ICS 点击此处添加 ICS 号
CCS 点击此处添加中国标准文献分类号

团 体 标 准

T/CNEA XXXX—XXXX

核能行业网络安全等级保护实施指引 第 1 部分：安全通用要求

Implementation guidelines for cybersecurity classified protection in nuclear energy industry-Part 1：Security General requirements

（征求意见稿）

XXXX- XX - XX 发布 XXXX - XX - XX 实施

中国核能行业协会 发布

目　次

前　言

《核能行业网络安全等级保护实施指引》分为六部分构成：

——《核能行业网络安全等级保护实施指引 第1部分：安全通用要求》

——《核能行业网络安全等级保护实施指引 第2部分：云计算安全扩展要求 》

——《核能行业网络安全等级保护实施指引 第3部分：移动互联安全扩展要求》

——《核能行业网络安全等级保护实施指引 第4部分：物联网安全扩展要求 》

——《核能行业网络安全等级保护实施指引 第5部分：工业控制系统安全扩展要求》

——《核能行业网络安全等级保护实施指引 第6部分：大数据安全扩展要求》

本文件为第1部分。本文件作为《核能行业网络安全等级保护实施指引》系列标准的总领，针对共性化保护需求提出要求，保护对象必须根据其安全保护等级实现相应级别的要求。其余各部分文件作为补充针对个性化保护需求提出，保护对象需要根据安全保护等级和其使用的特定技术或特定应用场景选择性实现安全扩展要求。

本文件按照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。本文件发布机构不承担识别这些专利的责任。

本文件由中国核能行业协会提出并归口，技术支持单位为上海核工程研究设计院股份有限公司、核工业标准化研究所、苏州热工研究院有限公司。

本文件起草单位：上海核工程研究设计院股份有限公司、江苏核电有限公司、山东核电有限公司、华能山东石岛湾核电有限公司、中广核智能科技（深圳）有限责任公司、国核自仪系统工程有限公司、杭州木链物联网科技有限公司、深信服科技股份有限公司、华能信息技术有限公司、中国宝原投资有限公司等。

本文件主要起草人： 刘磊、程懿、毛磊、魏国华、郑威、丁海霞、春增军、苏辉、王甲强、崔士柱、马仁贵、杨林、王芙艳、郭云、周书亮、杜昊阳、孙伟、王喆等。

本文件为首次发布。

引　　言

为贯彻《中华人民共和国网络安全法》中明确要求的“国家实行网络安全等级保护制度”的规定，落实、细化核能行业实施网络安全等级保护制度的具体工作，提升核能行业整体网络安全水平，增强应对网络安全威胁的能力，全面开展网络安全建设，编制中国核能行业协会团体系列标准《核能行业网络安全等级保护实施指引》。通过编制《核能行业网络安全等级保护实施指引》系列标准，指导核能行业所属单位执行网络安全等级保护制度、规范网络安全等级保护工作实施操作细节、提升相关单位通过相应级别的网络安全测评的能力，保障核能行业网络安全水平，更好服务于核能行业安全健康发展。

1　范围

本文件主要依据国家《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》标准，结合核能行业特点以及信息系统安全建设需要，对核动力厂及装置（核电厂、核热电厂、核供气供热厂等）的信息安全体系架构采用分区分域设计、对不同等级的应用系统进行具体要求，以保障将国家等级保护要求行业化，具体化，提高核能行业各单位重要网络和信息系统信息安全防护水平。可参考本文件要求进行安全防护的核设施包括：核动力厂以外的研究堆、实验堆、临界装置等其他反应堆；核燃料生产、加工、贮存和后处理设施等核燃料循环设施；放射性废物的处理、贮存、处置设施。

本文件适用于实施信息系统安全等级保护的核能行业机构、测评机构和核能信息系统安全等级保护的主管部门。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的文件，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 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南

GB/T 36958-2018 信息安全技术 网络安全等级保护安全管理中心技术要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069-2010 信息安全技术 术语

3　术语和定义

（1）网络安全　cybersecurity

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。

（2）安全保护能力　security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

（3）物理机　physical machine

是指相对于虚拟机的物理服务器，可为虚拟机提供硬件环境。

（4）敏感数据　sensitive data

是指一旦泄露可能会对用户或机构造成损失的数据，包括但不限于：

a) 用户敏感数据，如用户口令、密钥等；
b) 系统敏感数据，如系统的密钥、关键的系统管理数据；
c) 其他需要保密的敏感业务数据；
d) 关键性的操作指令；
e) 系统主要配置文件；
f) 其他需要保密的数据。

4 缩略语

下列缩略语适用于本文件。

QoS：服务质量（Quality of Service）

TCP：传输控制协议（Transmission Control Protocol）

VPN：虚拟专用网络（Virtual Private Network）

API：应用程序编程接口（Application Programming Interface）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol Secure）

IP：互联网协议（Internet Protocol）

XSS：跨站脚本攻击（Cross-site Scripting）

FTP：文件传输协议（File Transfer Protocol）

HMI：人机界面（Human Machine Interface）

IP：互联网协议（Internet Protocol）

IT：信息技术（Information Technology）

TCB：可信计算基（Trusted Computing Base）

APT：高级可持续威胁攻击（Advanced Persistent Threat ）

5 网络安全等级保护概述

5.1 等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常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，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网(IoT)、工业控制系统和采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

5.2 不同级别的安全保护能力

不同级别的等级保护对象应具备的基本安全保护能力如下：

第一级安全保护能力：应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：略。

5.3 安全通用要求和安全扩展要求

由于业务目标的不同、使用技术的不同、应用场景的不同等因素，不同的等级保护对象会以不同的形态出现，表现形式可能称之为基础信息网络、信息系统（包含采用移动互联等技术的系统）、云计算平台/系统、大数据平台/系统、物联网、工业控制系统等。形态不同的等级保护对象面临的威胁有所不同，安全保护需求也会有所差异。为了便于实现对不同级别的和不同形态的等级保护对象的共性化和个性化保护，等级保护要求分为安全通用要求和安全扩展要求。

安全通用要求针对共性化保护需求提出，等级保护对象无论以何种形式出现，必须根据安全保护等级实现相应级别的安全通用要求；安全扩展要求针对个性化保护需求提出，需要根据安全保护等级和使用的特定技术或特定的应用场景选择性实现安全扩展要求。安全通用要求和安全扩展要求共同构成了对等级保护对象的安全要求。

5.4 核能行业增强性安全要求

本文件新增“核能行业增强性安全要求”，在文本中以粗体表示。核能行业增强性安全要求在结合核能行业相关规定的基础上对等级保护要求进行补充和完善。

6 核能行业总体要求

6.1 总体技术要求

1) 核能行业信息系统安全防护工作应当落实国家信息安全等级保护制度，按照国家信息安全等级保护的有关要求，坚持“安全分区、网络专用、横向隔离、纵向认证”的原则，保障系统的安全运行；

2) 核能行业内部基于计算机和网络技术的业务系统，原则上划分为生产控制大区和管理信息大区。生产控制大区又分为控制区(又称安全区 I）和非控制区(又称安全区 II），管理信息大区是指生产控制大区以外的电力企业管理业务系统的集合。

3) 管理信息大区网络与生产控制大区网络应物理隔离；两网之间有信息通信交换时应部署符合电力系统要求的单向隔离装置；

4) 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；

5) 管理信息大区网络可进一步划分为内部网络和外部网络，两网之间有信息通信交换时防护强度应强于逻辑隔离；

6) 具有层次网络结构的单位可统一提供互联网出口；

7) 二级系统可统一成域，三级和四级系统单独成域；三级和四级系统域均由独立子网承载，每个域有唯一网络边界，应在网络边界处按照等保要求重点进行安全防护。

6.2 总体管理要求

1) 如果本单位管理信息大区和生产控制大区含有二级及以下等级信息系统时，通用管理要求等同采用二级；

2) 如果本单位管理信息大区和生产控制大区含有三级及以下等级信息系统时，通用管理要求等同采用三级；

3) 如果本单位管理信息大区和生产控制大区含有四级及以下等级信息系统时，通用管理要求等同采用四级。

6.3 组织架构与职责

在核能行业中开展网络安全等级保护工作会涉及到集团总部，发电站以及各成员单位的多个部门，首先应明确由核电企业网络安全工作的委员会或领导小组负责 IT 系统网络安全与工业控制系统网络安全领导工作，其最高领导由单位主管领导委任或授权；同时设立独立的负责工业控制系统网络安全管理工作的职能部门，设立工业控制系统安全主管及负责各个方面安全管理工作的安全管理员岗位；安全管理机构必须经各工业控制系统责任部门领导联合审查，以保证各部门领导对各自的责任有一致的理解，并明确所有重要职能。

同时应定义部门及各个工作岗位的职责，设立系统管理、安全管理、审计管理等网络岗位，并配备一定数量的系统管理员、安全管理员和审计管理员等，坚持特权岗位不可兼任原则。

7 第一级安全要求

略。

8 第二级安全要求

8.1 技术要求

8.1.1 安全物理环境

1） 物理位置的选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；

c) 机房场地应选择在具有抗核辐射的建筑内。

2） 物理访问控制

本项要求包括：

a) 机房出入口应安排专人 **24 小时值守**或配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 应对机房划分区域进行管理，如将机房划分为生产区、辅助区，其中生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域；

c) 生产环境机房应增加双因子或多因子认证鉴别方式，如指纹设备加密码、人脸识别加密码。

3） 防盗窃和防破坏

本项要求包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处。

4） 防雷击

本项要求包括：

应将各类机柜、设施和设备等通过接地系统安全接地。

5） 防火

本项要求包括：

a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；相关消防设备如灭火器等应定期检查，确保防火措施有效；

b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c) 机房内部通道设置、装饰材料、设备线缆等应满足消防要求，并通过消防验收。

6） 防水和防潮

本项要求包括：

a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

c） 机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房,与主机房相关的给排水管道必须有可靠的防渗漏措施；

7） 防静电

本项要求包括：

应采用防静电地板或地面并采用必要的接地防静电措施。

8） 温湿度控制

本项要求包括：

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

9） 电力供应

本项要求包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；

c） 机房重要区域、重要设备应提供 UPS 单独供电。

10） 电磁防护

本项要求包括：

电源线和通信线缆应隔离铺设，避免互相干扰。

8.1.2 安全通信网络

1） 网络架构

本项要求包括：

a） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

c） 网络区域和业务情况选择通过防火墙实现逻辑隔离或网闸设备实现物理隔离；

d） 生产区域应单独组网，核心生产区域与其他生产区域采用单向数据传输的方式进行组网。

e） 应保证网络各个部分的带宽满足业务高峰需要。

f） 应绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运

行情况相符。

2） 通信传输

本项要求包括：

应采用校验技术保证通信过程中数据的完整性。

3） 可信验证

本项要求包括：

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.3 **安全区域边界**

1） 边界防护

本项要求包括：

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

b） 可采用防火墙、正反向隔离装置等边界安全设备实现相关的访问控制功能。

2） 访问控制

本项要求包括：

a） 应在网络边界或区域之间根据访问控制策略设置**防火墙**访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

e） 对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；

f） 应定期检查并锁定或撤销网络设备中不必要的用户账号；

g） 地方发电生产控制大区的拨号访问服务，服务器和客户端均应使用经安全加固的达到国家二级等级保护要求的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。

