团体标准

20XX—XX—XX实施

20XX—XX—XX发布

电力行业关键信息基础设施安全保护要求

 Security protection of critical information infrastructure of power industry

（征求意见稿）

T/CSEE XXXX—YYYY

代替 T/XXXX

ICS 19.020

CCS K85

发 布

中国电机工程学会

目 次

前 言 4

引 言 5

1 适用范围 6

2 规范性引用文件 6

3 术语和定义 6

3.1 关键信息基础设施 critical information infrastructure 6

3.2 电力行业关键信息基础设施 critical information infrastructure of power industry 6

4 缩略语 6

5 安全保护基本原则 7

6 安全保护框架及活动 7

6.1 安全保护框架 7

6.2 安全保护活动 8

7 分析识别 9

7.1 业务识别 9

7.2 资产识别 9

7.3 风险识别 10

7.4 重大变更 10

8 安全防护 10

8.1 网络安全等级保护 10

8.2 安全管理制度 11

8.3 安全管理机构 11

8.4 安全管理人员 11

8.5 安全通信网络 11

8.6 安全计算环境 12

8.7 安全建设管理 13

8.8 安全运维管理 13

8.9 供应链安全保护 13

8.10 数据安全防护 13

9 检测评估 14

9.1 制度 14

9.2 方式和内容 14

10 监测预警 15

10.1 制度 15

10.2 监测 15

10.3 预警 16

11 主动防御 16

11.1 收敛暴露面 16

11.2 攻击发现和阻断 17

11.3 攻防演练 17

11.4 威胁情报 17

12 事件处置 18

12.1 制度 18

12.2 应急预案和演练 18

12.3 响应和处置 18

12.4 重新识别 19

前 言

本文件按照《中国电机工程学会标准管理办法（暂行）》的要求，依据GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国电机工程学会提出。

本文件由中国电机工程学会电力信息化标准专业委员会技术归口和解释。

本文件起草单位：国家电网有限公司信息通信分公司、路云天网络安全研究院、北京中电普华信息技术有限公司、深信服科技股份有限公司、国网河北省电力有限公司信息通信分公司、中国华能集团有限公司、国网智能电网研究院有限公司、国网青海省电力公司信息通信公司、南方电网深圳供电局有限公司、北京百度网讯科技有限公司、北京摄星科技有限公司。

本文件主要起草人：胡威、王少杰、欧阳述嘉、王思宁、杜昊阳、程杰、张錋、王婵、曾荣汉、刘世良、吕珍珍、王磊、姚海旭、孙强强、陈彪、朱少敏、贾涛、张吉州、俞晓舟、孙伟、于俊杰、胡少楠、伊玮珑、王术正、闫光武、范佳雪、辛锐、王军、郑倩、祝文军、丘惠军、张道娟、杨柳、钱珂翔

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中国电机工程学会标准执行办公室（地址：北京市西城区白广路二条1 号，100761，网址：http：//www.csee.org.cn，邮箱：cseebz@csee.org.cn）。

引 言

为推动落实《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《信息安全技术 关键信息基础设施安全保护要求》相关要求，在国家网络安全等级保护制度基础上，结合电力系统特点和安全现状，提出电力行业关键信息基础设施安全保护要求。从而明确电力行业关键信息基础设施安全防护的基本要求，为电力行业构建安全保护能力提供依据，确保电力行业关键信息基础设施网络安全，保障电力系统的长期安全、稳定运行。

电力行业关键信息基础设施安全保护要求

1. 适用范围

本文件给出了电力行业关键信息基础设施安全防护总体原则，规定了风险识别、防护、监测预警、应急处置等主要防护环节的保护要求。

本文件适用于电力生产、电力传输、电力配送等相关企业。针对其认定的关键信息基础设施，包括并不限于骨干型电网、发电侧等相关的重要IT系统或网络服务，指导开展安全防护能力的规划、设计、开发、建设和运营等活动，也可供第三方机构对关键信息基础设施安全防护能力进行评估时提供具体参考。

1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 25069-2022 信息安全技术 术语

GB/T 37138-2018 电力信息系统安全等级保护实施指南

GB/T 36572-2018 电力监控系统网络安全防护导则

GB/T 38318-2019 电力监控系统网络安全评估指南

1. 术语和定义

GB/T 36572-2018 界定的以及下列术语和定义适用于本文件。

* 1. 关键信息基础设施 critical information infrastructure

指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。

* 1. 电力行业关键信息基础设施 critical information infrastructure of power industry

电力行业中涉及到国家安全、国计民生、公共利益的重要信息系统、通信网络安全设施和数据资源等。

1. 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（Critical Information Infrastructure）

CBI：关键业务信息（Critical Business Information）

IP：互联网协议（Internet Protocol）

IDC：互联网数据中心(Internet Data Center)

DNS：域名系统(Domain Name System)

APT：高级持续性威胁（Advanced Persistent Threat）

VPN：虚拟专用网络(Virtual Private Network)

