电力行业网络安全管理办法

第一章　总　　则

第一条　为加强电力行业网络安全监督管理，规范电力行业网络安全工作，根据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国计算机信息系统安全保护条例》、《关键信息基础设施安全保护条例》及国家有关规定，制定本办法。

第二条　电力行业网络安全工作的目标是建立健全网络安全保障体系和工作责任体系，提高网络安全防护能力，保障电力系统安全稳定运行和电力可靠供应。

第三条　电力企业在中华人民共和国境内建设、运营、维护和使用网络（除核安全外），以及网络安全的监督管理，适用本办法。

本办法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，包括电力监控系统、管理信息系统及通信网络设施。

本办法不适用于涉及国家秘密的网络。涉及国家秘密的网络应当按照国家保密工作部门有关涉密信息系统管理规定和技术标准，结合网络实际情况进行管理。

第四条　电力行业网络安全工作坚持“积极防御、综合防范”的方针，遵循“依法管理、分工负责，统筹规划、突出重点”的原则。

第二章　监督管理职责

第五条　国家能源局及其派出机构、负有电力行业网络安全监督管理职责的地方能源主管部门（以下简称行业部门）在各自职责范围内依法依规履行电力行业网络安全监督管理职责。

第六条　电力行业网络安全监督管理工作主要包括以下内容：

（一）组织落实国家关于网络安全的方针、政策和重大部署，并与电力生产安全监督管理工作相衔接；

（二）组织制定电力行业网络安全等级保护、关键信息基础设施安全保护、电力监控系统安全防护、网络安全监测预警和信息通报、网络安全事件应急处置等方面的政策规定及技术规范，并监督实施；

（三）组织认定电力行业关键信息基础设施，制定关键信息基础设施安全规划，建立关键信息基础设施网络安全监测预警制度，组织开展关键信息基础设施网络安全检查检测，指导关键信息基础设施运营者做好网络安全事件应对处置；

（四）组织或参与网络安全事件的调查与处理；

（五）督促电力企业落实网络安全责任、保障网络安全经费、开展网络安全防护能力建设等工作；

（六）组织开展电力行业网络安全信息通报等工作；

（七）指导督促电力企业做好网络安全宣传教育工作；

（八）推动网络安全仿真验证环境（靶场）建设，组织建立网络安全监督管理技术支撑体系；

（九）电力行业网络安全监督管理的其它事项。

第七条　电力调度机构负责直接调度范围内的下一级电力调度机构、集控中心、变电站（换流站）、发电厂（站）等各类机构涉网部分的电力监控系统安全防护的技术监督。主要包括以下内容：

（一）自行组织或委托电力监控系统安全防护评估机构开展调度范围内电力监控系统的自评估工作，配合开展电力监控系统的检查评估工作，负责统一指挥调度范围内的电力监控系统安全应急处理，参与电力监控系统的网络安全事件调查和分析工作；

（二）组织并督促各相关单位开展电力监控系统安全防护技术培训和交流工作，贯彻执行国家和行业有关电力监控系统安全防护的标准、规程和规范；

（三）负责对电力监控系统专用安全产品开展监督管理，制定电力监控系统专用安全产品管理办法并监督实施；

（四）将并网电厂涉网部分电力监控系统网络安全运行状态纳入监测；

（五）每年 11 月 1 日前将技术监督工作开展情况报送行业部门。

第三章　电力企业责任义务

第八条　电力企业是本单位网络安全的责任主体，负责本单位的网络安全工作。

第九条　电力企业主要负责人是本单位网络安全的第一责任人。电力企业应当建立健全网络安全管理、评价考核制度体系，成立工作领导机构，明确责任部门，设立专职岗位，定义岗位职责，明确人员分工和技能要求，建立健全网络安全责任制。

电力行业关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，要明确一名领导班子成员（非公有制经济组织运营者明确一名核心经营管理团队成员）作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作；为每个关键信息基础设施明确一名安全管理责任人；设立专门安全管理机构，确定关键岗位及人员，并对机构负责人和关键岗位人员进行安全背景审查。

第十条　电力企业应当依法依规开展关键信息基础设施信息报送工作，关键信息基础设施发生较大变化，可能影响其认定结果的，关键信息基础设施运营者发生合并、分立、解散等情况的，应当及时将相关情况报告行业部门。

第十一条　电力企业应当按照国家网络安全等级保护制度、关键信息基础设施安全保护制度、数据安全制度、网络安全审查工作机制和电力监控系统安全防护规定的要求，对本单位的网络进行安全保护，并将网络安全纳入安全生产管理体系。

第十二条　电力企业应当选用符合国家有关规定、满足网络安全要求的网络产品和服务，开展网络安全建设或改建工作。接入生产控制大区的涉网安全产品需经电力调度机构同意。

第十三条　电力行业关键信息基础设施运营者应当优先采购安全可信的网络产品和服务，并按照有关要求开展风险预判工作，评估投入使用后可能对关键信息基础设施安全、电力生产安全和国家安全的影响，形成评估报告。影响或者可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第十四条　电力企业规划设计网络时，应当明确安全保护需求，保证安全措施同步规划、同步建设、同步使用，设计合理的总体安全方案并经专业技术人员评审通过，制定安全实施计划，负责网络安全建设工程的实施。网络上线前，电力企业应当委托网络安全服务机构开展第三方安全测试。