3） 入侵防范

本项要求包括：

a） 应在关键网络节点处部署**入侵检测设备或 APT 安全设备**监视网络攻击行为；

b） 应在生产网络关键网络节点处针对工控协议实现检测、防止或限制生产网络发生的攻击行为。通常可采用工控防火墙、工控流量审计等设备实现要求。

4） 恶意代码防范

本项要求包括：

应在关键网络节点处通过**防毒墙设备**对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5） 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点**部署综合日志审计设备**进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，保存时间不少于六个月；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d) 应在生产控制大区部署专用审计系统，或启用设备或系统审计功能，应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

6） 可信验证

本项要求包括：

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.4 **安全计算环境**

1） 身份鉴别

本项要求包括：

a) 应对**网络设备、安全设备、操作系统和应用程序**登录的用户进行身份标识和鉴别，鉴别**口令应在 8 位以上，由字母、数字、符号等混合组成并定期更换**，身份标识具有唯一性，

b) **网络设备、安全设备、操作系统和应用程序**应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 当进行远程管理时，应使用**基于国密算法的加密技术**防止鉴别信息在网络传输过程中被窃听。

d) 在生产环境中应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用国密密码技术来实现。

2） 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限；

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

e) **重要生产系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。**

3） 安全审计

本项要求包括：

a) 应**部署综合日志审计设备**，启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，保存时间不少于 6 个月；

d) **应在生产区域加强安全审计，审计不仅应该包含每个用户，对于重要系统进程事件、网络事件、注册表事件等系统进行审计。保存时间不少于 6 个月**；

e) **审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性**。

4） 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应通过**主机防火墙**关闭不需要的系统服务、默认共享和高危端口；

c) 应通过**堡垒机**设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e) 应**定期进行漏洞扫描**，发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞，**或采取修改、关停服务，限定访问等方式降低风险；**

f) **针对生产环境应提供持续检测能力，保证网络安全是在动态环境下的持续的监控，在面对 APT 攻击时能够更有效的防范。**

5） 恶意代码防范

本项要求包括：

a) 应**安装企业级防恶意代码软件**或配置具有相应功能的软件，并定期统一进行升级、管理和更新防恶意代码库；

b) **对与外网完全物理隔离的生产环境中部分设备如果确实无法安装防恶意代码软件，可通过在网络层部署恶意代码防范设备，加强 USB 介质管控等措施来适当降低风险等级，并配合免安装的恶意代码查杀工具来满足要求；**

6） 可信验证

本项要求包括：

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7） 数据完整性

本项要求包括：

应采用校验技术保证重要数据在传输过程中的完整性。

8） 数据备份恢复

本项要求包括：

a） 应提供重要数据的本地数据备份与恢复功能；

b） 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地；

c） 应提供数据恢复有效性的验证，保证数据恢复的效率和可行性。

9） 剩余信息保护

本项要求包括：

a） 应保证鉴别信息所在的存储空间被释放**并进行多次复写**或重新分配前得到完全清除；

b） 对于生产数据的存储报废进行物理破坏，确保数据无法正常恢复。

10） 个人信息保护

本项要求包括：

a） 应仅采集和保存业务必需的用户个人信息；

b） 应禁止未授权访问和非法使用用户个人信息；

8.1.5 安全管理中心

1） 系统管理

本项要求包括：

a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c） 应定期对设备运行状况进行检查，定期检验设备的软件版本信息，并留存记录；

2） 审计管理

本项要求包括：

a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b） 应通过**综合审计系统、数据库审计系统**对审计管理员的审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

8.2 **管理要求**

8.2.1 **安全管理制度**

1） 安全策略

本项要求包括：

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等；

2） 管理制度

本项要求包括：

a) 应对安全管理活动中重要的管理内容建立安全管理制度，**安全管理活动对象包括物理、网络、主机系统、数据、应用、建设和运维等内容。**

b) 应对安全管理人员或操作人员执行的日常管理操作建立操作规程，**编写完善的操作规程类文档，如系统维护手册和用户操作规程等。**

c) **地方应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力二次系统安全管理制度，制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等， 并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机 及数据网络的安全管理；**

3） 制定和发布

本项要求包括：

a) **由集团网络安全工作的委员会负责制定适用全机构范围安全管理制度，各单位网络安全工作的委员会负责制定适用辖内安全管理制度；**

b) **应指定或授权专门的部门或者人员负责对安全管理制度的落实进行监督；**

c) **安全管理制度应通过正式、有效的方式发布，并进行版本控制。应注意格式要求、版本编号等并通过正式有效的方式收发，如正式发文、领导签署、单位盖章等。**

4） 评审和修订

本项要求包括：

a) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；

b) **应由信息/网络安全主管定期进行论证和审定，并形成记录。**

8.2.2 **安全管理机构**

1） 岗位设置

本项要求包括：

a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义

各负责人的职责；

b) 网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理；

c) 除信息化主管部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的网络安全管理工作，协同信息化主管部门开展网络安全管理工作；

d) 应设立系统管理员、审计管理员、和安全管理员等岗位，并定义部门及各个工作岗位的职责。

e) 应明确由主管安全生产的领导作为电力二次系统安全防护的主要责任人。

2） 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；

b) 安全管理员不能兼任网络管理员、系统管理员、数据库管理员等。

3） 授权和审批

本项要求包括：

a) **应编写部门职责文档明确各部门审批事项、编写岗位职责文档明确各岗位审批事项。**应根据各个部门和岗位的职责明确授权审批部门及批准人等。

b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程，**应形成审批记录表单**。

c) **接入电力调度数据网络的节点、设备和应用系统，其接入技术方案和安全防护措施须经负责本级电力调度数据网络的调度机构核准。**

4） 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议**形成会议记录**。共同协作处理网络安全问题；

b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

5） 审核和检查

本项要求包括：

应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，**并形成检查记录表单。**

8.2.3 安全管理人员

1） 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用；

b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查；

c) 应制定管理制度类文档和记录表单，内容包括学历、学位要求，安全背景、专业资质，技术人员专业技术水平，管理人员安全管理知识等；

d) 应对网络安全管理人员应实行备案管理。网络安全管理人员的配备和变更情况，应及时报上级机构备案；

e) 凡是因违反国家法律法规和核能机构有关规定受到过处罚或处分的人员，不得从事网络安全管理工作。

f) 应与安全管理员、系统管理员、网络管理员等关键岗位的人员签署保密协议。

2） 人员离岗

本项要求包括：

应及时终止离岗人员的所有访问权限**并形成登记记录表单**，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

3） 安全意识教育和培训

本项要求包括：

a) 应制定安全教育和培训计划；

b) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，并告知相关的安全责任和惩戒措施；

c) 应制定定安全教育培训计划的内容包括培训周期、培训方式、培训内容、考核方式、安全责任、惩戒措施等。

d) 每年至少对网络安全管理人员进行一次网络安全培训。

4） 外部人员访问管理

本项要求包括：

a) 应指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同，并登记备案；

b) 应制定人员访问管理制度类和记录表单，明确访问范围、进入条件、访问控制措施，并记录批准签字、重要区域进入时间、离开时间、访问区域、陪同人员等内容。

c) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案；

d) 应制定管理记录表单，明确申请审批流程，并记录批准签字、权限、时限、账户等内容；

e) 获得外部人员访问授权的所有机构和个人应与核能机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，不得复制和泄漏核能机构的任何信息；

f) 外部人员进入核能机构现场实施时，应事先提交计划操作内容，核能机构人员应在现场陪同外部人员，核对操作内容并记录；

g) 外部人员离场后应及时清除其所有的访问权限。

h) 应制定管理制度记录表单，明确外部人员离场后及时清除其所有的访问权限，并记录访问权限清除时间。

8.2.4 **安全建设管理**

1） 定级和备案

本项要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c) 应保证定级结果经过相关部门的批准；

d) **应确保信息系统的定级结果经过行业信息安全主管部门批准，**方可到公安机关备案。

2） 安全方案设计

本项要求包括：

i) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施，编写安全规划设计方案；

a) 应根据保护对象的安全保护等级进行安全方案设计；

b) 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并经过上级信息安全主管部门和相应电力调度机构的审核，方案实施完成后应当由相关机构共同组织验收。

3） 产品采购和使用

本项要求包括：

a) 应确保网络安全产品采购和使用符合**《网络关键设备和网络安全专用产品目录》**要求；

b) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；

c) 扫描、检测类网络安全产品应报本机构信息化主管部门批准、备案；

d) 扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的网络管理员使用；

e) 应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告；

f) 应定期对各类网络安全产品产生的日志和报表进行备份存档；

g) 应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。

h) 接入电力二次系统生产控制大区中的安全产品，其功能、性能应获得国家或行业指定机构安全检测证明，其电磁兼容性还需有电力系统电磁兼容检测证明。

4） 自行软件开发

本项要求包括：

a） 应将开发环境与实际运行环境物理分开；

b） 应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；

c） 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；

d） 应具备软件安全测试报告和代码审计报告。

5） 外包软件开发

本项要求包括：

a） 应在软件交付前检测其中可能存在的恶意代码，**具备交付前的恶意代码检测报告**；

b） 应保证开发单位提供软件设计文档和使用指南，**具备分析说明书、软件设计说明书、软件操作手册或使用指南等；**

c） 应定期对外包服务活动和外包服务商的服务能力进行审核和评估；

d） 应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；

e） 应禁止外包服务商转包并严格控制分包，保证外包服务水平；

f） 应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行；

g） 应在外包开发合同中明确开发单位、供应商所提供的电力二次设备及系统应包含保密、生命周期、禁止关键技术和设备扩散等方面的条款；

h） 外包开发的软件应在本单位存有源代码备份，并已通过软件后门等安全性检测。

6） 工程实施

本项要求包括：

a） 应指定或授权专门的部门或人员负责工程实施过程的管理；

b） 应制定安全工程实施方案控制工程实施过程，**编写记录表单，记录工程时间限制、进度控制、质量控制等方面内容，阶段性文件等。**

7） 测试验收

本项要求包括：

a） 应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b） 应明确说明参与测试的部门、人员、测试验收内容、现场操作过程以及相关部门和人员的审定意见；

c） 应进行系统上线前的安全性测试，并出具安全测试报告；

d） 对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系

统及数据恢复、生产系统审核等计划，确保生产系统的安全。

8） 系统交付

本项要求包括：

a） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b） 建设单位应在完成建设任务后将提供建设过程文档和运行维护文档，**并将建设过程文档和运维文档全部移交信息化主管部门；**

c） 外部建设单位应与核能机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开；

d） 应对负责运行维护的技术人员进行相应的技能培训，形成培训记录，包括培训内容、培训时间和参与人员等。

e） 应提供建设过程文档和运行维护文档。

9） 等级测评

本项要求包括：

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改，应留存等级测评报告和安全整改方案。

b） 应在发生重大变更或级别发生变化时进行等级测评；

c） 应确保测评机构的选择**公安部认可的《全国等级保护测评机构推荐目录》中的测评单位进行等级测评，并与测评单位签订安全保密协议。**

10） 服务供应商选择

本项要求包括：

a） 应确保服务供应商的选择符合国家的有关规定；

b） 选择服务供应商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；

c） 应与选定的安全服务商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

8.2.5 **安全运维管理**

1） 环境管理

本项要求包括：

a） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

b） 机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；

c） 应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理；**填写机房值班记录、巡视记录**；

d) **机房人员进出机房必须使用主管部门制发的证件；**

e) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；**

f) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；**

g) **机房出入口和内部应安装 7*24 小时录像监控设施，录像至少保存一周；**

h) **机房应设置弱电井，并留有可扩展空间；**

i) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

2） 资产管理

本项要求包括：

应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

3） 介质管理

本项要求包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

b) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；**

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；

d) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开；如是电子文档则应采用 OA 等电子化办公审批平台进行管理；**

