ICS 29.020
K 07
备案号：53948-2016

DL

中华人民共和国电力行业标准

DL / T 1527 — 2016

用电信息安全防护技术规范

Technology specification of electric power utilization information security protection

2016-01-07发布　　2016-06-01实施

国家能源局　发布

目　次

前　言

本标准依据 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》的规则起草。

本标准由中国电力企业联合会提出。

本标准由电力行业供用电标准化技术委员会归口。

本标准主要起草单位：中国电力科学研究院。

本标准参加起草单位：国家电网公司、中国南方电网有限责任公司、南方电网科学研究院、国网上海市电力公司、国网天津市电力公司、国网新疆电力公司、国网山东省电力公司、国网福建省电力有限公司、国网四川省电力公司、国网河南省电力公司。

本标准主要起草人：翟峰、杜蜀薇、刘鹰、杜新纲、章欣、吕英杰、赵兵、徐英辉、张明明、葛得辉、孙志强、杨湘江、彭楚宁、周晖、付义伦、李保丰、徐湛、岑炜、梁晓兵、冯占成、曹永峰、钱斌、朱彬若、解岩、冯勇军、徐新光、钟小强、张嘉岷、侯慧娟。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

用电信息安全防护技术规范

1 范围

本标准规定了电力行业用电信息系统及其相关信息系统的安全防护技术要求。

本标准适用于指导用电信息系统及其相关信息系统的安全防护建设工作。

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，仅注日期的版本适用于本文件。凡是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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

中华人民共和国国家发展和改革委员会令 第 14 号 电力监控系统安全防护规定

电监信息〔2007〕44 号 电力行业信息系统安全等级保护定级工作指导意见

3 术语和定义

下列术语和定义适用于本文件。

3.1

用电信息系统 electric power utilization information system

面向广大城乡电力用户的用电信息采集和监控系统。

3.2

生产控制大区 production control area

用以支持电力企业生产自动化控制，使用电力调度数据网或专用通道进行数据传输，具有实时控制功能或具备在线运行但不具备控制功能的业务系统或业务模块的集合。

3.3

管理信息大区 management information area

用以支持电力企业信息管理和决策，除生产控制大区以外的电力企业管理业务系统或业务模块的集合。

3.4

公用通信网络 public communication network

由网络服务商或电力企业建设的，供电力企业内部公共业务使用的通信网络，如 GPRS/CMDA 网、TD-SCDMA 网、无线局域网、微波网、ADSL 宽带等。

3.5

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件及在系统遭受损害后能够恢复到先前状态的程度。

3.6

管理类信息系统 management information system

由计算机网络和处理设备组成，能提供电力企业管理所需信息，以支持企业信息管理和决策的人机系统。

3.7

生产控制类信息系统 production control information system

由计算机网络和处理设备组成，能提供电力企业生产所需信息，以支持企业生产自动化控制的人机系统。

3.8

组件　package

在用电信息系统中具有相对独立功能、与用电信息系统有明显依赖关系，可独立部署、组装的子系统或业务模块。

3.9

信息安全性要求　information security requirement

保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权修改的信息安全类要求。

3.10

系统可用性要求　system availability requirement

保护系统连续正常运行，免受未授权修改、破坏而导致系统不可用的服务保证类要求。

3.11

系统安全性要求　system security requirement

保护系统安全可靠运行，免受恶意攻击的系统安全类要求。针对用电信息系统的信息安全性要求是用电信息系统安全防护的基础。

4　系统分区防护要求

为了确保用电信息系统安全，抵御黑客、病毒、恶意代码等各种形式的恶意破坏和攻击，特别是抵御集团式攻击，防止用电信息系统崩溃或瘫痪，以及由此造成的电力系统事故或大面积停电事故，根据《电力监控系统安全防护规定》和《电力行业信息系统安全等级保护定级工作指导意见》等相关规定，结合用电信息系统的实际应用情况，依据“分区、分级、分域”防护方针，将用电信息系统部署在管理信息大区，独立成域，并进行防护设计。用电信息系统所属分区如图 1 所示。