1. 安全保护基本原则

电力行业键信息基础设施安全保护应在网络安全等级保护制度基础上，实行重点保护，应遵循以下基本原则：

——以实战需求为牵引的顶层设计。坚持网络安全与信息化同步规划、同步建设、同步使用，夯实基础、完善体系、提升能力、补足短板，坚持顶层设计，保障安全保护建设的先进性、实用性和有效性。

——以关键业务为核心的整体防控。以保护电力行业关键业务持续稳定运行为目标，对关键业务所涉及的一个或多个网络和信息系统进行体系化安全设计，构建整体安全防控体系。

——以风险管理为导向的动态防护。持续监测电力行业关键信息基础设施的安全状态，构建形成动态的安全防护机制，实现安全控制措施的动态调整，及时有效地防范应对安全风险。

——以信息共享为基础的协同联防。积极构建相关方广泛参与的信息共享、协同处置、联动防护的保护机制，提升协同联防能力，积极应对并有效防御网络攻击。

——以智能聚合为抓手的能力整合。采用人机结合、人工智能等方式，将现有的安全能力进行优化整合，将分析识别、安全防护、检测评估、监测预警、技术对抗、事件处置六大环节安全能力聚合，实现各环节安全数据共享及安全系统对接联动，促进安全业务闭环综合管理。

——以平战结合为一体的智能运营。基于日常和特殊时期的安全运营需求，构建动态、闭环、流程化、运营能力可迭代自提升的安全运营体系，实现流程化、自动化、一体化的智能运营。

1. 安全保护框架及活动
	1. 安全保护框架

电力行业关键信息基础设施安全保护框架如图所示。



图1 电力行业关键信息基础设施安全保护框架

电力行业关键信息基础设施安全保护框架以顶层设计、整体防控、动态防护、协同联防、能力整合、智能运营为安全保护基础原则，安全保护体系包括管理体系、技术体系、保障体系和运营体系方面，通过聚合分析识别、安全防护、检测评估、监测预警、主动防御和事件处置等六大环节，全面动态掌握网络安全业务开展状况，动态化持续性防控网络安全风险隐患，开展一体化、动态化、智能化安全运营，强化提升信息共享和协调指挥的能力，提升网络安全整体防护、技术对抗和抵御大规模网络攻击能力，实现以电力行业关键业务和重要数据为核心的整体防控，以风险管理和隐患防范为导向的动态防护，以信息共享和业务联动为基础的协同联防，切实保障电力行业核心业务系统稳定、持续运行。

* 1. 安全保护活动

本文件参照GB/T 39204-2022，从分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等六个环节提出相应安全控制措施。运营者应在满足网络安全等级保护GB/T 22239相应级别要求的基础上，遵循以实战需求为牵引的顶层设计、以关键业务为核心的整体防控、以风险管理为导向的动态防护、以信息共享为基础的协同联防、以智能聚合为抓手的能力整合、以平战结合为一体的智能运营等基本原则，根据自身具体情况和识别的安全风险，选择应采取的安全控制措施，确保将安全风险控制在可接受的范围，保护核心业务系统稳定、持续地运行。

1. 分析识别：围绕电力行业关键信息基础设施承载的关键业务，开展业务依赖性识别、关键资产识别、风险识别等活动，本环节是其他环节活动基础。
2. 安全防护：根据电力行业已识别的关键业务、资产、安全风险，在安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面实施安全管理和技术保护措施，采用安全能力智能聚合等方式，促进安全防护能力迭代提升，确保关键信息基础设施的运行安全，本环节是构建整体防控体系的关键。
3. 检测评估：应建立相应的检测评估制度，确定检测评估的流程及内容等，开展安全检测与风险隐患评估，分析潜在安全风险可能引发的安全事件，检验安全防护措施的有效性，促进安全防护环节的动态调整。
4. 监测预警：建立并实施网络安全监测预警和信息通报制度，针对发生的网络安全事件或发现的网络安全威胁，提前或及时发出安全警示，构建协同联防机制，主动应对网络攻击。
5. 主动防御：应对检测评估和监测预警发现的安全风险和攻击行为，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作，提升对网络威胁和攻击行为的主动防御能力。
6. 事件处置：对网络安全事件进行报告和处置，并采取适当的应对措施，恢复由于网络安全事件而受损的功能或服务，持续提升流程化、自动化、一体化的智能运营能力。
7. 分析识别
	1. 业务识别