e) **对载有敏感信息存储介质的销毁，应报有关部门备案，由信息化主管部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在核能机构内部使用的情况，否则应进行信息的不可恢复性销毁；**

f) **应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；**

g) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；**

h) **应建立生产控制大区移动存储介质安全管理制度，对移动存储介质的使用进行严格限制；**

i) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。**

4） 设备维护管理

本项要求包括：

a) **各机构信息化主管部门负责对网络系统相关的**各种设备（包括备份和冗余设备）、线路等定期进行维护管理；

b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

c） **新购置的设备应经过测试，测试合格后方能投入使用；**

d） **应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；**

e） **需要废止的设备，应由信息化主管部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到核能机构以外的单位，应由信息化主管部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理；**

f） **设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息；**

g） **应制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容。**

5） 漏洞和风险管理

本项要求包括：

应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

6） 网络和系统安全管理

本项要求包括：

a） 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c） 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、重要文件备份等方面作出规定；

d） 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f） **应对网络环境运行状态进行巡检，巡检应保留记录，并有操作和复核人员的签名；**

g） **应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构的信息化主管部门核准，提请被访问机构信息化主管部门开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；**

h） **各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经核能机构信息化主管部门批准，不得在机构内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；**

i） **网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经信息化主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络；**

j） **系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门同意，并详细记录维护信息过程；**

k） 每年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补。

7） 恶意代码防范管理

本项要求包括：

a） 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b） 应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；

c） 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

8） 配置管理

本项要求包括：

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。

9） 密码管理

本项要求包括：

a） 应遵循密码相关国家标准和行业标准；

b） 应使用国家密码管理主管部门认证核准的密码技术和产品；

c） 应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工；

d） 系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求。

10） 变更管理

本项要求包括：

a） 应确明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b） 变更前应做好系统和数据的备份。风险较大的变更，应在变更后对系统的运行情况进行跟踪。

11） 备份与恢复管理

本项要求包括：

a） 应规定备份信息的备份方式、备份频度、存储介质和保存期等；

b） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等；

c） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

d） 恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质；

e） 应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练。

12） 安全事件处置

本项要求包括：

a） 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过 程，总结经验教训；

d） 应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。

13） 应急预案管理

本项要求包括：

a） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

b） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

c） 应急领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；

d） 突发事件应急处置领导小组统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报上级监管部门；

e） 应定期对原有的应急预案重新评估，并根据安全评估结果，定期修订、演练，并进行专项内部审计。

14） 外包运维管理

本项要求包括：

a） 应确保外包运维服务商的选择符合国家的有关规定；

b） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

9 第三级安全要求

9.1 技术要求

9.1.1 安全物理环境

1） 物理位置的选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，如果不可避免，应采取有效防水措施。

c) 机房应避开火灾危险程度高的区域，周围 100 米内不得有加油站、煤气站等危险建筑和重要军事目标；

d) 机房场地应选择在具有抗核辐射的建筑内。

2） 物理访问控制

本项要求包括：

a) 机房出入口应安排专人 **24 小时**值守或配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 需进入机房的来访人员应经过申请和审批流程，由专人陪同，并限制和监控其活动范围,对于重要区域还应限制来访人员携带的随身物品；

c) 应对机房划分区域进行管理（如将机房划分为核心区、生产区、辅助区等），在重要区域前设置交付或安装等过渡区域，其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备或系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域。

d) 生产环境机房应增加双因子或多因子认证鉴别方式，如指纹设备加密码、人脸识别加密码。

3） 防盗窃和防破坏

本项要求包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b) 应将通信线缆铺设在隐蔽安全处，**可架空铺设在地板下或置于管道中，强弱电需隔离铺设并进行统一标识；**

c) 非 7*24 小时人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置；

d) 应建立机房视频监控系统和动环监控系统，能进行 24 小时连续监视，并对监控内容进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设施，视频监控记录至少保存三个月，门禁系统出入记录至少保存六个月。

4） 防雷击

本项要求包括：

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

b） 机房所在建筑应设置防直击雷装置。装设避雷针、避雷线、避雷网、避雷带等避雷装置，定期对防雷设施进行维护和防雷检测；

c） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；

d） 机房应设置直流地、交流工作地、安全保护地、防雷保护地。

5） 防火

本项要求包括：

a） 机房应设置有效的**自动灭火系统，能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位**通过烟感、温感等多种方式自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施

d） 机房应设置自动消防报警系统，并备有一定数量的对电子设备影响小的手持式灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发；

e） 机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内；

f） 主机房宜采用管网式洁净气体灭火系统也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器；

g） 应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练；

h） 机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上应设置显著的消防标志。

6） 防水和防潮

本项要求包括：

a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

c） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

d） 为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。

7） 防静电

本项要求包括：

a） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

b） 应采用防静电地板或地面并采用必要的接地防静电措施；

c） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等；

d） **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。**

8） 温湿度控制

本项要求包括：

a） 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

b） 机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求；

c） 空调系统的主要设备应有备份，空调设备在容量上应有一定的余量；

d） 安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料；

e） 采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施；

f） 设备开机时主机房的温、湿度应执行 A 级，基本工作间可根据设备要求按 A，B 两级执行，其他辅助房间应按设备要求确定。开机时计算机机房内的温、湿度，应符合下表的规定。

项目	级别		
	A 级		B 级
	夏天	冬天	全年
温度	23±1℃	20±2℃	18~28℃
相对湿度(开机时)	40%~55%		35%~75%
相对湿度(停机时)	40%~70%		20%~80%
温度变化率	<5℃/h 并不得结露		<10℃/h 并不得结露

9） 电力供应

本项要求包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应（**如备用发电机**），至少满足设备在断电情况下的正常运行要求，**每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用；**

c） 机房重要区域、重要设备应提供 UPS 单独供电，UPS 供电系统的冗余方式应采用 N+1、N+2、2N、2(N+1) 等方式。没有建立柴油发电机应急供电系统的单位，UPS 后备时间至少 1 小时；

d） 应设置冗余或并行的电力电缆线路为计算机系统供电；**保障断电情况下，一定时间内系统可正常运行或保障数据存储完整的；**

e） 机房内要求采用机房专用插座，市电、UPS 电源插座分开，满足负荷使用要求；

f） **计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接；**

g） 机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。

10） 电磁防护

本项要求包括：

a） 电源线和通信线缆应隔离铺设，避免互相干扰。

b） 应对关键设备实施电磁屏蔽；

c） 计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。

9.1.2 安全通信网络

1） 网络架构

本项要求包括：

a） 应保证网络设备的业务处理能力满足业务高峰期需要；

b） 应保证网络各个部分的带宽满足业务高峰期需要；

c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，**提供相关网络设备的配置信息，验证划分的网络区域是否与划分原则一致；**

d） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应**通过防火墙实现逻辑隔离或网闸设备实现物理隔离；**

e） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性；

f） 主要网络设备业务处理能力能满足业务高峰期需要的 1 倍以上，双线路设计时，宜由不同的服务商提供；

g） 应将生产区域单独组网，核心生产区域与其他生产区域采用单向数据传输的方式进行组网。

h） 单个系统应单独划分安全域，系统由独立子网承载，每个域的网络出口应唯一；

i） 采用冗余技术设计网络拓扑结构，提供主要网络设备、通信线路的硬件冗余,避免关键节点存在单点故障。

2） 通信传输

本项要求包括：

a） 应采用**基于国密算法**的校验技术保证通信过程中数据的完整性；

b） 应采用**基于国密算法**的密码技术保证通信过程中数据的保密性。**如设备上开启基于国密算法的 SSH 或 HTTPS 协议或创建加密通道，通过这些加密方式传输敏感信息**；

3） 可信验证

本项要求包括：

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

9.1.3 安全区域边界

1） 边界防护

本项要求包括：

a) 应保证跨越边界的访问和数据流通过**防火墙、网闸**等边界设备提供的受控接口进行通信。

b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制；**应可采用能够对违规内联行为进行检查、定位和阻断的安全准入产品实现要求；**

a) 应能够对内部用户非授权联到外部网络的行为进行检查或限制，**应采用能够对违规外联行为进行检查、定位和阻断的主机安全管理产品实现要求；如机房、网络等环境可控，非授权外联可能较小，相关设备上的 USB 接口、无线网卡等有管控措施，能对网络异常进行监控及日志审查**；

b) 应限制无线网络的使用，**内部核心网络不应与无线网络互联，无线覆盖区严格受控，仅有授权人员方可进入覆盖区域，对无线接入有严格的管控及身份认证措施**，保证无线网络通过受控的边界设备接入内部网络。

2） 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置**防火墙**访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

e) 应对进出网络的数据流通过应用层访问控制能力的网关设备实现基于应用协议和应用内容的访问控制；

f) 网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；

g) 应定期检查并锁定或撤销网络设备中不必要的用户账号；

h) 应按用户对系统的最小访问权限决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。以拨号或 VPN 等方式接入网络或管理信息大区内访问资源，应采用强认证方式，并需根据访问终端、网络环境、用户行为的风险变化灵活收敛或限制用户权限，实现持续信任评估、最小化动态权限控制；

i) 在网络出口和核心网络接口处应限制网络最大流量数及网络连接数。

3） 入侵防范

本项要求包括：

a) 应在关键网络节点处部署**入侵防护设备、抗 APT 攻击设备、网络回溯系统**检测、防止或限制从外部发起的网络攻击行为；

b) 应在关键网络节点处**部署抗 APT 攻击设备**检测、防止或限制从内部发起的网络攻击行为；

c) 应**部署抗 APT 攻击设备**对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析，**并通过网络侧、终端侧自动化关联分析对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应**；

d) **入侵检测设备、APT 检测设备**检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警；

e) 应在生产网络关键网络节点处针对工控协议实现检测、防止或限制生产网络发生的攻击行为。通常可采用工控防火墙、工控流量审计等设备实现要求。

4） 恶意代码防范和垃圾邮件防范

本项要求包括：

a) 应在关键网络节点处通过**防毒墙设备**对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

b) 应在关键网络节点处**部署防垃圾邮件网关**设备对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

5） 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点**部署综合日志审计设备**进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，保存时间不少于六个月；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

6） 可信验证

本项要求包括：

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

9.1.4 安全计算环境

1） 身份鉴别

本项要求包括：

a) 应对**网络设备、安全设备、操作系统和应用程序**登录的用户进行身份标识和鉴别，鉴别**口令应在 8 位以上，由字母、数字、符号等混合组成并定期更换**，身份标识具有唯一性，

b) **网络设备、安全设备、操作系统和应用程序**应具有登录失败处理功能和安全登录设置，应配置并启用（限制登录角色、警示信息）、结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

e) 当进行远程管理时，应使用**基于国密算法的加密技术**防止鉴别信息在网络传输过程中被窃听。

f) 在生产环境中应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用**国密码技术**来实现；

g) 设备通过本地登录方式（非网络方式）维护时，本地物理环境可控，可以采用身份认证服务器、堡垒机使用两种用户名/口令认证措施（两重口令不同）进行认证。

h) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术，对用户的关键操作进行身份鉴别，且其中一种鉴别技术至少应使用**基于国密算法的**密码技术来实现。

2） 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限，**限制或禁用匿名账户、默认账户的访问权限；**

