助的。

第六十八条【违反保密和密码管理责任】违反本条例有关

保密管理和密码管理规定的，由保密行政管理部门或者密码管理部门按照各自职责分工责令改正，拒不改正的，给予警告，并通报向其上级主管部门，建议对其主管人员和其他直接责任人员依法给予处分。

第六十九条【监管部门渎职责任】网信部门、公安机关、国家保密行政管理部门、密码管理部门以及有关行业主管部门及其工作人员有下列行为之一，对直接负责的主管人员和其他直接责任人员，或者有关工作人员依法给予处分：

（一）玩忽职守、滥用职权、徇私舞弊的；

（二）泄露、出售、非法提供在履行网络安全等级保护监管职责中获悉的国家秘密、个人信息和重要数据；或者将获取其他信息，用于其他用途的。

第七十条【法律竞合处理】违反本条例规定，构成违反治安管理行为的，由公安机关依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章　附　则

第七十一条【术语解释】本条例所称的“内”、“以上”包含本数；所称的“行业主管部门”包含行业监管部门。

第七十二条【军队】军队的网络安全等级保护工作，按照军队的有关法规执行。

第七十三条【生效时间】本条例由自　年 月 日起施行。