电力行业关键信息基础设施运营者应：

1. 建立关键信息基础设施业务分析识别管理制度，指导开展业务识别工作。对组织开展关键业务分析识别工作进行管理，明确重点保护和管理范围，明确关基业务分析识别的工作依据、适用范围、负责人员、识别内容、分析粒度、分析频率等。通过关键信息基础设施业务分析识别流程规范，规范关键业务基础情况梳理、关键业务信息化情况梳理、关键业务信息（CBI）梳理和CII要素确定四个的流程步骤，输出关键信息基础设施业务信息化描述文档，描述关键业务集成情况、关键业务信息化情况、关键业务信息描述以及CII关键要素等内容；
2. 识别本组织的关键业务及其所依赖的关键信息基础设施，并明确关键信息基础设施的范围分布、运营情况、影响范围、业务类别、业务逻辑等，测绘业务网络结构、区域分布、核心节点、业务接口等业务图谱，为掌握业务运行状态和安全态势等提供支撑；
3. 采用人工梳理和自动化识别相结合的方式，分析识别本单位的关键业务和关键业务所依赖的外部业务，绘制关键业务网络、逻辑、边界、关联关系等图谱，依据电力相关单位关键业务特征，充分考虑骨干型电网、发电侧等相关的特殊系统或网络服务等相关要素；
4. 标识外部业务对本单位关键业务的重要等级，当本单位关键业务为外部业务提供服务时，识别并标识关键业务对外部业务的重要等级；
5. 通过技术手段或自动化方式及时发现关键属性的变化，关键信息基础设施的关键属性如业务连续性、系统完整性和数据保密性或上述特性的组合。
	1. 资产识别

电力行业关键信息基础设施运营者应参照GB/T 20984-2022，识别关键业务链所依赖的资产：

1. 建立关键信息基础设施业务风险分析管理制度，指导开展风险识别工作。提出关键信息基础设施资产风险评估要求与风险管理办法，定期对资产开展风险评估，制定资产价值评估、安全风险分析及风险处置原则。建立软硬件供应链安全风险识别机制，识别掌握关键业务链面临的风险隐患；通过关键信息基础设施业务风险分析流程规范，制定资产识别与价值评估、漏洞扫描、渗透测试、策略分析、风险分析、处置加固与风险复测的闭环风险管理流程。通过定期开展资产风险评估输出关键信息基础设施业务风险评估报告，明确目前资产存在的安全风险、风险等级、影像范围以及解决方案，推动关基资产安全风险管理工作的开展；
2. 确定资产分类方法并进行资产识别，例如，根据资产的表现形式，可将资产分为数据、服务、信息系统、平台或支撑系统、基础设施及人员等；
3. 围绕关键信息基础设施承载的关键业务，进行资产业务承载性识别和资产关联性识别；
4. 基于资产类别、资产本身的重要性以及资产所支撑的业务的重要性，对资产进行优先排序，确定资产防护的优先级；
5. 采用资产探测技术手段、资产台账导入、人工录入等方式，建立和维护各类资产清单，明确资产的管理责任人/部门、资产所支撑的关键业务以及资产的重要性；
6. 采用资产管理相关技术工具，实现资产数据的统一管理，为安全防护、检测评估、监测预警、主动防御、事件处置等活动开展提供数据或业务接口。
	1. 风险识别

电力行业关键信息基础设施运营者应参照GB/T 20984，围绕关键业务链进行以下活动：

1. 建立关键信息基础设施业务风险分析管理制度，指导开展风险识别工作。提出关键信息基础设施资产风险评估要求与风险管理办法，定期对资产开展风险评估，制定资产价值评估、安全风险分析及风险处置原则。建立软硬件供应链安全风险识别机制，识别掌握关键业务链面临的风险隐患；通过关键信息基础设施业务风险分析流程规范，制定资产识别与价值评估、漏洞扫描、渗透测试、策略分析、风险分析、处置加固与风险复测的闭环风险管理流程。通过定期开展资产风险评估输出关键信息基础设施业务风险评估报告，明确目前资产存在的安全风险、风险等级、影像范围以及解决方案，推动关基资产安全风险管理工作的开展；
2. 采用探测扫描、检测评估、渗透测试、情报共享等方式，对业务、资产、威胁、脆弱性及已有安全措施进行识别，分析主要安全风险点，确定风险处置的优先级，形成安全风险报告；
3. 采用适当的方法与工具确定威胁利用脆弱性的可能性，进而分析导致安全事件发生的可能性；
4. 综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险；
5. 采用风险识别动态管控技术手段，掌握风险危害程度、分布状况和态势信息，动态持续性开展风险识别和管理，掌握软硬件供应链安全风险状况，考虑极端情况下可能引发安全风险的要素。
	1. 重大变更

电力行业关键信息基础设施运营者应：

1. 建立关键信息基础设施业务重大变更管理制度，指导开展重大变更工作。对关键信息基础设施业务重大变更进行监控与管理，提出关键业务的监控、业务发生重大变化判断依据、业务重新认定识别与变更通知通报等相关要求。通过业务重大变更流程规范，明确业务变更监测、业务重新识别认定、业务变更申请通报的工作流程，生成关键信息基础设施业务重大变更文档，对变更工作进行记录，并且更新关键信息基础设施业务信息化描述文档报送监督管理部门；
2. 当关键信息基础设施发生改建、扩建、所有人变更等较大变化时，应重新开展识别工作，有可能影响认定结果的，应及时将相关情况报告保护工作部门，并更新资产清单；
3. 针对重大变更情形，包括但不限于网络拓扑发生重大变化、关键业务链或关键属性发生变化、业务服务范围发生重大变化等，重新进行资产、业务链、重要性、依赖性等识别，安全风险识别，更新资产清单，更新业务分布和运营情况，为安全防护、监测预警、主动防御等活动开展同步信息。
4. 安全防护
	1. 网络安全等级保护