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则，**授权主体管理用户负责配置访问控制策略；**

f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

g) 系统应建立关键账户与权限的关系表；

h) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

3） 安全审计

本项要求包括：

a) 应**部署综合日志审计设备**，启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**保存时间不少于 6 个月；**

d) 应对审计进程进行保护，防止未经授权的中断，**应采取技术手段确保非审计管理员的其他账户无法中断审计进程；**

e) 应在生产区域加强安全审计，审计不仅应该包含每个用户，对于重要系统进程事件、网络事件、注册表事件等系统进行审计；

f) 审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。

4） 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应持续发现、监测并关闭不需要的系统服务、默认共享和高危端口；

c) 应通过**堡垒机**设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

g) 应**定期进行漏洞扫描、持续监测漏洞，及时发现设备、主机、软件供应链中可能存在的漏洞**，并在经过充分测试评估后，及时修补漏洞，**或采取修改、关停服务，限定访问等方式降低风险；**

e) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

f) 针对生产环境应提供持续检测能力，保证网络安全是在动态环境下的持续的监控，在面对 APT 攻击时能够更有效的防范，并对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应；

g) 所有设备应全部专用化，不使用生产设备进行与业务不相关的操作；

5） 恶意代码防范

本项要求包括：

a) 应**安装企业级防恶意代码软件**或主动免疫可信验证机制及时识别入侵和病毒行为，将其有效阻断并定期统一进行升级和更新防恶意代码库；

b) 应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控；

c) 对与外网完全物理隔离的生产环境中部分设备如果确实无法安装防恶意代码软件，可通过在网络层部署恶意代码防范设备，加强 USB 介质管控等措施来适当降低风险等级，并配合免安装的恶意代码查杀工具来满足要求；

6） 可信验证

本项要求包括：

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7） 数据完整性

本项要求包括：

a) 应采用校验技术或密码技术保证重要数据在**采集、**传输、**使用、**和存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b) 在可能涉及法律责任认定的应用中，应采用基于国密算法的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。证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录。

8） 数据保密性

本项要求包括：

应采用基于国密算法的密码技术保证重要数据在**采集**、传输、**使用**、和存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

9） 数据备份恢复

本项要求包括：

a) 应提供重要数据的本地数据备份与恢复功能，采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，数据保存期限依照国家相关规定；

b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地；

c) 系统通信链路、网络设备、安全设备、服务器、存储等应为冗余设计，避免单点故障。对于同城应用级灾难备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到 100 公里；

d) **应对灾难恢复方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果**；

e) 应提供重要数据处理系统的热冗余，**确保数据恢复时间目标在可接受范围内**，保证系统的高可用性。

10） 剩余信息保护

本项要求包括：

a) 应保证鉴别信息所在的存储空间被释放**并进行多次复写**或重新分配前得到完全清除；

b) 对于生产数据的存储报废进行物理破坏，确保数据无法正常恢复；

c) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除；

d) **需要在存储空间保留敏感数据，相关敏感数据进行了有效加密/脱敏处理的，且有必要的提示信息。**

e) **应关闭或拆除主机的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的必须通过安全管理平台实施严格管理。**

11） 个人信息保护

本项要求包括：

a) 应仅采集和保存业务必需的用户个人信息；

b) 应禁止未授权访问和非法使用用户个人信息，**禁止在未授权和未脱敏情况下将用户信息提交给第三方处理或用于其他业务用途。**

9.1.5 安全管理中心

1） 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c) 应定期对设备运行状况进行检查；

d) 应定期检验设备的软件版本信息，并通过有效测试验证进行相应的升级，同时留存测试验证相关记录。

2） 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

b) 应通过**综合审计系统、数据库审计系统对**审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

3） 安全管理

本项要求包括：

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计，**包括根据安全策略对审计记录进行存储、管理和查询等**；

b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统 一安全标记，对主体进行授权，配置可信验证策略等。

4） 集中管控

本项要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

b) 应**采用安全方式（如 SSH、Https、IPsec VPN 等）**能够建立一条安全的信息传输路径，**使用独立的带外管理网络**对安全设备或安全组件进行管理；

c) 对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

d) 应**部署日志审计服务器，统一收集各设备的审计数据，进行集中分析**应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

f) **针对网络环境应提供持续检测能力，通过网络侧及终端侧持续关联监测分析，更有效防范各类 APT 攻击，各类安全事件进行识别、报警和分析，并对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应**。

9.2 管理要求

9.2.1 安全管理制度

1） 安全策略

本项要求包括：

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等；

2） 管理制度

本项要求包括：

a) 应对安全管理活动中重要的管理内容建立安全管理制度，**安全管理活动对象包括物理、网络、主机系统、数据、应用、建设和运维等内容**；

b) 应对安全管理人员或操作人员执行的日常管理操作建立操作规程，**编写完善的操作规程类文档，如系统维护手册和用户操作规程等。**

c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

d) **应按照“谁主管谁负责，谁运营谁负责”的原则，建立电力二次系统安全管理制度，制定信息 安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将电力二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理；**

e) **应对安全管理活动中各类管理内容建立安全管理制度，主要包括：门禁管理、人员管理、权限 管理、访问控制管理、防尾随管理、安全防护系统的维护管理、常规设备及各系统的维护管理、 恶意代码的防护管理、审计管理、数据及系统的备份管理、用户口令密钥及数字证书的管理、 培训管理等；**

3） 制定和发布

本项要求包括：

a) **由集团网络安全工作的委员会负责制定适用全机构范围安全管理制度，各单位网络安全工作的委员会负责制定适用辖内安全管理制度；**

b) **应指定或授权专门的部门或者人员负责对安全管理制度的落实进行监督；**

c) **安全管理制度应通过正式、有效的方式发布，并进行版本控制；应注意格式要求、版本编号等并通过正式有效的方式收发，如正式发文、领导签署、单位盖章等。**

4） 评审和修订

本项要求包括：

a) 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；

b) **应由信息/网络安全主管定期进行论证和审定，并形成记录；**

c) **应该建立对门户网站内容发布的审核、管理和监控机制。**

9.2.2 **安全管理机构**

1） 岗位设置

本项要求包括：

a) 应设立**由本机构领导、业务与技术相关部门主要负责人组成的**网络安全工作的委员会或领导小组，

其最高领导由单位主管领导担任或授权**负责协调本机构及辖内信息安全管理工作，决策本机构及辖内信息安全重大事宜；**

b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c) 网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理；

d) 除信息化主管部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的网络安全管理工作，协同信息化主管部门开展网络安全管理工作；

e) 应设立系统管理员、审计管理员、和安全管理员等岗位，并定义部门及各个工作岗位的职责；

f) **应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。**

2） 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；

b) 安全管理员不应兼任网络管理员、系统管理员、数据库管理员等。

3） 授权和审批

本项要求包括：

a) **应编写部门职责文档明确各部门审批事项、编写岗位职责文档明确各岗位审批事项，**应根据各个部门和岗位的职责明确授权审批部门及批准人等。

b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程，**形成审批记录表单**，对重要活动建立逐级审批制度；

c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，**形成审批记录表单**；

d) **用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录；**

e) **应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。**

4） 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议**形成会议记录**，共同协作处理网络安全问题；

b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

5） 审核和检查

本项要求包括：

a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，**并形成检查记录表单；**

b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况，**形成检查记录表单**等；

c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上级机构备案；**

d) **应制定违反和拒不执行安全管理措施规定的处罚细则。**

9.2.3 **安全管理人员**

1） 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用；

b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

c) 应制定管理制度类文档和记录表单，内容包括学历、学位要求，安全背景、专业资质，技术人员专业技术水平，管理人员安全管理知识等；

d) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；

e) 应对网络安全管理人员应实行备案管理。网络安全管理人员的配备和变更情况，应及时报上级机构备案；

f) 凡是因违反国家法律法规和核能机构有关规定受到过处罚或处分的人员，不得从事网络安全管理工作。

2） 人员离岗

本项要求包括：

a) 应及时终止离岗人员的所有访问权限**并形成登记记录表单**，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

3） 安全意识教育和培训

本项要求包括：

a) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

b) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，并告知相关的安全责任和惩戒措施；

e) **应制定定安全教育培训计划的内容包括培训周期、培训方式、培训内容、考核方式、安全责任、惩戒措施等；**

c) **每年至少对网络安全管理人员进行一次网络安全培训；**

d) 应定期对不同岗位的人员进行技能考核。

4） 外部人员访问管理

本项要求包括：

a) **应指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同，并登记备案；**

b) **应制定人员访问管理制度类和记录表单，明确访问范围、进入条件、访问控制措施，并记录批准签字、重要区域进入时间、离开时间、访问区域、陪同人员等内容。**

c) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案；

d) **应制定管理记录表单，明确申请审批流程，并记录批准签字、权限、时限、账户等内容；**

e) **获得外部人员访问授权的所有机构和个人应与核能机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作，**不得复制和泄漏核能机构的任何信息；

f) **外部人员进入核能机构现场实施时，应事先提交计划操作内容，核能机构人员应在现场陪同外部人员，核对操作内容并记录；**

g) 外部人员离场后应及时清除其所有的访问权限。

h) **应制定管理制度记录表单，明确外部人员离场后及时清除其所有的访问权限，并记录访问权限清除时间。**

9.2.4 安全建设管理

1） 定级和备案

本项要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c) 应保证定级结果经过相关部门的批准；

d) 应将备案材料报主管部门和相应公安机关备案。

2） 安全方案设计

本项要求包括：

a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施，**编写安全规划设计方案；**

b) 应指定和授权专门的部门对网络系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

c) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

d) 应根据保护对象的安全保护等级进行安全方案设计；

e) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

3） 产品采购和使用

本项要求包括：

i) 应确保网络安全产品采购和使用符合**《网络关键设备和网络安全专用产品目录》**要求；

a) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；

b) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

c) **扫描、检测类网络安全产品应报本机构信息化主管部门批准、备案；**

d) 扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的网络管理员使用；

e) 应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告；

f) 应定期对各类网络安全产品产生的日志和报表进行备份存档，保存时间超过 6 个月；

g) 应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。

4） 自行软件开发

本项要求包括：

a) 应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，**不得在程序中设置后门或恶意代码程序**；

b) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

c) 应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；

d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e) 在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性；

f) 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测，**应具备软件安全测试报告和代码审计报告；**

g) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

h) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

5） 外包软件开发

本项要求包括：

i） 应在软件交付前检测其中可能存在的恶意代码；**具备交付前的恶意代码检测报告；**

j） 应保证开发单位提供软件设计文档和使用指南，具备分析说明书、软件设计说明书、软件操作手册或使用指南等；

a） 应定期对外包服务活动和外包服务商的服务能力进行审核和评估；

b） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；

c） 应具备交付前的第三方源代码审查报告或软件安全性测试证明（非源码审核）；

d） 应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；

e） 应禁止外包服务商转包并严格控制分包，保证外包服务水平；

f） **应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行。**

6） 工程实施

本项要求包括：

a） 应指定或授权专门的部门或人员负责工程实施过程的管理；

c） 应制定安全工程实施方案控制工程实施过程，编写记录表单，记录工程时间限制、进度控制、质量控制等方面内容，阶段性文件等。

b） 应通过第三方工程监理控制项目的实施过程；

c） 应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；

d） **系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。**

7） 测试验收

本项要求包括：

a） 应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b） 应明确说明参与测试的部门、人员、测试验收内容、现场操作过程以及相关部门和人员的审定意见；

