关键信息基础设施安全保护条例

（征求意见稿）

第一章 总则

第一条 为了保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 在中华人民共和国境内规划、建设、运营、维护、使用关键信息基础设施，以及开展关键信息基础设施的安全保护，适用本条例。

第三条 关键信息基础设施安全保护坚持顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。

第四条 国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。

国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关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按照国家有关规定开展关键信息基础设施安全保护工作。

第五条 关键信息基础设施的运营者（以下称运营者）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

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。

第六条 关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。

第七条 任何个人和组织发现危害关键信息基础设施安全的行为，有权向网信、电信、公安等部门以及行业主管或监管部门举报。

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 支持与保障

第八条 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。

第九条 国家制定产业、财税、金融、人才等政策，支持关键信息基础设施安全相关的技术、产品、服务创新，推广安全可信的网络产品和服务，培养和选拔网络安全人才，提高关键信息基础设施的安全水平。

第十条 国家建立和完善网络安全标准体系，利用标准指导、规范关键信息基础设施安全保护工作。

第十一条 地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。

第十二条 国家鼓励政府部门、运营者、科研机构、网络安全服务机构、行业组织、网络产品和服务提供者开展关键信息基础设施安全合作。

第十三条 国家行业主管或监管部门应当设立或明确专门负责本行业、本领域关键信息基础设施安全保护工作的机构和人员，编制并组织实施本行业、本领域的网络安全规划，建立健全工作经费保障机制并督促落实。

第十四条 能源、电信、交通等行业应当为关键信息基础设施网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持。

第十五条 公安机关等部门依法侦查打击针对和利用关键信息基础设施实施的违法犯罪活动。

第十六条 任何个人和组织不得从事下列危害关键信息基础设施的活动和行为：

（一）攻击、侵入、干扰、破坏关键信息基础设施；

（二）非法获取、出售或者未经授权向他人提供可能被专门用于危害关键信息基础设施安全的技术资料等信息；

（三）未经授权对关键信息基础设施开展渗透性、攻击性扫描探测；

（四）明知他人从事危害关键信息基础设施安全的活动，仍然为其提供互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等帮助；

（五）其他危害关键信息基础设施的活动和行为。

第十七条 国家立足开放环境维护网络安全，积极开展关键信息基础设施安全领域的国际交流与合作。

第三章 关键信息基础设施范围

第十八条 下列单位运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围：

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）其他重点单位。

第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。

国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。

关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。

第二十条 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。

国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。

第四章 运营者安全保护

第二十一条 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。

第二十二条 运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。

第二十三条 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，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；

（二）采取技术措施，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；

（三）采取技术措施，监测、记录网络运行状态、网络安全事件，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认证等措施。

第二十四条 除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务：

（一）设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位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，及时对系统漏洞等安全风险采取补救措施；

（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。

第二十五条 运营者网络安全管理负责人履行下列职责：

（一） 组织制定网络安全规章制度、操作规程并监督执行；

（二）组织对关键岗位人员的技能考核；

（三）组织制定并实施本单位网络安全教育和培训计划；

（四）组织开展网络安全检查和应急演练，应对处置网络安全事件；

（五）按规定向国家有关部门报告网络安全重要事项、事件。

第二十六条 运营者网络安全关键岗位专业技术人员实行执证上岗制度。

执证上岗具体规定由国务院人力资源社会保障部门会同国家网信部门等部门制定。

第二十七条 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于 1 个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于 3 个工作日。

第二十八条 运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。

运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时进行整改，并将有关情况报国家行业主管或监管部门。

第二十九条 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，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。

第五章 产品和服务安全

第三十条 运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。

第三十一条 运营者采购网络产品和服务，可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。

第三十二条 运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测。

第三十三条 运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告。

第三十四条 关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。

第三十五条 面向关键信息基础设施开展安全检测评估，发布系统漏洞、计算机病毒、网络攻击等安全威胁信息，提供云计算、信息技术外包等服务的机构，应当符合有关要求。

具体要求由国家网信部门会同国务院有关部门制定。

第六章 监测预警、应急处置和检测评估

第三十六条 国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息。

第三十七条 国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息。

国家行业主管或监管部门应当组织对安全监测信息进行研判，认为需要立即采取防范应对措施的，应当及时向有关运营者发布预警信息和应急防范措施建议，并按照国家网络安全事件应急预案的要求向有关部门报告。

第三十八条 国家网信部门统筹协调有关部门、运营者以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享。

第三十九条 国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。

国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况。

第四十条 国家行业主管或监管部门应当定期组织对本行业、本领域关键信息基础设施的安全风险以及运营者履行安全保护义务的情况进行抽查检测，提出改进措施，指导、督促运营者及时整改检测评估中发现的问题。

国家网信部门统筹协调有关部门开展的抽查检测工作，避免交叉重复检测评估。

第四十一条 有关部门组织开展关键信息基础设施安全检测评估，应坚持客观公正、高效透明的原则，采取科学的检测评估方法，规范检测评估流程，控制检测评估风险。

运营者应当对有关部门依法实施的检测评估予以配合，对检测评估发现的问题及时进行整改。

第四十二条 有关部门组织开展关键信息基础设施安全检测评估，可采取下列措施：

（一）要求运营者相关人员就检测评估事项作出说明；

（二）查阅、调取、复制与安全保护有关的文档、记录；

（三）查看网络安全管理制度制订、落实情况以及网络安全技术措施规划、建设、运行情况；

（四）利用检测工具或委托网络安全服务机构进行技术检测；

（五）经运营者同意的其他必要方式。

第四十三条 有关部门以及网络安全服务机构在关键信息基础设施安全检测评估中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第四十四条 有关部门组织开展关键信息基础设施安全检测评估，不得向被检测评估单位收取费用，不得要求被检测评估单位购买指定品牌或者指定生产、销售单位的产品和服务。

第七章 法律责任

第四十五条 运营者不履行本条例第二十条第一款、第二十一条、第二十三条、第二十四条、第二十六条、第二十七条、第二十八条、第三十条、第三十二条、第三十三条、第三十四条规定的网络安全保护义务的，由有关主管部门依据职责责令改正，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。

第四十六条 运营者违反本条例第二十九条规定，在境外存储网络数据，或者向境外提供网络数据的，由国家有关主管部门依据职责责令改正，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；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。

第四十七条 运营者违反本条例第三十一条规定，使用未经安全审查或安全审查未通过的网络产品或者服务的，由国家有关主管部门依据职责责令停止使用，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。

第四十八条 个人违反本条例第十六条规定，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；构成犯罪的，依法追究刑事责任。

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。

违反本条例第十六条规定，受到刑事处罚的人员，终身不得从事关键信息基础设施安全管理和网络运营关键岗位的工作。

第四十九条 国家机关关键信息基础设施的运营者不履行本条例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负责人员依法给予处分。

第五十条 有关部门及其工作人员有下列行为之一的，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；构成犯罪的，依法追究刑事责任：

（一）在工作中利用职权索取、收受贿赂；

（二）玩忽职守、滥用职权；

（三）擅自泄露关键信息基础设施有关信息、资料及数据文件；

（四）其他违反法定职责的行为。

第五十一条 关键信息基础设施发生重大网络安全事件，经调查确定为责任事故的，除应当查明运营单位责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第五十二条 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、国家安全机关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。

第八章 附则

第五十三条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。

第五十四条 军事关键信息基础设施的安全保护，由中央军事委员会另行规定。

第五十五条 本条例自****年**月**日起施行。