应落实国家网络安全等级保护制度相关要求，对关键信息基础设施相关的保护对象开展定级、备案、安全建设整改和等级测评等工作。

1. 邀请网络安全等级保护工作专家组、电力行业专家对关键信息基础设施进行评审，确定信息系统安全保护等级；
2. 运营者持关键信息基础设施的定级备案材料到当地公安机关网安部门进行备案，获取备案证明；
3. 运营者参照网络安全等级保护相关标准及规范要求，对关键信息基础设施进行整改加固；
4. 运营者委托测评机构对关键信息基础设施进行等级测评，形成正式的测评报告。如存在剩余安全问题，应制定整改计划。
	1. 安全管理制度

安全管理制度应满足GB/T 39204-2022中的7.2相关要求。

* 1. 安全管理机构

安全管理机构应满足GB/T 39204-2022中的7.3相关要求。

* 1. 安全管理人员

安全管理人员应满足GB/T 39204-2022中的7.4相关要求。

* 1. 安全通信网络
		1. 网络架构

网络架构要求包括：

1. 应划分为生产控制大区和信息管理大区，生产控制大区可以分为控制区（又称安全区I）和非控制区（又称安全区II），信息管理大区可分为信息管理Ⅲ区、信息管理Ⅳ区；
2. 控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区的关键链路、关键设备应采取冗余备份，避免单点故障。
	* 1. 互联安全

互联安全要求包括：

1. 生产控制大区与信息管理大区之间应设置专用单向安全隔离装置，隔离强度应当接近或达到物理隔离；
2. 生产控制大区内部的安全区之间应当采用具有访问控制功能的网络设备、防火墙或者相当功能的设施，实现逻辑隔离；
3. 应保持同一用户在不同网络安全等级保护系统、不同业务系统、不同区域中的访问控制措施与安全互联策略的一致性，实现基于全局身份的认证校验和策略控制，围绕访问过程的持续信任评估，避免存在绕过指定访问控制策略的情况；
4. 控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区之间应部署专用加密认证装置，通过密码技术对通信的双方进行验证或鉴别；
5. 采用电力专用光纤进行长距离通信时，应采用网络访问控制、入侵检测等措施保证通信安全。
6. 租用电信运营商专线或光缆进行长距离通信时，应采用链路加密、VPN等技术保证数据加密传输；
7. 第三方机构网络接入时，应采用网络专线接入，设置第三方网络接入区，并采取网络防火墙实现安全隔离；
8. 作业类、采集类等专用终端通过电信运营商专线/无线网络接入时，应采用安全接入网关和信息安全网络隔离装置，实现接入认证和数据传输加密。
	* 1. 边界防护

边界防护要求包括：

1. 控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区的不同网络安全等级保护系统、不同业务系统、不同区域的系统、不同运营者的系统之间互操作、数据交换和信息流应设置访问控制措施，避免越权访问行为；
2. 应对控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区的未授权设备进行动态发现及管控，实时监测并阻断非授权设备的接入，仅允许通过运营者授权的软硬件运行；
3. 针对业务系统间数据交互制定访问控制策略，细化至端口级别。
	* 1. 安全审计

控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区的系统应记录系统运行状态、日常操作、故障维护操作、远程运维等日志。

1. 启用服务器主机操作系统日志审计功能，或采用第三方安全审计产品实现主机安全审计功能；
2. 审计范围覆盖服务器和重要客户端上的每个操作系统用户；
3. 审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；
4. 日志数据留存时间不少于6个月。
	1. 安全计算环境
		1. 鉴别与授权

鉴别与授权要求包括：

1. 应明确电力监控系统、调度控制系统等重要业务操作、重要用户操作或异常用户操作行为，并形成业务操作清单，包括相关设备、用户、服务、应用、重要业务数据的访问，并采取技术手段验证关键业务访问行为与业务操作清单的一致性，出现差异应及时修正，避免出现非授权业务操作；
2. 应对设备、用户、服务或应用、数据进行安全管控，对于重要业务操作、重要用户操作或异常用户操作行为，建立动态的身份鉴别方式，或者采用多因子身份鉴别等方式，包括动态口令、数字证书、生物特征等方式，对于关键操作行为应建立二次鉴别机制；
3. 针对重要业务数据资源的操作，应基于安全标记等技术实现访问控制。包括采用安全操作系统和安全数据库，对所有主体和客体设置敏感标记；
4. 应提供专用的或采用统一的登录控制模块对用户进行身份标识和鉴别，鉴别过程应在服务端完成；
5. 应提供用户身份标识唯一性检查功能，保证系统中不存在重复标识的用户；
6. 应避免存在内置匿名账号，依据实名制原则创建账号，保证账号具有可追溯性；
7. 应定期对账号信息进行审计分析，根据账号状态、操作行为等维度设置安全策略；
8. 应提供对用户鉴别信息进行配置和检查的功能，并满足以下要求：