c） 应进行系统上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容；

d） 新系统上线前，对系统进行安全性评估，及时修补评估过程中发现的问题；

e） 新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行；

f） **对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。**

8） 系统交付

本项要求包括：

a） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

f） 建设单位应在完成建设任务后将提供建设过程文档和运行维护文档，**并将建设过程文档和运维文档全部移交信息化主管部门；**

b） 外部建设单位应与核能机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开；

c） 应对负责运行维护的技术人员进行相应的技能培训，形成培训记录，包括培训内容、培训时间和参与人员等；

d） 应提供建设过程文档和运行维护文档。

9） 等级测评

本项要求包括：

d） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改，应留存等级测评报告和安全整改方案。

a） 应在发生重大变更或级别发生变化时进行等级测评；

b） 应确保测评机构的选择**公安部认可的《全国等级保护测评机构推荐目录》中的测评单位进行等级测评，并与测评单位签订安全保密协议。**

10） 服务供应商选择

本项要求包括：

a） 应确保服务供应商的选择符合国家的有关规定；

b） **选择服务供应商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素**；

c） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；

d） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

9.2.5 安全运维管理

1） 环境管理

本项要求包括：

a） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

b） **机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰**；

c） 应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，**填写机房值班记录、巡视记录**；

d） **机房人员进出机房必须使用主管部门制发的证件；**

e) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；**

f) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；**

g) **机房出入口和内部应安装 7*24 小时录像监控设施，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管录像至少保存一周；**

h) **机房应设置弱电井，并留有可扩展空间；**

i) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

2） 资产管理

本项要求包括：

a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

3） 介质管理

本项要求包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

b) **所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；**

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制；

d) **应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；**

e) **对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开；如是电子文档则应采用 OA 等电子化办公审批平台进行管理；**

f) **对载有敏感信息存储介质的销毁，应报有关部门备案，由信息化主管部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在核能机构内部使用的情况，否则应进行信息的不可恢复性销毁；**

g) **应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；**

h) **应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；**

i) **应制定移动存储介质使用规范，并定期核查移动存储介质的使用情况；**

j) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。**

4） 设备维护管理

本项要求包括：

a) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修

过程的监督控制等；

b) 新购置的设备应经过测试，测试合格后方能投入使用；

c) 各机构信息化主管部门负责对网络系统相关的各种设备（包括备份和冗余设备）、线路等定期进行维护管理；

d) 应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；

e) 需要废止的设备，应由信息化主管部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到核能机构以外的单位，应由信息化主管部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理；

f) 设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息；

g) 应制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。

h) 应确保信息处理设备必须经过审批才能带入机房或办公地点。

5） 漏洞和风险管理

本项要求包括：

a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

b) 应对发现的安全漏洞和隐患进行评估，分析被利用的可能性，判断安全风险的等级，在可接受的范围内进行残余风险评估，明确风险等级；

c) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

6） 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、重要文件备份等方面作出规定；

d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计

日志，操作结束后应删除工具中的敏感数据；

i） **应使用商业化的运维工具，严禁运维人员私自下载第三方未商业化的运维工具；如使用官方正版商用化工具，或自行开发的，安全可控的运维工具，并对于运维工具的接入有严格的控制措施；**

j） 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

k） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为；

l） **应明确所有与外部连接的授权和批准制度，并定期对相关违反行为进行检查，可采取终端管理系统实现违规外联和违规接入，设置合理的安全策略，在出现违规外联和违规接入时能第一时间进行检测和阻断；**

m） **应对网络环境运行状态进行巡检，巡检应保留记录，并有操作和复核人员的签名；**

n） **应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构的信息化主管部门核准，提请被访问机构信息化主管部门开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；**

o） **各机构以不影响正常网络传输为原则，合理控制多媒体网络应用规模和范围，未经核能机构信息化主管部门批准，不得在机构内部网络上提供跨辖区视频点播等严重占用网络资源的多媒体网络应用；**

p） **网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经信息化主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络；**

q） **系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门同意，并详细记录维护信息过程；**

r） **每半年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报。**

7） 恶意代码防范管理

本项要求包括：

a） 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；

b） **应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；**

c） **应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；**

d） **应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防 病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报 表和总结汇报。**

e） 应定期验证防范恶意代码攻击的技术措施的有效性。

8） 配置管理

本项要求包括：

a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

b） 应将基本配置信息改变纳入变更范畴,实施对配置信息改变的控制,并及时更新基本配置信息库。

9） 密码管理

本项要求包括：

a） 应遵循密码相关国家标准和行业标准；

b） 应使用国家密码管理主管部门认证核准的密码技术和产品；

c） 应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工；

d） 系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求；

e） 生产环境重要计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经信息化主管部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放；

f） 密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；

g） 确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。

10） 变更管理

本项要求包括：

a） 应确明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b） 变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪；

c） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

d） 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

e） 变更前做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪；

f） 如果需要在生产环境进行测试或者变更，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全；

11） 备份与恢复管理

本项要求包括：

a） 应规定备份信息的备份方式、备份频度、存储介质和保存期等；

b） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢

复程序等；

c） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

d） 恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质；

e） 应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练；

f） 应定期对备份数据的有效性进行检查，备份数据应实行异地保存；

g） 生产环境应建立灾难备份系统，主备系统实际切换时间应少于 60 分钟，灾备系统处理能力应不低于主用系统处理能力的 50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理能力相同、轮换交替使用的双系统模式。

h） 应建立电力二次系统联合防护和应急机制，负责处置跨部门电力二次系统安全事件。

12） 安全事件处置

本项要求包括：

a） 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过 程，总结经验教训；

d） 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

e） 应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。

13） 应急预案管理

本项要求包括：

a） 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b） 业务处理系统应急预案的编制工作应由相关业务部门和信息化主管部门共同完成，并由预案涉及的相关机构签字盖章；

c） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

d） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

e） 应急领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；

f） 突发事件应急处置领导小组统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报上级监管部门；

g） 在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；

h) **实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度；**

i) **应急演练结束后，应撰写应急演练情况总结报告；总结报告内容应包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。**

j) 应定期对原有的应急预案重新评估，**并根据安全评估结果，定期修订、演练，并进行专项内部审计。**

k) **应制定电力二次系统联合防护和应急处置预案，并经过演练**。

l) **应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次**

14） 外包运维管理

本项要求包括：

a) 应确保外包运维服务商的选择符合国家的有关规定；

b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

10 第四级安全要求

10.1技术要求

10.1.1 安全物理环境

1） 物理位置的选择

本项要求包括：

a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，否则应加强防水和防潮措施；

c) 机房应避开火灾危险程度高的区域，周围 100 米内不得有加油站、煤气站等危险建筑和重要军事目标；

d) 机房场地应选择在具有抗核辐射的建筑内。

2） 物理访问控制

本项要求包括：

a) 机房出入口应安排专人 **24 小时**值守或配置电子门禁系统，控制、鉴别和记录进入的人员；

b) 需进入机房的来访人员应经过申请和审批流程，由专人陪同，并限制和监控其活动范围,对于重要区域还应限制来访人员携带的随身物品；

c) 应对机房划分区域进行管理（如将机房划分为核心区、生产区、辅助区，区域和区域之间设置物理隔离装置），在重要区域前设置交付或安装等过渡区域，其中核心区是指装有关键业务系统服务器、主要通信设备、网络控制器、通讯保密设备和（或）系统打印设备的要害区域，生产区是指放置一般业务系统服务器、客户端（工作站）等设备的运行区域，辅助区是指放置供电、消防、空调等设备的区域；

d) 重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员；

e) 生产环境机房应增加双因子或多因子认证鉴别方式，如指纹设备加密码、人脸识别加密码。

3） 防盗窃和防破坏

本项要求包括：

a) 应将主要设备放置在机房内；

b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

d) 应将通信线缆铺设在隐蔽安全处，可架空铺设在地板下或置于管道中，强弱电需隔离铺设并进行统一标识；

c) 非 7*24 小时人员值守和巡查的机房，主要出入口应安装红外线探测设备等光电防盗设备，一旦发现有破坏性入侵即时显示入侵部位，并驱动声光报警装置；

d) 应建立机房视频监控系统和动环监控系统，能进行 24 小时连续监视，并对监控内容进行记录，监控对象包括机房空调、消防、不间断电源（UPS）、门禁系统等重要设施，视频监控记录至少保存三个月，门禁系统出入记录至少保存六个月。

4） 防雷击

本项要求包括：

a） 应将各类机柜、设施和设备等通过接地系统安全接地；

e） 机房所在建筑应设置防直击雷装置。装设避雷针、避雷线、避雷网、避雷带等避雷装置，定期对防雷设施进行维护和防雷检测；

b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；

c） **机房应设置直流地、交流工作地、安全保护地、防雷保护地。**

5） 防火

本项要求包括：

a） 机房应设置有效的**自动灭火系统，能够通过在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位**通过烟感、温感等多种方式自动检测火情、自动报警，并自动灭火；

b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

c） 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施；

d） 机房应设置自动消防报警系统，并备有一定数量的对电子设备影响小的手持式灭火器。消防报警系统应具有与空调系统、新风系统、门禁系统联动的功能，一般工作状态为手动触发；

e） 机房内所使用的设备线缆应符合消防要求，纸张，磁带和胶卷等易燃物品，要放置于金属制的防火柜内；

f） 主机房宜采用管网式洁净气体灭火系统也可采用高压细水雾灭火系统，应同时设置两种火灾探测器，且火灾报警系统应与灭火系统联动；凡设置洁净气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器；

g） 应定期检查消防设施，每年至少组织各运维相关部门联合开展一次针对机房的消防培训和演练；

h） **机房应设置二个以上消防逃生通道，同时应保证机房内各分区到各消防通道的道路通畅，方便人员逃生时使用。在机房通道上应设置显著的消防标志。**

6） 防水和防潮

本项要求包括：

a） 主机房尽量避开水源，与主机房无关的给排水管道不得穿过主机房,与主机房相关的给排水管道必须有可靠的防渗漏措施

b） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

c） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；

d） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

e） 为便于地下积水的转移，漏水隐患区域地面周围应设排水沟和地漏，当采用吊顶上布置空调风口

时，风口位置不宜设置在设备正上方以避免水蒸气结露和渗透。

7） 防静电

本项要求包括：

a） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

b） 应采用防静电地板或地面并采用必要的接地防静电措施；

c） 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等；

d） **主机房和辅助区内的工作台面宜采用导静电或静电耗散材料。**

8） 温湿度控制

本项要求包括：

a） 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

b） 机房应采用专用空调设备，空调机应带有通信接口，通信协议应满足机房监控系统的要求；

c） 空调系统的主要设备应有备份，空调设备在容量上应有一定的余量；

d） 安装在活动地板上及吊顶上的送风口、回风口应采用难燃材料或非燃材料；

e） 采用空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施；

f） 设备开机时主机房的温、湿度应执行 A 级，基本工作间可根据设备要求按 A，B 两级执行，其他辅助房间应按设备要求确定。开机时计算机机房内的温、湿度，应符合下表的规定。

项目	级别		
	A 级		B 级
	夏天	冬天	全年
温度	23±1℃	20±2℃	18~28℃
相对湿度(开机时)	40%~55%		35%~75%
相对湿度(停机时)	40%~70%		20%~80%
温度变化率	<5℃/h 并不得结露		<10℃/h 并不得结露