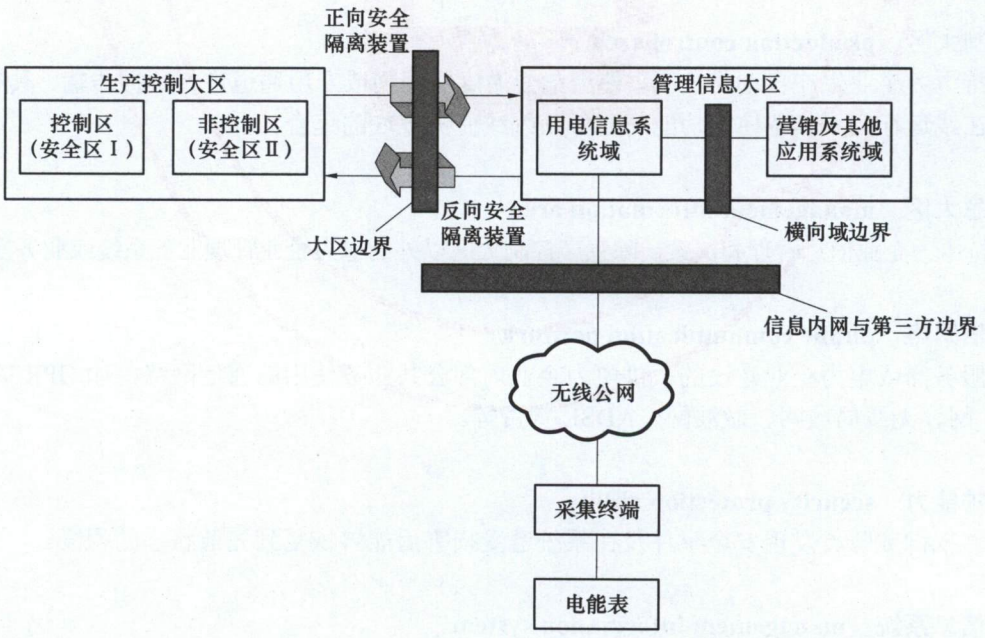

图 1　用电信息系统所属分区

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，结合用电信息系统与相关信息系统的数据交互特点进行系统安全防护，重点强化边界防护，提高内

部安全防护能力，保证用电信息系统及相关信息系统的安全。用电信息系统部署在管理信息大区。管理信息大区和生产控制大区之间使用正反向横向单向安全隔离装置作为边界安全防护的大区边界。用电信息系统域与营销及其他应用系统域之间为横向域边界。用电信息系统主站与采集终端的无线接入区作为信息内网与第三方的边界。

用电信息系统分区防护要求包括：

a） 用电信息系统通信网络与其他系统通信网络间应部署符合电力系统要求的横向单向安全隔离装置，确保横向单向安全隔离装置配置策略安全有效，禁止任何穿越边界的E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

b） 在用电信息系统通信网络与广域网的纵向交接处应当设置经过国家指定部门检测认证的电力专用纵向加密认证装置或者加密认证网关及相应设施，确保纵向加密认证装置的策略配置安全有效，实现双向身份认证、数据加密和访问控制。

c） 用电信息系统网络边界应采取必要的安全防护措施，禁止任何穿越管理信息大区边界的通用网络服务。

d） 用电信息系统通信网络可进一步划分为内部网络和外部网络，两网之间信息通信交互时应设置一个物理隔离，但逻辑相连的环境需部署专用防护设备，防护强度应强于逻辑隔离。

e） 用电信息系统各组件应提供统一的互联网网络出口，在网络出口处应部署符合本标准要求的安全防护设备。

f） 用电信息系统各组件可结合自身实际划分为不同的子域，各子域安全防护措施应符合本标准的相关要求。

5 系统安全防护框架

本标准结合用电信息系统具体情况，从物理安全、网络安全、主机安全、应用安全和数据安全五个层面提出系统安全防护框架的要求，主要通过在信息系统中部署软件、硬件并正确地配置其安全功能来实现安全防护技术。