1）应禁止用户配置鉴别口令时与该用户名相同或包含用户名；

2）鉴别口令长度应不少于8位字符，并包含大写字母、小写字母、数字、特殊字符中三种或三种以上的组合；

3）用户口令应定期修改，且修改前后不能一致；

4）应具备连续登录失败处理机制，包括账号自动锁定等；

5）应强制要求新建用户首次登录系统时必须修改初始口令；

6）如采用动态口令、数字证书等密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。

* + 1. 入侵防范

入侵防范要求包括：

1. 生产控制大区和信息管理大区应分别采取技术手段，对网络流量、业务操作、用户操作等行为进行综合分析，提高对高级可持续威胁（APT）等网络攻击行为的入侵防范能力；
2. 生产控制大区和信息管理大区应分别采取技术手段，包括防恶意代码、威胁诱捕、安全沙箱等，实现系统主动防护，采用离线方式及时升级经测试验证过的系统特征库，及时识别并阻断入侵和病毒行为；
3. 检测对重要服务器进行入侵的行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。
	* 1. 自动化工具

自动化工具要求包括：

1. 应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，应在经过验证后及时修补。自动化工具应支持配置信息批量分发，漏洞和补丁的回滚等操作；
2. 扫描应当在非关键业务时段进行并制定详细的回退计划，对于扫描发现的漏洞及配置弱点应及时进行处理；
3. 应定期备份相关设备、用户、服务、应用的重要配置文件，采取技术手段对配置文件的完整性进行保护，并验证配置文件的可恢复性；
4. 应使用自动化工具来支持系统安全功能、安全渗透、代码扫描等测试管理。对于发现的安全问题应及时整改并验证。
	1. 安全建设管理

安全建设管理应满足GB/T 39204-2022中的7.7相关要求。

* 1. 安全运维管理

 安全运维管理应满足GB/T 39204-2022中的7.8相关要求。

* 1. 供应链安全保护

电力行业供应链安全保护应满足GB/T 39204-2022中7.9的相关要求，同时包括：

1. 确保采购、使用的网络产品和服务（如网络安全产品、网络专用设备、社会化云服务、安全检测服务），符合法律、行政法规的规定和相关国家标准的要求；
2. 列入《网络关键设备和网络安全专用产品目录》的设备和产品，确保其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，方可采购；
3. 对于可能影响国家安全的网络产品和服务，采购时确保其按照网络产品和服务安全审查有关法规的要求通过网络安全审查，不应采购审查未通过的网络产品和服务。产品和服务是否影响国家安全由关键信息基础设施安全保护工作部门确定；
4. 采购网络产品和服务时，应明确提供者的安全责任和义务，与网络产品和服务供应商签订协议：安全保密协议，明确供应商的安全责任和义务，做出必要的安全承诺，协议内容应包括安全职责、保密内容、奖惩机制、有效期等。供应商协议，明确产品和服务供应链相关的网络安全风险处理要求。服务级别协议（SLA），明确服务级别可满足关键信息基础设施拟对外提供的服务级别；
5. 当变更供应商时，对供应商变更带来的安全风险进行评估，并采取有关措施对风险进行控制。
	1. 数据安全防护

电力行业数据安全保护应满足GB/T 39204-2022中7.10的相关要求，同时包括：

1. 采取措施确保境内运营中收集和产生的个人信息和重要数据在境内存储，如对个人信息和重要数据的流动情况进行监测；
2. 因业务需要，确需向境外提供的，在数据出境前，自行组织或报请关键信息基础设施保护工作部门，按照个人信息和重要数据出境安全评估办法等相关规定和标准进行安全评估，并对评估结果负责，法律、行政法规另有规定的，依照其规定；
3. 保留对数据的操作记录，增强操作可追溯性；
4. 在可能涉及法律责任认定的应用中，能够基于密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖；
5. 应建立业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。
6. 检测评估
	1. 制度

应建立健全关键信息基础设施安全检测评估制度，包括但不限于针对关基保护对象的检测评估流程、方式方法、周期、人员组织、资金保障等，工业控制系统的专门检测评估流程及方式方法。