9） 电力供应

本项要求包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应（**如备用发电机**），至少满足设备在断电情况下的正常运行要求，**每年需进行备用供电系统的模拟演练，并定期对备用电力供应设备进行检修和维护，确保其能正常使用；**

c） 机房重要区域、重要设备应提供 UPS 单独供电，UPS 供电系统的冗余方式应采用 N+1、N+2、2N、2(N+1) 等方式。没有建立柴油发电机应急供电系统的单位，UPS 后备时间至少 1 小时；

d） 应设置冗余或并行的电力电缆线路为计算机系统供电，输入电源应采用双路自动切换供电方式；**保**

障断电情况下，一定时间内系统可正常运行或保障数据存储完整的；

e） 应提供应急供电设施。

f） 机房内要求采用机房专用插座，市电、UPS 电源插座分开，满足负荷使用要求；

g） 计算机系统应选用铜芯电缆，避免铜、铝混用。若不能避免时，应采用铜铝过渡头连接；

h） **机房应设置应急照明和安全出口指示灯，供配电柜（箱）和分电盘内各种开关、手柄、按钮应标志清晰，防止误操作。**

10） 电磁防护

本项要求包括：

a） 电源线和通信线缆应隔离铺设，避免互相干扰。

b） 应对关键设备和关键区域实施电磁屏蔽；

c） **计算机系统设备网络布线不得与空调设备、电源设备的无电磁屏蔽的布线平行；交叉时，应尽量以接近于垂直的角度交叉，并采取防延燃措施。**

10.1.2 安全通信网络

1） 网络架构

本项要求包括：

a） 应保证网络设备的业务处理能力满足业务高峰期需要；

b） 应保证网络各个部分的带宽满足业务高峰期需要；

c） 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址，**提供相关网络设备的配置信息，验证划分的网络区域是否与划分原则一致；**

d） 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应**通过防火墙实现逻辑隔离或网闸设备实现物理隔离；**

e） 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性；

f） 主要网络设备业务处理能力能满足业务高峰期需要的 1 倍以上，双线路设计时，宜由不同的服务商提供；

g） 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保障重要业务服务的带宽；

h） **应将生产区域单独组网，核心生产区域与其他生产区域采用单向数据传输的方式进行组网。**

2） 通信传输

本项要求包括：

a） 应采用**基于国密算法**校验技术保证通信过程中数据的完整性；

b） 应采用**基于国密算法**的密码技术保证通信过程中数据的保密性。**如设备上开启基于国密算法的 SSH 或 HTTPS 协议或创建加密通道，通过这些加密方式传输敏感信息；**

c） 应在通信前基于密码技术对通信的双方进行验证或认证；

d） 应基于硬件密码模块对重要通信过程进行密码运算和密钥管理，**如使用具备密码技术功能的设备或组件，基于硬件密码模块产生密钥并进行密码运算。**

3） 可信验证

本项要求包括：

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

10.1.3 **安全区域边界**

1） 边界防护

本项要求包括：

c） 应保证跨越边界的访问和数据流通过**防火墙、网闸**等边界设备提供的受控接口进行通信。

d） 应能够对非授权设备私自联到内部网络的行为进行检查或限制；**应可采用能够对违规内联行为进行检查、定位和阻断的安全准入产品实现要求；**

c） 应能够对内部用户非授权联到外部网络的行为进行检查或限制，**应采用能够对违规外联行为进行检查、定位和阻断的主机安全管理产品实现要求；如机房、网络等环境可控，非授权外联可能较小，相关设备上的 USB 接口、无线网卡等有管控措施，能对网络异常进行监控及日志审查**；

d） 应限制无线网络的使用，**内部核心网络不应与无线网络互联，无线覆盖区严格受控，仅有授权人员方可进入覆盖区域，对无线接入有严格的管控及身份认证措施**，保证无线网络通过受控的边界设备接入内部网络。

e） 应**部署终端管理系统**能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断；

f） 应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。

2） 访问控制

本项要求包括：

a） 应在网络边界或区域之间根据访问控制策略设置**防火墙**访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

e） 应对进出网络的数据流通过应用层访问控制能力的网关设备实现基于应用协议和应用内容的访问控制；

f） **应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换**；

j) **网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度；**

k) **应定期检查并锁定或撤销网络设备中不必要的用户账号。**

l) **应按用户对系统的最小访问权限决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。以拨号或 VPN 等方式接入网络或管理信息大区内访问资源，应采用强认证方式，并需根据访问终端、网络环境、用户行为的风险变化灵活收敛或限制用户权限，实现持续信任评估、最小化动态权限控制。**

3） 入侵防范

本项要求包括：

a) 应在关键网络节点处部署**入侵防护设备、抗 APT 攻击设备、网络回溯系统**检测、防止或限制从外部发起的网络攻击行为；

b) 应在关键网络节点处**部署抗 APT 攻击设备**检测、防止或限制从内部发起的网络攻击行为；

c) 应**部署抗 APT 攻击设备**对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析，**并通过网络侧、终端侧自动化关联分析对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应**；

d) **入侵检测设备、APT 检测设备**检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警；

e) **应在生产网络关键网络节点处针对工控协议实现检测、防止或限制生产网络发生的攻击行为。通常可采用工控防火墙、工控流量审计等设备实现要求。**

4） 恶意代码防范和垃圾邮件防范

本项要求包括：

a) 应在关键网络节点处通过**防毒墙设备**对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

b) 应在关键网络节点处**部署防垃圾邮件网关**对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

5） 安全审计

本项要求包括：

a) 应在**生产控制大区、**各网络边界、重要网络节点**部署综合日志审计设备**进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，保存时间不少于六个月；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

6） 可信验证

本项要求包括：

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

10.1.4 **安全计算环境**

1） 身份鉴别

本项要求包括：

a) 应对**网络设备、安全设备、操作系统和应用程序**登录的用户进行身份标识和鉴别，鉴别**口令应在 8 位以上，由字母、数字、符号等混合组成并定期更换，用户名和口令禁止相同，**身份标识具有唯一性；

b) 网络设备标识应唯一；同一网络设备的用户标识应唯一；禁止多个人员共用一个账号；

c) **网络设备、安全设备、操作系统和应用程序**应具有登录失败处理功能和安全登录设置，应配置并启用（限制登录角色、警示信息）、结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

d) 当进行远程管理时，应使用**基于国密算法的加密技术**防止鉴别信息在网络传输过程中被窃听；

e) 在生产环境中应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用**国密码技术**来实现；

f) 设备通过本地登录方式（非网络方式）维护时，本地物理环境可控，可以采用身份认证服务器、堡垒机使用两种用户名/口令认证措施（两重口令不同）进行认证。

g) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术，对用户的关键操作进行身份鉴别，且其中一种鉴别技术至少应使用**基于国密算法的**密码技术来实现。

2） 访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限，**限制或禁用匿名账户、默认账户的访问权限；**

b) 应重命名或删除默认账户，修改默认账户的默认口令；

c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

i) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则，**授权主体管理用户负责配置访问控制策略；**

e) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

j) 系统应建立关键账户与权限的关系表；

f) 应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。

3） 安全审计

本项要求包括：

a） 应**部署综合日志审计设备**，启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b） 审计记录应包括事件的日期和时间、事件类型、主体标识、客体标识和结果等；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，**保存时间不少于 6 个月；**

g） 应对审计进程进行保护，防止未经授权的中断，**应采取技术手段确保非审计管理员的其他账户无法中断审计进程；**

h） 应在生产区域加强安全审计，审计不仅应该包含每个用户，对于重要系统进程事件、网络事件、注册表事件等系统进行审计；

i） **审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。**

4） 入侵防范

本项要求包括：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b） 应持续发现、监测并关闭不需要的系统服务、默认共享和高危端口；

c） 应通过**堡垒机**设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

e） 应**定期进行漏洞扫描、持续监测漏洞，及时发现设备、主机、软件供应链中可能存在的漏洞**，并在经过充分测试评估后，及时修补漏洞，**或采取修改、关停服务，限定访问等方式降低风险；**

f） 针对生产环境应提供持续检测能力，保证网络安全是在动态环境下的持续的监控，在面对 APT 攻击时能够更有效的防范，并对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应；

g） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

h） **所有设备应全部专用化，不使用生产设备进行与业务不相关的操作。**

5） 恶意代码防范

本项要求包括：

a） 应**安装企业级防恶意代码软件**或主动免疫可信验证机制及时识别入侵和病毒行为，将其有效阻断并定期统一进行升级和更新防恶意代码库；

a） 应建立病毒监控中心，对网络内计算机感染病毒的情况进行监控；

b） **对与外网完全物理隔离的生产环境中部分设备如果确实无法安装防恶意代码软件，可通过在网络层部署恶意代码防范设备，加强 USB 介质管控等措施来适当降低风险等级，并配合免安装的恶意代码查杀工具来满足要求。**

6） 可信验证

本项要求包括：

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

7） 数据完整性

本项要求包括：

a） 应采用校验技术或密码技术保证重要数据在**采集、**传输、**使用、**和存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

b） **在可能涉及法律责任认定的应用中，应采用基于国密算法的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。证据包括应用系统操作与管理记录，至少应包括操作时间、操作人员及操作类型、操作内容等记录。**

8） 数据保密性

本项要求包括：

应采用基于国密算法的密码技术保证重要数据在**采集**、传输、**使用**、和存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

9） 数据备份恢复

本项要求包括：

f) 应提供重要数据的本地数据备份与恢复功能，**采取实时备份与异步备份或增量备份与完全备份的方式，增量数据备份每天一次，完全数据备份每周一次，备份介质场外存放，数据保存期限依照国家相关规定；**

a） 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地；

b) 应建立异地灾难备份中心，提供业务应用的实时切换，**对于同城应用级灾难备份中心，应与生产中心直线距离至少达到 30 公里，可以接管所有核心业务的运行；对于异地应用级灾难备份中心，应与生产中心直线距离至少达到 100 公里；**

c） **应对灾难恢复方案中关键技术应用的可行性进行验证测试，并记录和保存验证测试的结果**

g） 应提供重要数据处理系统的热冗余，**确保数据恢复时间目标在可接受范围内**，保证系统的高可用性。

10） 剩余信息保护

本项要求包括：

a） 应保证鉴别信息所在的存储空间被释放**并进行多次复写**或重新分配前得到完全清除；

b) **对于生产数据的存储报废进行物理破坏，确保数据无法正常恢复；**

c） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除；

d) **需要在存储空间保留敏感数据，相关敏感数据进行了有效加密/脱敏处理的，且有必要的提示信息。**

11） 个人信息保护

本项要求包括：

a) 应仅采集和保存业务必需的用户个人信息；

b) 应禁止未授权访问和非法使用用户个人信息，**禁止在未授权和未脱敏情况下将用户信息提交给第三方处理或用于其他业务用途。**

10.1.5 **安全管理中心**

1） 系统管理

本项要求包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

c) 应定期对设备运行状况进行检查；

d) **应定期检验设备的软件版本信息，并通过有效测试验证进行相应的升级，同时留存测试验证相关记录。**

2） 审计管理

本项要求包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；

c) 应通过**综合审计系统、数据库审计系统对**审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；

3） 安全管理

本项要求包括：

a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计，**包括根据安全策略对审计记录进行存储、管理和查询等**；

b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统 一安全标记，对主体进行授权，配置可信验证策略等。

4） 集中管控

本项要求包括：

a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

b) 应**采用安全方式（如 SSH、Https、IPsec VPN 等）**能够建立一条安全的信息传输路径，**使用独立的带外管理网络**对安全设备或安全组件进行管理;

c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

d) 应**部署日志审计服务器，统一收集各设备的审计数据，进行集中分析**应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

f) **针对网络环境应提供持续检测能力，通过网络侧及终端侧持续关联监测分析，更有效防范各类 APT 攻击，各类安全事件进行识别、报警和分析，并对攻击进行全链条溯源，溯源至进程、文件级，保证对攻击入口及攻击根因的有效加固及处置，实现深度检测、精准响应**；