安全防护技术体系和安全管理体系是确保用电信息系统信息安全不可分割的两个部分，如图2所示，其中，安全管理体系将在附录 A 中详细描述。

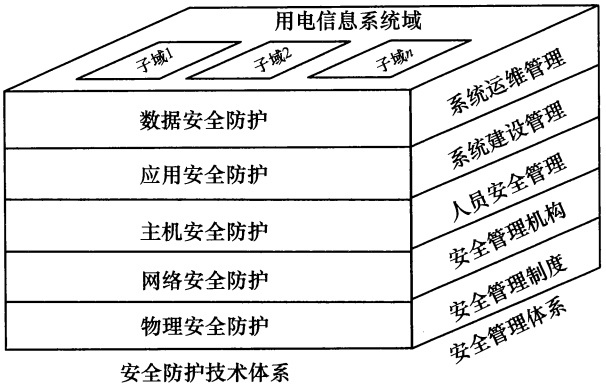

图 2 用电信息系统安全防护框架

安全防护体系从各个层面或方面提出了系统的每个组件（子系统）应该满足的安全要求，信息系统具有的整体安全防护能力通过不同组件（子系统）安全防护的实现来保证。除了保证系统的每个组件（子系统）满足本标准要求外，还需考虑组件（子系统）之间的相互关系，以保证用电信息系统的整体安全防护能力。

6 总体安全防护要求

6.1 总体技术要求

用电信息安全防护总体应满足如下技术要求：

a） 用电信息系统应遵循本标准所提出的安全要求，除保证系统的每个组件满足安全要求外，还要考虑组件之间的相互关系，来保证信息系统的整体安全防护能力。

b） 保护用电信息系统数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改。

c） 保护用电信息系统连续正常的运行，免受未授权修改、破坏而导致系统不可用。

6.2 防护效果要求

应能够在统一安全策略下对用电信息系统进行防护，使其免受恶意攻击、较为严重的自然灾害所造成的主要资源损害。同时能够发现安全漏洞和安全事件，并在系统遭到损害后，能够较快恢复绝大部分功能。

7 分层防护

7.1 物理安全防护

7.1.1 物理位置的选择

物理位置选择应满足如下要求：

a） 机房和办公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，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） 智能电能表等量测设备及网络设备应部署在温度、湿度相对合适的环境中，减少自然灾害或人为事故引起的破坏。

7.1.2 物理访问控制

物理访问控制应满足如下要求：

a） 机房各出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

b） 进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

c） 应对机房划分区域进行管理，区域和区域之间应用物理方式隔断，在重要区域前设置或安装过渡区域。

d） 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

e） 应对用电信息系统各类设备予以正确的维护，确保其持续的可用性和完整性。

7.1.3 防盗窃和防破坏

防盗窃和防破坏应满足如下要求：

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。

c） 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

d） 应对介质分类标识，存储在介质库或档案室中。

e） 应利用光、电等技术设置机房防盗报警系统。

f） 应对机房设置监控报警系统。
g） 应加强智能电能表等量测设备的防破坏措施，避免用户私自打开或配置量测设备，影响量测数据的可用性。

7.1.4 防雷击

防雷击应满足如下要求：
a） 机房建筑应设置避雷装置。
b） 应设置防雷保安器，防止感应雷。
c） 机房应设置交流电源地线。
d） 对安装在室外的量测设备或安装外置天线的设备应考虑防雷措施，避免雷击造成设备的损坏。

7.1.5 防火

防火应满足如下要求：
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、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） 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

7.1.6 防水和防潮

防水和防潮应满足如下要求：
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） 应安装敏感的检测仪表或元件，对机房进行防水检测和报警。

7.1.7 防静电

防静电应满足如下要求：
a） 主要设备采用必要的接地防静电措施。
b） 机房应采用防静电地板。

7.1.8 温、湿度控制

温、湿度控制应满足如下要求：
机房应设置温、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。

7.1.9 电力供应

电力供应应满足如下要求：
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，至少满足主要设备在断电情况下的正常运行要求。
c） 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。
d） 应建立备用供电系统。

7.1.10 电磁防护

电磁防护应满足如下要求：

a） 电源线和通信线缆应隔离铺设，避免互相干扰。
b） 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。
c） 应对关键设备和磁介质实施电磁屏蔽。