* 1. 方式和内容

方式和内容要求包括：

1. 应自行或者委托网络安全服务机构对关键信息基础设施安全性和可能存在的风险，每年可进行两次检测评估，并及时整改发现的问题；
2. 在涉及多个运营者时，应定期组织或参加跨运营者的关键信息基础设施安全检测评估，并及时整改发现的问题；
3. 在检测评估时，通过调研询问、网络采集、工具扫描、搜索引擎等方式，最大限度的收集检测对象的相关信息。信息收集的信息类型包括但不限于：
4. IT资产信息（网络拓扑图、子网划分情况、IP地址清单、相关域名、子域名等）；
5. 安全防护情况（网络安全产品部署情况、安全策略配置情况、安全检测评估报告等）；
6. 产品、服务供应商（软硬件提供商、运维服务提供商、安全服务提供商、网络接入服务商、IDC提供商、DNS服务商、域名注册信息等）；
7. 运营单位和产品服务供应商相关的人员信息（组织架构、岗位设置，人员姓名、手机、邮箱等）。
8. 应检查关键基础设施责任单位组织机构建设情况和人员投入情况，电力行业关键信息基础设施运营者的主要负责人应对关键信息基础设施安全保护负总责，应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；
9. 应检查电力行业单位的关键信息基础设施网络安全专项经费落实情况、关键信息基础设施网络安全教育培训开展情况及网络安全等级保护制度落实情况；
10. 应检查商用密码应用安全性评估情况，包括不限于控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区之间部署的专用加密认证装置等；
11. 应通过深入分析检测关键信息基础设施业务流程，借助流量抓取、协议分析或手工检测等方式，以发现检测对象业务逻辑层面可能存在的安全漏洞和设计缺陷。业务安全测试的内容包括但不限于：越权缺陷、验证缺陷、接口调用缺陷、数据一致性缺陷、任意跳转缺陷等；
12. 应检查电力行业关键信息基础设施数据的使用、加工、传输、提供、公开、销毁等关键环节的数据安全性，应检查数据备份恢复机制的落实情况；
13. 应检查关键信息基础设施供应链安全保护情况，检查软件供应链的开源组件安全情况，检查供应链安全评估机制落实情况；
14. 应检查电力系统关键信息基础设施资产风险清单，检查风险评估定期开展相关报告及记录；
15. 应检查电力系统关键信息基础设施开展应急演练情况、攻防演练情况等，尤其关注关键信息基础设施跨控制区、非控制区、信息管理Ⅲ区、信息管理Ⅳ区之间的信息流动，及其资产的安全防护情况；
16. 在关键信息基础设施发生改建、扩建、所有人变更等较大变化时，应自行或者委托网络安全服务机构进行检测评估，分析关键业务链以及关键资产等方面的变更，评估上述变更给关键信息基础设施带来的风险变化情况，并依据风险变化以及发现的安全问题进行有效整改后方可上线；
17. 应针对特定的业务系统或系统资产，经有关部门批准或授权，采取模拟网络攻击方式，检测关键信息基础设施在面对实际网络攻击时的防护和响应能力；对于电力行业重要工控系统，可采用沙盘模拟攻防演习等方式，检验电力行业关键信息基础设施的安全防护和响应能力；
18. 在安全风险抽查检测工作中，应配合提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务链、网络日志等必要的资料和技术支持，针对抽查检测工作中发现的安全隐患和风险建立清单，制定整改方案，并及时整改。
19. 监测预警
	1. 制度

制度要求包括：

1. 应建立并落实常态化监测预警、快速响应机制，制定自身的监测预警和信息通报制度，确定网络安全预警分级准则，明确监测策略、监测内容和预警流程，对关键信息基础设施的安全风险进行监测预警；
2. 应关注国内外及行业关键信息基础设施安全事件、安全漏洞、解决方法和发展趋势，并对涉及到的关键信息基础设施安全性进行研判分析，必要时发出预警；
3. 应建立网络产品安全漏洞信息管理制度，建立网络产品安全漏洞接收渠道并保持畅通，发现或者获知存在安全漏洞后，应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；
4. 应建立关键信息基础设施的预警信息报告和响应处置程序，明确不同级别预警的报告、响应和处置流程；
5. 应建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
6. 应建立与外部组织之间、与其他运营者之间，以及运营者内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作机制，定期召开协调会议，共同研判、处置网络安全问题；
7. 应建立信息通报机制，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；
8. 应建立网络安全信息共享机制，例如：建立与保护工作部门、同一关键信息基础设施的其他运营者、研究机构、网络安全服务机构、业界专家之间的沟通与合作机制，网络安全共享信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。当网络安全共享信息为漏洞信息时，应符合国家关于漏洞管理制度的要求；
9. 应建立常态值班值守制度，构建网络安全态势感知能力，并与行业部门、公安机关等有关平台对接。
	1. 监测