第十五条　电力企业应当按照国家有关规定开展电力监控系统安全防护评估、网络安全等级保护测评、关键信息基础设施网络安全检测和风险评估、商用密码应用安全性评估和网络安全审查等工作，未达到要求的应当及时进行整改。

第十六条　电力企业不得委托在近3年内被行业部门通报有不良行为或被相关部门通报整改的网络安全服务机构。

第十七条　电力企业应当按照国家有关规定开展网络安全风险评估工作，建立健全网络安全风险评估的自评估和检查评估制度，完善网络安全风险管理机制。发现风险隐患可能对电力行业网络安全产生较大影响的，应当向行业部门报告。

第十八条　电力企业应当依据国家和行业相关标准、规程和规范开展网络安全技术监督工作，可委托网络安全服务机构协助开展。

第十九条　电力企业应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，发现或者获知存在安全漏洞后，应当立即评估安全漏洞的影响范围及程度，及时对安全漏洞进行验证并完成修补。

第二十条　电力企业应当建立健全本单位网络安全监测预警和信息通报机制，及时掌握本单位网络安全运行状况、安全态势，及时处置网络安全威胁与隐患，定期向行业部门报告有关情况。

电力行业关键信息基础设施运营者应当建立 7×24 小时值班值守制度，建设网络安全态势感知平台，并与行业部门、公安机关等有关平台对接。

第二十一条　电力企业应当按照电力行业网络安全事件应急预案，制修订本单位网络安全事件应急预案，每年至少开展一次应急演练。制修订电力监控系统专项网络安全事件应急预案并定期组织演练。定期组织开展网络攻防演习，检验安全防护和应急处置能力。

第二十二条 电力企业应当在国家重要活动、会议期间结合实际制定网络安全保障专项工作方案和应急预案，成立保障组织机构，明确目标任务，细化措施要求，组织预案演练，确保重要信息系统、电力监控系统安全稳定运行。

第二十三条 电力企业发生网络安全事件后，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，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，注意保护现场，并按照规定向有关主管部门报告。

第二十四条 电力企业应当按照国家有关规定，建立健全容灾备份制度，对重要系统和重要数据进行有效备份。

第二十五条 电力企业应当建立健全全流程数据安全管理和个人信息保护制度，按照国家和行业重要数据目录及数据分类分级保护相关要求，确定本单位的重要数据具体目录，对列入目录的数据进行重点保护。

第二十六条 电力企业应当建立网络安全资金保障制度，安排网络安全专项预算，确保网络安全投入不低于信息化总投入的 5%。

第二十七条 电力企业应当加强网络安全从业人员考核和管理，建立与网络安全工作特点相适应的人才培养机制，做好全员网络安全宣传教育，提高网络安全意识。从业人员应当定期接受相应的政策规范和专业技能培训，并经培训合格后上岗。

第二十八条 电力企业应当督促电力监控系统专用安全产品研发单位和供应商按照国家有关要求做好保密工作，防止关键技术泄露。严禁在互联网上销售、购买电力监控系统专用安全产品。

第二十九条 电力企业应当于每年 11 月 1 日前，将当年网络安全工作的专项总结报行业部门。总结内容应当包括但不限于网络安全工作开展情况、网络安全等级保护情况、电力监控系统安全防护评估情况、数据安全情况、安全监测预警情况、风险隐患治理情况、网络安全事件应对处置情况、应急预案及演练情况、网络产品和服务采购情况、下一年度工作计划等。

电力行业关键信息基础设施运营者应当于每年 11 月 1 日前，将当年关键信息基础设施安全保护工作的专项总结报行业部门。总结内容应当包括但不限于关键信息基础设施的运行情况、认定报送情况、安全监测预警情况、网络安全检测和风险评估情况、网络安全事件应对处置情况、应急预案及演练情况、网络产品和服务采购情况、密码使用情况、下一年度安全保护计划等。

第四章 监督检查

第三十条 行业部门在各自职责范围内依法依规对电力企业网络安全工作进行监督检查，定期组织开展电力行业关键信息基础设施网络安全检查检测。

第三十一条 行业部门进行监督检查和事件调查时，可以采取下列措施：

（一）进入电力企业进行检查；

（二）询问相关单位的工作人员，要求其对有关检查事项作出说明；

（三）查阅、复制与检查事项有关的文件、资料，对可能被转移、隐匿、损毁的文件、资料予以封存；

（四）对检查中发现的问题，责令其当场改正或者限期改正。

第三十二条 行业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电力企业法定代表人或者主要负责人进行约谈，情节严重的依据国家有关法律、法规予以处理。

行业部门可就网络安全缺陷、漏洞等风险，网络攻击、恶意软件等威胁，网络安全事件开展行业通报，电力企业应当及时排查并采取风险防范措施。

第三十三条 行业部门工作人员必须对在履行监督管理职责中知悉的国家秘密、工作秘密、商业秘密、重要数据、个人信息和隐私严格保密，不得泄露、出售或者非法向他人提供。

第五章 附 则

第三十四条 本办法由国家能源局负责解释。

第三十五条 本办法自发布之日起施行，有效期5年。《电力行业网络与信息安全管理办法》（国能安全〔2014〕317号）同时废止。