7.2 网络安全防护

7.2.1 结构安全

结构安全应满足如下要求：

a） 用电信息系统域与生产控制大区网络应物理隔离，两网之间有信息交换时应部署符合电力系统要求的横向单向安全隔离装置。
b） 用电信息系统各组件（子系统）可结合自身实际划分为不同的子域，各子域安全防护措施应符合本标准相关要求。
c） 用电信息系统可进一步划分为内部网络和外部网络，两网之间信息通信交换时应设置一个物理隔离，但逻辑相连的环境需部署专用防护设备，防护强度应强于逻辑隔离。
d） 用电信息系统及各组件应提供统一的网络出口，在网络出口处应部署符合本标准要求的安全设备。
e） 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰时段需要。
f） 应保证网络各个部分的带宽满足业务高峰期需要。
g） 各层面的数据网络之间应通过路由限制措施进行安全隔离，保证网络故障和安全事件限制在局部区域之内。
h） 应在业务终端与业务服务器之间进行路由控制，建立安全的访问路径。
i） 应绘制完整的网络拓扑结构图，网络拓扑结构图要有相应的网络配置表，并包含设备 IP 地址等主要信息，且要与当前运行情况相符。
j） 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。
k） 在业务高峰时段，现有带宽不能满足要求时，应按照对业务服务的重要次序来制定带宽分配优先级，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。
l） 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。
m） 在进行内、外网隔离的情况下，应将应用系统部署在内网，如有与外网交互功能的应用系统，可将前端部署在外网，数据库部分部署在内网。

7.2.2 访问控制

访问控制应满足如下要求：

a） 应在网络边界部署访问控制设备，启用访问控制功能。
b） 访问控制设备应能根据会话状态信息为数据流提供明确的允许或拒绝访问的能力，控制粒度为端口级。
c） 应按用户和系统之间的访问规则，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 等方式接入网络的，应采用强认证方式，并对用户访问权限进行严格限制。
d） 拨号访问服务及服务器均应使用经安全加固的达到国家三级等级保护要求的操作系统，客户端应使用经安全加固的操作系统，并采取加密、数字证书认证和访问控制等安全防护措施。
e） 应限制具有拨号、VPN 等访问权限的用户数量。
f） 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等

协议命令级的控制。

g） 应在会话处于非活跃一定时间或会话结束后终止网络连接。

h） 在互联网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。

i） 重要网段应采取技术手段防止地址欺骗。

7.2.3 安全审计

安全审计应满足如下要求：

a） 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。

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） 应能够根据记录数据进行分析，并生成审计报表，网络设备不支持的应采用第三方工具生成审计报表。

d） 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

7.2.4 边界完整性检查

边界完整性检查应满足如下要求：

a） 应能够对非授权设备私自连到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

b） 应能够对内部网络用户私自连到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

7.2.5 入侵防范

入侵防范应满足如下要求：

a） 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、拒绝服务攻击、IP 碎片攻击和网络蠕虫攻击等。

b） 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击时间，在发生严重入侵事件时应提供报警。

7.2.6 恶意代码防范

恶意代码防范应满足如下要求：

a） 应在网络边界处对恶意代码进行检测和清除。

b） 应维护恶意代码库的升级和检测系统的更新。

7.2.7 网络设备防护

网络设备防护应满足如下要求：

a） 应对登录网络设备的用户进行身份鉴别。

b） 应对网络设备的管理员登录地址进行限制。

c） 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。

d） 身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换，应修改默认用户和口令，不得使用默认口令。口令长度不得小于 8 位，要求是字母和数字或特殊字符的混合，不得与用户名相同。口令应定期更换，并加密存储。

e） 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

f） 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

g） 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

h） 应实现设备特权用户的权限分离，系统不支持的应部署日志服务器保证管理员的操作能够被审计，并且网络特权用户管理员无权对审计记录进行操作。

i） 应封闭不需要的网络端口，关闭不需要的网络服务。如需使用 SNMP 服务，应采用安全性增强版本，并应设定复杂的 Community 控制字段，不使用 Public、Private 等默认字段。