监测要求包括：

1. 应建立覆盖全部网域的网络安全监测体系，实现全业务、全时域、全区域的全场景安全监测；
2. 应在网络边界、网络出入口、内部重点区域等网络关键节点部署攻击监测、分析设备，发现网络攻击和未知威胁；
3. 应对云平台、数据中台等新型基础设施进行监测，特别是针对云平台内、云平台间、数据中台内的横向流量实施安全检测，发现内部未授权访问或横向攻击威胁；
4. 应对关键业务所涉及的系统进行监测（例如：对不同网络安全等级保护系统、不同区域的系统之间的网络流量进行监测等），对监测信息采取保护措施，防止其受到未授权的访问、修改和删除；
5. 应对电力重要数据和个人信息数据的全生命周期过程进行安全监测，对敏感数据的共享和使用采取可视化方式实施合规监测，对监测信息采取保护措施，防止其受到未授权的访问、修改和删除，支持数据泄露或违规使用的溯源分析；
6. 应分析系统通信流量或事态的模式，建立常见系统通信流量或事态的模型，并使用这些模型调整监测工具参数，以减少误报和漏报；
7. 应全面收集网络安全日志，构建违规操作模型、攻击入侵模型、异常行为模型，强化监测预警能力；
8. 应采用自动化机制，对关键业务所涉及的系统的所有监测信息进行整合分析，以便及时关联资产、脆弱性、威胁等，分析关键信息基础设施的网络安全态势；
9. 关键信息基础设施跨组织、跨地域建设时，应建立覆盖总部和分支机构的多级监测联动平台，构建全面监测、统一指挥、多级联动的态势感知能力；
10. 应将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势。包括：分析不同存储库的审计日志并使之关联；将多个信息系统内多个组件的审计记录关联；将信息系统审计记录信息与物理访问监控的信息关联；将来自非技术源的信息（例如：供应链信息、关键岗位人员信息等）与信息系统审计信息关联；网络安全共享信息的信息关联等；
11. 应通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效，必要时进行更新。
	1. 预警

预警要求包括：

1. 应建立多级预警平台，构建本单位内部预警信息的集中统一管理，支持一点预警、全局感知；
2. 应建立与行业主管机构、安全机构的预警联动能力，支持对外部机构预警系统的对接，实现预警信息的收集、分析与共享；
3. 应将监测工具设置为自动模式。当发现可能危害关键业务的迹象时，能自动报警，并自动采取相应措施，降低关键业务被影响的可能性。例如：恶意代码防御机制、入侵检测设备或者防火墙等弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警；
4. 应对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按照相关部门要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、宜采取的应对措施等；
5. 应能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案。获取的安全预警信息应按照规定通报给相关人员和相关部门；
6. 采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程；
7. 应动态更新优化应急预案，并开展安全教育与宣传。
8. 主动防御
	1. 收敛暴露面

收敛暴露面要求包括：

1. 应识别和减少互联网和内网资产的互联网协议地址、端口、应用服务等暴露面，压缩互联网出口数量；
2. 应减少对外暴露组织架构、邮箱账号、组织通信录等内部信息，防范社会工程学攻击；
3. 不应在公共存储空间（例如：代码托管平台、文库、网盘等）存储可能被攻击者利用的技术文档。例如：网络拓扑图、源代码、互联网协议地址规划等；
4. 应采用最小化原则，仅启用业务访问需要的协议、端口及应用；
5. 应加强访问控制，对网络、业务及系统等的访问限制在最小范围内；
6. 对重要业务系统可采用白名单机制，仅允许可信应用启动，可信端点访问；
7. 应加强对网络安全相关敏感信息进行保护，包括网络拓扑、规划或建设文档等；
8. 应加强网络安全意识，防止社工攻击，对公司组织架构、邮箱账号、员工通信录进行保护；
9. 应加强对内部文档的管理，防止敏感文档扩散到第三方或公共网络空间。
	1. 攻击发现和阻断

攻击发现和阻断要求包括：

1. 应分析网络攻击的方法、手段，针对拒绝服务攻击等各类攻击，采取有针对性的防护策略和技术措施，制定总体技术应对方案；
2. 应针对监测发现的攻击活动，分析攻击路线、攻击目标，设置多道防线，采取捕获、干扰、阻断、封控、加固等多种技术手段，切断攻击路径，快速处置网络攻击；
3. 应及时对网络攻击活动开展溯源，对攻击者进行画像，为案件侦查、事件调查、完善防护策略和措施提供支持；
4. 应系统分析网络攻击意图、技术与过程，进行攻击行为关联分析与还原，并以此改进安全防护策略；
5. 应具备对基于特征的已知威胁的发现及追踪溯源能力；
6. 应具备对基于行为的未知威胁的发现及追踪溯源能力；
7. 应构建网络流量或文件的深度检测系统，通过动态或静态检测，实现对可疑内容的深度检测；
8. 应构建统一安全监测能力，实现对全网或部分区域内的流量日志收集及威胁发现；
9. 应具备攻击处置能力，宜实现对威胁的自动应急处置。
	1. 攻防演练