g) 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

10.2**管理要求**

10.2.1 **安全管理制度**

1） 安全策略

本项要求包括：

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

2） 管理制度

本项要求包括：

a) **应按照“谁主管谁负责，谁运营谁负责”的原则，建立核电二次系统安全管理制度，制定网络安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等，并将核电二次系统安全防护及其信息报送纳入日常安全生产管理体系，负责所辖范围内计算机及数据网络的安全管理**

b) 应对安全管理活动中重要的管理内容建立安全管理制度，**安全管理活动对象包括物理、网络、主机系统、数据、应用、建设和运维等内容**；

c) 应对安全管理人员或操作人员执行的日常管理操作建立操作规程，**编写完善的操作规程类文档，如系统维护手册和用户操作规程等。**

d) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

3） 制定和发布

本项要求包括：

a) **由集团网络安全工作的委员会负责制定适用全机构范围安全管理制度，各单位网络安全工作的委员会负责制定适用辖内安全管理制度；**

b) **应指定或授权专门的部门或者人员负责对安全管理制度的落实进行监督；**

c) 安全管理制度应通过正式、有效的方式发布，并进行版本控制，**应注意格式要求、版本编号等并通过正式有效的方式收发，如正式发文、领导签署、单位盖章等。**

d) **有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。**

4） 评审和修订

本项要求包括：

a) 信息安全领导小组应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

b) 应由信息/网络安全主管定期进行论证和审定，并形成记录；

c) 应该建立对门户网站内容发布的审核、管理和监控机制。

10.2.2 **安全管理机构**

1） 岗位设置

本项要求包括：

a) 应明确由主管安全生产的领导作为核电二次系统安全防护的主要责任人，成立指导和管理信息 安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权

b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c) 网络安全管理工作应实行统一领导、分级管理，总部统一领导分支机构的网络安全管理，各机构负责本单位和辖内的网络安全管理；

d) 除信息化主管部门外，其他部门均应指定至少一名部门计算机安全员，具体负责本部门的网络安全管理工作，协同信息化主管部门开展网络安全管理工作；

e) 应设立系统管理员、审计管理员、和安全管理员等岗位，并定义部门及各个工作岗位的职责。

f) **应坚持三分离原则，实现前后台分离、开发与操作分离、技术与业务分离，信息技术人员任职要专岗专责，不得由业务人员兼任，也不得兼任业务职务。**

2） 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、审计管理员和安全管理员等；

b) **安全管理员不应兼任网络管理员、系统管理员、数据库管理员等；**

c) 关键事务岗位应配备多人共同管理。

3） 资金保障

本项要求包括：

a) 应保障落实核电二次系统安全建设、运维及等级保护测评资金等；

b) **系统建设资金筹措方案和年度系统维护经费应包括信息安全保障资金项目。**

4） 授权和审批

本项要求包括：

a) **应编写部门职责文档明确各部门审批事项、编写岗位职责文档明确各岗位审批事项，**应根据各个

部门和岗位的职责明确授权审批部门及批准人等。

b) 应针对系统变更、重要操作、物理访问和系统接入等事项执行审批过程，**形成审批记录表单**，对重要活动建立逐级审批制度；

f) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，**形成审批记录表单**；

c) **用户应被授予完成所承担任务所需的最小权限，重要岗位的员工之间应形成相互制约的关系。权限变更应执行相关审批流程，并有完整的变更记录；**

d) **应建立系统用户及权限清单，定期对员工权限进行检查核对，发现越权用户要查明原因并及时调整，同时清理过期用户权限，做好记录归档。**

5） 沟通和合作

本项要求包括：

a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议**形成会议记录**，共同协作处理网络安全问题；

b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；

c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；

d) **应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。**

6） 审核和检查

本项要求包括：

a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况，**并形成检查记录表单；**

b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况，**形成检查记录表单**等；

c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，**要求限期整改的需要对相关整改情况进行后续跟踪，并将每次安全检查报告和整改落实情况整理汇总后，对安全检查结果进行通报并报上级机构备案；**

d) **应制定违反和拒不执行安全管理措施规定的处罚细则。**

10.2.3 **安全管理人员**

1） 人员录用

本项要求包括：

a) 应指定或授权专门的部门或人员负责人员录用；

g) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；

h) 应制定管理制度类文档和记录表单，内容包括学历、学位要求，安全背景、专业资质，技术人员

专业技术水平，管理人员安全管理知识等；

b) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；

c) 应从内部人员中选拔从事关键岗位的人员。

d) 应对网络安全管理人员应实行备案管理。网络安全管理人员的配备和变更情况，应及时报上级机构备案；

e) 关键事务岗位应配备多人共同管理；

f) 对网络安全管理人员应实行备案管理。网络安全管理人员的配备和变更情况，应及时报上级机构备案。

i) **凡是因违反国家法律法规和核能机构有关规定受到过处罚或处分的人员，不得从事网络安全管理工作。**

2） 人员离岗

本项要求包括：

a) 应及时终止离岗人员的所有访问权限**并形成登记记录表单**，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

b) **应严格调离手续的办理程序，只有在收回访问权限和各种证件、设备后，关键岗位人员承诺履行调离后的保密义务后，方可办理调离手续。**

3） 安全意识教育和培训

本项要求包括：

a) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

b) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，并告知相关的安全责任和惩戒措施；

c) 应制定定安全教育培训计划的内容包括培训周期、培训方式、培训内容、考核方式、安全责任、惩戒措施等；

d) 每年至少对网络安全管理人员进行一次网络安全培训；

e) 应定期对不同岗位的人员进行技能考核。

4） 外部人员访问管理

本项要求包括：

a) 应指定责任部门负责非涉密计算机系统和网络相关的外部人员访问授权审批，批准后由专人全程陪同，并登记备案；

b) 应制定人员访问管理制度类和记录表单，明确访问范围、进入条件、访问控制措施，并记录批准签字、重要区域进入时间、离开时间、访问区域、陪同人员等内容。

c) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案；

d) **应制定管理记录表单，明确申请审批流程，并记录批准签字、权限、时限、账户等内容；**

e) 对关键区域或关键系统不允许外部人员访问；

f) **获得外部人员访问授权的所有机构和个人应与核能机构签订安全保密协议，不得进行未授权的增加、删除、修改、查询数据操作**，不得复制和泄漏核能机构的任何信息；

g) 外部人员进入核能机构现场实施时，应事先提交计划操作内容，核能机构人员应在现场陪同外部人员，核对操作内容并记录；

h) 外部人员离场后应及时清除其所有的访问权限。

i) 应制定管理制度记录表单，明确外部人员离场后及时清除其所有的访问权限，并记录访问权限清除时间。

10.2.4 **安全建设管理**

1） 定级和备案

本项要求包括：

a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；

c) 应保证定级结果经过**行业网络安全主管部门**的批准；

d) 应将备案材料报主管部门和相应公安机关备案。

2） 安全方案设计

本项要求包括：

f) 应根据安全保护等级选择基本安全措施，并依据**核电二次系统安全防护要求和**风险分析的结果补充和调整安全措施，**编写安全规划设计方案；**

g) 应指定和授权专门的部门对网络系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

h) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

i) 应根据保护对象的安全保护等级进行安全方案设计；

j) 应组织相关部门和有关安全专家对安全方案的合理性和正确性进行论证和审定，经过批准后才能正式实施。

3） 产品采购和使用

本项要求包括：

j) 应确保网络安全产品采购和使用符合**国家和行业的有关规定**；

a) 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；

b) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

c） 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品；

d） **扫描、检测类网络安全产品应报本机构信息化主管部门批准、备案；**

e） 扫描、检测类网络安全产品仅限于本机构网络安全管理人员或经主管领导授权的网络管理员使用；

f） 应定期查看各类网络安全产品相关日志和报表信息并汇总分析，若发现重大问题，立即采取应急措施并按规定程序报告；

g） 应定期对各类网络安全产品产生的日志和报表进行备份存档，保存时间超过 6 个月；

h） **应及时升级维护网络安全产品，凡超过使用期限的或不能继续使用的网络安全产品，要按照固定资产报废审批程序处理。**

4） 自行软件开发

本项要求包括：

a） 应制定软件开发管理制度和代码编写安全规范，明确说明开发过程的控制方法和人员行为准则，要求开发人员参照规范编写代码，**不得在程序中设置后门或恶意代码程序**；

b） 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；

c） 应确保开发人员和测试人员分离，开发人员不能兼任系统管理员或业务操作人员，确保测试数据和测试结果受到控制；

d） 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；

e） 在软件开发过程中，应同步完成相关文档手册的编写工作，保证相关资料的完整性和准确性；

f） 应在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测，**应具备软件安全测试报告和代码审计报告；**

g） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

h） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

5） 外包软件开发

本项要求包括：

a） 应在软件交付前检测其中可能存在的恶意代码，**具备交付前的恶意代码检测报告**；

b） 应保证开发单位提供软件设计文档和使用指南，**具备分析说明书、软件设计说明书、软件操作手册或使用指南等；**

c） 应定期对外包服务活动和外包服务商的服务能力进行审核和评估；

a） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；

b） 应具备交付前的第三方源代码审查报告或软件安全性测试证明（非源码审核）；

c） 应要求外包服务商保留操作痕迹、记录完整的日志，相关内容和保存期限应满足事件分析、安全取证、独立审计和监督检查需要；

d） 应禁止外包服务商转包并严格控制分包，保证外包服务水平；

e) **应制定数据中心外包服务应急计划，制订供应商替换方案，以应对外包服务商破产、不可抗力或其它潜在问题导致服务中断或服务水平下降的情形，支持数据中心连续、可靠运行；**

f) **应在外包开发合同中明确开发单位、供应商所提供的核电二次设备及系统应包含保密、生命周 期、禁止关键技术和设备扩散等方面的条款。**

6） 工程实施

本项要求包括：

a) 应指定或授权专门的部门或人员负责工程实施过程的管理；

d) 应制定安全工程实施方案控制工程实施过程，**编写记录表单，记录工程时间限制、进度控制、质量控制等方面内容，阶段性文件等。**

b) 应通过第三方工程监理控制项目的实施过程；

c) **应制定灾难备份系统集成与测试计划并组织实施。通过技术和业务测试，确认灾难备份系统的功能与性能达到设计指标要求；**

d) **系统的建设、升级、扩充等工程应经过科学的规划、充分的论证和严格的技术审查，有关材料应妥善保存并接受主管部门的检查。**

7） 测试验收

本项要求包括：

g) 应制定测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

h) **应明确说明参与测试的部门、人员、测试验收内容、现场操作过程以及相关部门和人员的审定意见；**

i) 应进行系统上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容；

j) **新系统上线前，对系统进行安全性评估，及时修补评估过程中发现的问题；**

k) 新建应用系统投入生产运行前，原则上应进行不少于1个月的模拟运行和不少于3个月的试运行；

l) **对于在生产系统上进行的测试工作，必须制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全。**