7.3 主机安全防护

7.3.1 身份鉴别

身份鉴别应满足如下要求：

a） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

b） 操作系统和数据库系统的管理用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换，口令长度不得小于 8 位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同。

c） 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，限制同一用户连续失败登录次数。

d） 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

e） 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

f） 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

7.3.2 访问控制

访问控制应满足如下要求：

a） 应启用访问控制功能，依据安全策略控制用户对资源的访问。

b） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

c） 应实现操作系统和数据库系统特权用户的权限分离。

d） 应限制默认账户的访问权限，并要求用户首次登录时重命名系统默认账户，修改这些账户的默认口令。

e） 应定期对账户进行管理，及时删除多余的、过期的账户，避免共享账户的存在。

f） 应对重要信息资源设置敏感标记，系统不支持设置敏感标记的，应采用专用安全设备生成敏感标记，用以支持强制访问控制机制。

g） 应依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。

7.3.3 安全审计

安全审计应满足如下要求：

a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户，系统不支持该要求的，应以系统运行安全和效率为前提，采用第三方安全审计产品实现审计要求。

b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）；对于数据库审计，审计内容应该至少包括 DDL、DML、ACL、函数和存储过程的调用等。

c） 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

d） 对于数据库审计记录，应该至少包括访问语句、成功与否、语句参数、影响行数。

e） 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

f） 应能够通过操作系统自身功能或第三方工具根据记录数据进行分析，并生成审计报表。

g） 应保护审计进程，避免受到未预期的中断。

7.3.4 剩余信息保护

剩余信息保护应满足如下要求：

a） 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是内存中。

b） 应确保系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

7.3.5 入侵防范

入侵防范应满足如下要求：

a） 对面向互联网应用的系统，其操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。对其他应用的系统，当系统存在高危漏洞且面临严重威胁，尚无其他有效控制手段时，应及时安装相关补丁。在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

b） 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的时间，并在发生严重入侵事件时提供报警，对于 SQL 注入、数据库漏洞攻击等入侵行为能够提供报警和阻断。

c） 应能够对重要程序的完整性进行检测，并具有完整性恢复的能力。

d） 当系统存在高危漏洞且面临严重威胁，尚无其他有效控制手段时，应及时安装相关补丁。在安装系统补丁前，应首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

7.3.6 恶意代码防范

恶意代码防范应满足如下要求：

a） 应在本机安装防恶意代码软件或独立部署恶意代码防护设备，并及时更新防恶意代码软件版本和恶意代码库。

b） 应支持防恶意代码的统一管理。

c） 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

7.3.7 资源控制

资源控制应满足如下要求：

a） 应通过设定终端接入方式、网络地址范围等条件限制终端登录。

b） 应根据安全策略设置登录终端的操作超时锁定。

c） 应根据需要限制单个用户对系统资源的最大或最小使用限度。

d） 应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况。

e） 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

f） 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。

g） 应采取措施控制桌面终端对移动硬盘、优盘等移动介质的使用，禁止桌面终端与手机、相机等外部设备连接。

7.4 应用安全

7.4.1 身份鉴别

身份鉴别应满足如下要求：

a） 应提供专用的登录控制模块对登录用户进行身份标识和鉴别。

b） 应用系统用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换，应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，用户在第一次登录系统时修改分发的初始口令，口令长度不得小于 8 位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同，应用软件不得明文存储口令数据。

c） 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

d） 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

e） 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

f） 在与用户互动建立连接时，应鉴别用户身份，防止信息泄露。

7.4.2 访问控制

访问控制应满足如下要求：

a） 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。

b） 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。

c） 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限。

d） 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

e） 应对权限的赋予、变更、撤销制定严格的审核、批准、操作流程，权限变动经相关人员审核批准后方可执行或生效。

f） 应依据权限最小化原则对用户赋予适当的权限，执行角色分离，禁止多人共用账号，并定期进行权限复核。

g） 仅对必要的用户赋予远程互动接入权限，对于接入用户的权限应进行严格限制，由相关负责人授权后方可开通，并依据其业务访问需求制定访问控制策略。

h） 应依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。

7.4.3 安全审计

安全审计应满足如下要求：

a） 应提供覆盖到每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件进行审计。

b） 应保证审计活动的完整性和连续性，保证无法删除、修改或覆盖审计记录。

c） 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

d） 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

7.4.4 剩余信息保护

剩余信息保护应满足如下要求：

a） 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。

b） 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户

前得到完全清除。

7.4.5 通信完整性

通信完整性应满足如下要求：

a） 应采用数字签名技术保证通信的完整性。

b） 系统应能够检测到管理数据、认证信息和重要业务数据在传输过程中的完整性是否受到破坏。

c） 系统在检测到完整性错误时应能采取必要的恢复措施。

7.4.6 通信保密性

通信保密性应满足如下要求：

a） 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。

b） 应采用认证、加密等技术措施实现数据的远方安全传输以及纵向边界的安全防护，包含以下几点要求：

1） 应在用电信息系统主站侧配置国家密码管理局认可的密码机设备，实现数据的加密和解密，密码机设备必须集成有对称密码算法和非对称密码算法；

2） 应在智能采集终端中采用国家密码管理局认可的硬件安全模块实现数据的加密和解密，智能采集终端的硬件安全模块应采用同时集成有国家密码管理局认可的对称密码算法和非对称密码算法的安全模块；