攻防演练要求包括：

1. 应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，每年至少开展一次实战攻防演练，检验安全防护和应急处置能力；
2. 实战攻防演练应涵盖关键业务及应用场景，演练范畴应包含关键信息基础设施核心供应链、紧密上下游产业链等业务相关单位，提高网络安全防护实战化能力；
3. 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，确保系统安全稳定运行；
4. 应针对攻防演练中发现的安全问题及风险进行及时整改，消除结构性、全局性风险；
5. 对不适用实网演练的场景，可通过搭建仿真平台或沙盘推演的方式进行。
	1. 威胁情报

威胁情报要求包括：

1. 应建立本部门、本单位网络威胁情报共享机制，实现公司不同部门、不同区域及协防单位的情报共享，对新型威胁及时网内排查研判，并研究应对措施；
2. 应建立外部协同网络威胁情报共享机制，与权威网络威胁情报机构开展协同联动，实现跨行业领域网络安全联防联控；
3. 应搭建内部威胁情报系统，具备收集网内威胁情报的能力；
4. 应采用定期更新威胁情报库，及时掌握网外威胁特征及安全热点。
5. 事件处置
	1. 制度

制度要求包括：

1. 应建立网络安全事件管理制度，明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程等，制定应急预案等网络安全事件管理文档，包括公司层面网络安全应急管理规范、应急响应预案、应急培训计划、应急演练计划等。事件处置制度应符合国家联防联控及电力行业相关要求，及时将信息共享给相关方；
2. 应为网络安全事件处置提供相应资源，组织建立专门网络安全应急支撑队伍、专家队伍，应储备相关物资、技术装备，发现不足应及时调整补充，保障安全事件得到及时有效处置；
3. 应按规定参与和配合相关部门开展的网络安全应急演练、应急处置、案件侦办等工作，检查应急预案实用性和可操作性、完善应急储备、强化队伍处置能力、构建相关单位和人员联动机制、提升风险防范意识。
	1. 应急预案和演练

应急预案和演练要求包括：

1. 应在国家网络安全事件应急预案的框架下，根据电力行业负荷减载、电厂和重要变电站安全要求，制定网络安全事件应急预案；
2. 应在应急预案中明确，一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间。应急预案不仅应包括本组织应急事件的处理，也应包括电网间、厂网间的应急事件的处理；
3. 在制定应急预案时，应同所涉及到的运营者内部相关计划（例如：业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足；
4. 应在应急预案中包括非常规时期（重大活动保障）、遭受大规模攻击时等处置流程；
5. 应对网络安全应急预案定期进行评估修订，包括事件分级变动、处置流程完善、人员队伍构成、技术装备指引等；
6. 应每年至少组织开展1次本组织的应急演练，每半年至少开展1次省间或网间的应急演练。关键信息基础设施跨组织、跨地域运行的，应定期组织或参加跨组织、跨地域的应急演练。
	1. 响应和处置

12.3.1事件报告

事件报告要求包括：

1. 电力行业关键信息基础设施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；
2. 当发生有可能危害关键业务的安全事件时，应及时向安全管理机构报告，并组织研判，形成事件报告；
3. 应及时将可能危害关键业务的安全事件通报到可能受影响的内部部门和人员，并按照规定向供应链涉及的、与事件相关的其他组织通报安全事件。

12.3.2 事件处理和恢复

事件处理和恢复要求包括：

1. 应按照事件处置流程、应急预案进行事件处理，恢复关键业务和信息系统到已知的状态；
2. 应按照先应急处置、后调查评估的原则，在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的响应活动被适当记录，便于日后分析。在进行取证分析时，应与业务连续性计划相协调；
3. 在事件处理完成后，应采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理；
4. 在恢复关键业务和信息系统后，应对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键业务和信息系统遭受再次破坏、危害或故障，重点评估应急指挥、应急响应、系统恢复、信息报告等环节。
5. 应收集保存应急处置全过程资料，主动配合评估调查，并对应急处置评估调查报告相关建议和问题进行闭环整改。事件的处置评估工作原则上在应急响应结束后30天内完成；
6. 应开展系统、设备安全隐患排查和治理工作，整理受损系统、设备资料，更新网络拓扑结构和设备台账信息，备份系统数据；
7. 应恢复电力监控系统正常的部署和配置方式，恢复抢修主用系统取代应急响应中的临时措施。对于破坏严重且无法立即恢复的电力监控系统，应制订系统重建方案并实施；
8. 在进行事件处理活动时，应协调组织内部多个部门和外部相关组织，以更好的对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

12.3.3 事件通报

应采用邮件、平台、专用App等技术手段，按照相关规定及时将安全事件及其处置情况进行通报，及时将安全事件及其处置情况通报到可能受影响的部门和相关人员，向供应链涉及的、与事件相关的其他组织提供安全事件信息，并按照法律政策规定报告相关部门。

* 1. 重新识别

应根据检测评估、主动防御、监测预警中发现的安全隐患和发生的安全事件，以及处置结果，结合安全威胁和风险变化情况开展评估，必要时重新开展业务、资产和风险识别工作，并更新安全策略。

1.