8） 系统交付

本项要求包括：

a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

g) 建设单位应在完成建设任务后将提供建设过程文档和运行维护文档，**并将建设过程文档和运维文档全部移交信息化主管部门；**

b) **外部建设单位应与核能机构签署相关知识产权保护协议和保密协议，不得将系统采用的关键安全技术措施和核心安全功能设计对外公开；**

c) 应对负责运行维护的技术人员进行相应的技能培训，**应形成培训记录，包括培训内容、培训时间**

和参与人员等；

d) **应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。**

9） 等级测评

本项要求包括：

a) **应至少每半年对系统进行一次等级测评**，发现不符合相应等级保护标准要求的及时整改，**应留存等级测评报告和安全整改方案。**

b) 应在发生重大变更或级别发生变化时进行等级测评；**发现级别发生变化的及时调整级别并进行安全 改造， 发现不符合相应等级保护标准要求的及时整改**

c) **应选择具有国家相关技术资质和安全资质的并由行业信息安全主管部门指定的测评单位进行 等级测评；**

d) **应指定或授权专门的部门或人员负责等级测评的管理。**

10） 服务供应商选择

本项要求包括：

a) 应确保服务供应商的选择符合国家的有关规定；

b) **选择服务供应商时应评估其资质、经营行为、业绩、服务体系和服务品质等要素；**

c) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；

d) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制

10.2.5 **安全运维管理**

1） 环境管理

本项要求包括：

j) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；

k) **机房应采用结构化布线系统，配线机柜内如果配备理线架，应做到跳线整齐，跳线与配线架统一编号，标记清晰；**

l) 应指定部门负责机房安全，指派专人担任机房管理员，对机房的出入进行管理，定期巡查机房运行状况，对机房供配电、空调、温湿度控制等设施进行维护管理，**填写机房值班记录、巡视记录；**

a) **机房人员进出机房必须使用主管部门制发的证件；**

b) **机房管理员应经过相关培训，掌握机房各类设备的操作要领；**

c) **应定期对机房设施进行维修保养，加强对易损、易失效设备或部件的维护保养；**

d) **机房出入口和内部应安装 7*24 小时录像监控设施，重要机房区域实行 24 小时警卫值班，机房实行封闭式管理，设置一个主出入口和一个或多个备用出入口，出入口控制、入侵报警和电视监控设备运行资料应妥善保管录像至少保存一周；**

e) **机房应设置弱电井，并留有可扩展空间；**

f) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等；

g) 应对出入人员进行相应级别的授权，**具备出入人员授权审批记录表单**，对进入重要安全区域的人员和活动实时监视，**同时应在重要区域安装监控系统，实时监控进入人员活动。**

2） 资产管理

本项要求包括：

a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；

c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

3） 介质管理

本项要求包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

b) 所有数据备份介质应防磁、防潮、防尘、防高温、防挤压存放；

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制；

k) 应对介质归档和查询等进行登记记录，管理员应根据存档介质的目录清单定期盘点；

l) 对于重要文档，如是纸质文档则应实行借阅登记制度，未经相关部门领导批准，任何人不得将文档转借、复制或对外公开；如是电子文档则应采用 OA 等电子化办公审批平台进行管理；

m) 对载有敏感信息存储介质的销毁，应报有关部门备案，由信息化主管部门进行信息消除、消磁或物理粉碎等销毁处理，并做好相应的销毁记录。信息消除处理仅限于存储介质仍将在核能机构内部使用的情况，否则应进行信息的不可恢复性销毁；

n) 应按照统一格式对技术文档进行编写并及时更新，达到能够依靠技术文档恢复系统正常运行的要求；

o) 应对技术文档实行有效期管理，对于超过有效期的技术文档降低保密级别，对已经失效的技术文档定期清理，并严格执行技术文档管理制度中的销毁和监销规定；

p) 应制定生产控制大区移动存储介质使用规范，并定期核查移动存储介质的使用情况；

q) **应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。**

4） 设备维护管理

本项要求包括：

a) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

i) 新购置的设备应经过测试，测试合格后方能投入使用；

j) 各机构信息化主管部门负责对网络系统相关的各种设备（包括备份和冗余设备）、线路等定期进

行维护管理；

k) 应做好设备登记工作，制定设备管理规范，落实设备使用者的安全保护责任；

l) 需要废止的设备，应由信息化主管部门使用专用工具进行数据信息消除处理，如废止设备不再使用或调配到核能机构以外的单位，应由信息化主管部门对其数据信息存储设备进行消磁或物理粉碎等不可恢复性销毁处理；

m) 设备确需送外单位维修时，应彻底清除所存的工作相关信息，并与设备维修厂商签订保密协议，与密码设备配套使用的设备送修前必须请生产设备的科研单位拆除与密码有关的硬件，并彻底清除与密码有关的软件和信息；

n) **应制定规范化的故障处理流程，建立详细的故障日志(包括故障发生的时间、范围、现象、处理结果和处理人员等内容)。**

5） 漏洞和风险管理

本项要求包括：

d) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

e) 应对发现的安全漏洞和隐患进行评估，分析被利用的可能性，判断安全风险的等级，在可接受的范围内进行残余风险评估，明确风险等级；

f) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

6） 网络和系统安全管理

本项要求包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；

c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期、重要文件备份等方面作出规定；

d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；

i) 应使用商业化的运维工具，严禁运维人员私自下载第三方未商业化的运维工具；如使用官方正版商用化工具，或自行开发的，安全可控的运维工具，并对于运维工具的接入有严格的控制措施；

j) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

k） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为；

l） 应明确所有与外部连接的授权和批准制度，并定期对相关违反行为进行检查，可采取终端管理系统实现违规外联和违规接入，设置合理的安全策略，在出现违规外联和违规接入时能第一时间进行检测和阻断；

m） 应对网络环境运行状态进行巡检，巡检应保留记录，并有操作和复核人员的签名；

n） 应制定远程访问控制规范，确因工作需要进行远程访问的，应由访问发起机构的信息化主管部门核准，提请被访问机构信息化主管部门开启远程访问服务，并采取单列账户、最小权限分配、及时关闭远程访问服务等安全防护措施；

o） 网络安全管理人员经本部门主管领导批准后，有权对本机构或辖内网络进行安全检测、扫描，检测、扫描结果属敏感信息，未经授权不得对外公开，未经信息化主管部门授权，任何外部机构与人员不得检测或扫描机构内部网络；

p） 系统管理员不得对业务数据进行任何增加、删除、修改等操作，系统管理员确需对计算机系统数据库进行技术维护性操作的，应征得业务部门同意，并详细记录维护信息过程；

q） **每半年应至少进行一次漏洞扫描，对发现的系统安全漏洞及时进行修补，扫描结果应及时上报。**

7） 恶意代码防范管理

本项要求包括：

a） 应提高所有用户的防恶意代码意识，**告知及时升级防病毒软件，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，**对外来计算机或存储设备接入系统前进行恶意代码检查等；

b） 应统一安装病毒防治软件，设置用户密码和屏幕保护口令等安全防护措施，确保及时更新病毒特征码并安装必要的补丁程序；

c） 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；

d） 应定期验证防范恶意代码攻击的技术措施的有效性。

8） 配置管理

本项要求包括：

a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

9） 密码管理

本项要求包括：

a） 应遵循密码相关国家标准和行业标准；

b） 应使用国家密码管理主管部门认证核准的密码技术和产品；

c） 应采用硬件密码模块实现密码运算和密钥管理；

d） 应建立对所有密钥的产生、分发和接收、使用、存储、更新、销毁等方面进行管理的制度，密钥管理人员必须是本机构在编的正式员工；

e） 系统管理员、数据库管理员、网络管理员、业务操作人员均须设置口令密码，并定期更换，口令密码的强度应满足不同安全性要求；

f） 生产环境重要计算机系统和设备的口令密码设置应在安全的环境下进行，必要时应将口令密码纸质密封交相关部门保管，未经信息化主管部门主管领导许可，任何人不得擅自拆阅密封的口令密码，拆阅后的口令密码使用后应立即更改并再次密封存放；

g） 密钥注入、密钥管理功能调试和密钥档案的保管应由专人负责。密钥资料须保存在保险柜内。保险柜钥匙由专人负责。使用密钥和销毁密钥要在监督下进行并应有使用、销毁记录；

h） **确因工作需要经授权可远程接入内部网络的用户，应妥善保管其身份认证介质及口令密码，不得转借他人使用。**

10） 变更管理

本项要求包括：

a） 应确明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

b） 变更前应做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪；

c） 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

d） 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

e） 变更前做好系统和数据的备份，风险较大的变更，应在变更后对系统的运行情况进行跟踪；

f） 如果需要在生产环境进行测试或者变更，应纳入变更管理，并制定详细的系统及数据备份、测试环境搭建、测试后系统及数据恢复、生产系统审核等计划，确保生产系统的安全；

11） 备份与恢复管理

本项要求包括：

a） 应规定备份信息的备份方式、备份频度、存储介质和保存期等；

b） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等；

c） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

d） 恢复及使用备份数据时需要提供相关口令密码的，应妥善保管口令密码密封与数据备份介质；

e） 应建立灾难恢复计划，定期开展灾难恢复培训，并根据实际情况进行灾难恢复演练；

f） 应定期对备份数据的有效性进行检查，备份数据应实行异地保存；

g） **生产环境应建立灾难备份系统，主备系统实际切换时间应少于 60 分钟，灾备系统处理能力应不低于主用系统处理能力的 50%，通信线路应分别接入主备系统，有条件时可采用主、备系统处理**

能力相同、轮换交替使用的双系统模式。

12） 安全事件处置

本项要求包括：

a） 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

b） 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

c） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过 程，总结经验教训；

d） 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

e） 应建立联合防护和应急机制，负责处置跨单位安全事件。

f） 应建立有效的技术保障机制，确保在安全事件处置过程中不会因技术能力缺乏而导致处置中断或延长应急处置时间。

g） 应严格控制参与涉及国家秘密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案；

h） 应建立电力二次系统联合防护和应急机制，负责处置跨部门电力二次系统安全事件。

13） 应急预案管理

本项要求包括：

a） 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

b） 业务处理系统应急预案的编制工作应由相关业务部门和信息化主管部门共同完成，并由预案涉及的相关机构签字盖章；

c） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

d） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

e） 应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练；

f） 应对安全管理员、系统管理员、网络管理员等相关的人员进行应急预案培训，应急预案的培训 应至少每年举办一次；

g） 应急领导小组应严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法；

h） 突发事件应急处置领导小组统一领导计算机系统的应急管理工作，指挥、决策重大应急处置事宜，并协调应急资源，明确具体应急处置联络人，并将具体联系方式上报上级监管部门；

i） 在与第三方合作的业务中，应建立并完善内部责任机制和与相关机构之间的协调机制，制定完整的应急预案及应急协调预案，并定期参加联合演练；

j） 实施报告制度和启动应急预案的单位应当实行重大突发事件 24 小时值班制度；

k） **应急演练结束后，应撰写应急演练情况总结报告；总结报告内容应包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练结论。**

l） 应定期对原有的应急预案重新评估，**并根据安全评估结果，定期修订、演练，并进行专项内部审计。**

14） 外包运维管理

本项要求包括：

a） 应确保外包运维服务商的选择符合国家的有关规定；

b） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。

c） 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

d） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

11 第五级安全要求

略。

参 考 文 献

[1]《中华人民共和国网络安全法》

[2]《关键信息基础设施安全保护条例》(国务院第 745 号令)

[3]《电力行业信息安全等级保护基本要求释义》

[4]《电力监控系统安全防护规定》国家电力监管委员会 2014（14 号）

[5]《电力监控系统安全防护总体方案》国家能源局 2015（36 号）

[6]《国家能源局关于加强电力行业网络安全工作的指导意见》国家能源局 2018（72 号）

[7]《网络安全评估标准实用手册》邹来龙

[8]《网络安全评估实战》邹来龙

[9]《核动力厂网络安全技术政策》国家核安全局 2020（298 号）