3） 应在智能电能表中采用国家密码管理局认可的硬件安全模块以实现数据的加密和解密，智能电能表采用的硬件安全模块内部应至少集成有国家密码管理局认可的对称密码算法。

c） 经网络传输的用户名、口令等认证信息应杜绝明文传输。

7.4.7 抗抵赖

抗抵赖应满足如下要求：

a） 应具有日志记录并结合身份认证技术在请求的情况下为数据原发者或接收者提供数据原发证据的功能。

b） 应具有日志记录并结合身份认证技术在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

7.4.8 软件容错

软件容错应满足如下要求：

a） 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数据格式或长度符合系统设定要求。

b） 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

7.4.9 资源控制

资源控制应满足如下要求：

a） 当应用系统的通信双方中的一方在一段时间内未作响应时，另一方应能够自动结束会话。

b） 应能够对系统的最大并发会话连接数进行限制。

c） 应能够对单个账户的多重并发会话进行限制。

d） 应能够对一个时间段内可能的并发会话连接数进行限制。

e） 应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额。

f） 应能够对系统服务水平降低到预先规定的最小值进行检测和报警。

g） 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

7.5 数据安全

7.5.1 数据完整性

数据完整性应满足如下要求：

a） 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中的完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施。

b） 应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中的完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施。

7.5.2 数据保密性

数据保密性应满足如下要求：

a） 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输的保密性。

b） 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据存储的保密性。

c） 所有应用安全设备（密码机和安全模块）应完全受控，由专门机构管理、制作和发放，并采用经过国家密码管理局批准的加密方式、密码算法和密钥管理技术来增强安全保障。

d） 应用层应采用对称密码算法与非对称密码算法相结合的混合密码系统，对称密码算法可选用国密 SM1 或 SM4 算法，非对称密码算法可选用 SM2 算法。

7.5.3 备份和恢复

数据备份与恢复应满足如下要求：

a） 应提供数据本地备份与恢复功能，对重要信息进行备份，数据备份至少每天一次，已有数据备份可完全恢复至备份执行时状态，并对备份可恢复性进行定期演练，备份介质需要场外存放。

b） 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。

c） 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

附 录 A
（资料性附录）
用电信息系统安全管理要求

A.1 安全管理制度

A.1.1 管理制度

管理制度应满足如下要求：

a） 应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。
b） 应对安全管理活动中的各类管理内容建立安全管理制度。
c） 应对要求管理人员或操作人员执行的日常管理操作建立操作规程。
d） 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

A.1.2 制定和发布

制定和发布应满足如下要求：

a） 应指定或授权专门的部门或人员负责安全管理制度的制定。
b） 安全管理制度应具有统一的格式，并进行版本控制。
c） 应组织相关人员对制定的安全管理制度进行论证和审定。
d） 安全管理制度应通过正式、有效的方式发布。
e） 安全管理制度应注明发布范围，并对收发文进行登记。

A.1.3 评审和修订

评审和修订应满足如下要求：

a） 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。
b） 定期或在发生重大变更时对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

A.2 安全管理机构

A.2.1 岗位设置

岗位设置应满足如下要求：

a） 应设立信息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） 应设立系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责。
c） 应成立指导和管理信息安全工作的委员会或领导小组，电力企业主要负责人是本单位信息安全的第一责任人，对本单位的网络与信息安全负全面责任。
d） 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

A.2.2 人员配备

人员配备应满足如下要求：

a） 应配备一定数量的系统管理员、网络管理员、安全管理员等。
b） 每个电力企业应配备专职安全管理员，不可兼任。
c） 关键事务岗位应配备多人共同管理。

A.2.3 资金保障

资金保障应满足如下要求：
a） 应保障落实信息系统安全建设、运维、监督检查和等级保护测评的资金。
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。

A.2.4 授权和审批

授权和审批应满足如下要求：
a） 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。
b） 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，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。
d） 应针对关键活动建立审批流程，由批准人签字确认，并存档备查。

A.2.5 沟通和合作

沟通和合作应满足如下要求：
a） 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题。
b） 应加强与行业信息安全监管部门、公安机关、通信运营商、银行及相关单位和部门的合作与沟通。
c） 应加强与供应商、业界专家、专业的安全公司及安全组织的合作与沟通。
d） 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。
e） 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。

A.2.6 审核和检查

审核和检查应满足如下要求：
a） 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
b） 应由内部人员或上级单位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，并对安全检查结果进行通报。
d） 应制定安全审核和安全检查制度规范，定期按照程序进行安全审核和安全检查活动。

A.3 人员安全管理

A.3.1 人员录用

人员录用应满足如下要求：
a） 应指定或授权专门的部门或人员负责人员录用。
b） 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核。

c） 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。
d） 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岗位安全协议。

A.3.2 人员离岗

人员离岗应满足如下要求：
a） 应严格规范人员离岗过程，及时收回离岗员工的所有访问权限。
b） 应收回各种身份证件、钥匙、徽章等，以及机构提供的软件、硬件设备。
c） 只有在收回访问权限和各种证件、设备等之后方可办理调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

A.3.3 人员考核

人员考核应满足如下要求：
a） 应定期对各个岗位的人员进行安全技能及安全认知的考核。
b） 应对安全管理员、系统管理员、网络管理员、信息安全主管或专责等关键岗位的人员进行全面、严格的安全审查和技能考核。
c） 应对考核结果进行记录并保存。

A.3.4 安全意识教育和培训

安全意识教育和培训应满足如下要求：
a） 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。
b） 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒。
c） 应按照行业信息安全要求，对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等的培训应至少每年举办一次。
d） 应对安全教育和培训的情况和结果进行记录并归档保存。

A.3.5 外部人员访问管理

外部人员访问管理应满足如下要求：
a） 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。
b） 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

A.4 系统安全建设管理

A.4.1 系统定级

系统定级应满足如下要求：
a） 应明确信息系统的边界和安全保护目标。
b） 应以书面的形式说明确定用电信息系统安全保护等级的方法和理由。
c） 对于属同一电力公司，但跨省联网运行的信息系统，由公司责任部门统一确定安全保护等级，对于通用信息系统，由领导小组办公室提出安全保护等级建议，运营使用单位自主确定安全保护等级，对于运营使用单位所特有的信息系统，各运营使用单位自行确定安全保护等级。
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。

A.4.2 安全方案设计

安全方案设计应满足如下要求：

a） 应根据系统的安全防护目标选择基本安全措施，并依据风险分析的结果补充和调整安全措施。
b） 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制订近期和远期的安全建设工作计划。
c） 应根据信息系统的安全子域划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。
d） 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。
e） 应根据等级测评、安全评估的结果每年定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

A.4.3 产品采购和使用

产品采购和使用应满足如下要求：
a） 应确保安全产品采购和使用符合国家的有关规定。
b） 应确保密码产品采购和使用符合国家密码主管部门的要求。
c） 应指定或授权专门的部门负责产品的采购。
d） 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。
e） 电力系统专用信息安全产品应经行业主管部门指定的安全机构测评方可采购使用。

A.4.4 自行软件开发

自行软件开发应满足如下要求：
a） 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制。
b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。
c） 应制定代码编写安全规范，要求开发人员参照规范编写代码。
d） 应确保提供软件设计的相关文档和使用指南，并由专人负责保管。
e） 应确保对程序资源库的修改、更新、发布进行授权和批准。

A.4.5 外包软件开发

外包软件开发应满足如下要求：
a） 应根据开发要求检测软件质量。
b） 应在软件安装之前检测软件包中可能存在的恶意代码。
c） 应要求开发单位提供软件设计的相关文档和使用指南。
d） 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。

A.4.6 工程实施

工程实施应满足要求：
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） 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程。
c） 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

A.4.7 测试验收

测试与验收应满足如下要求：

a） 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告。
b） 在测试验收前应根据设计方案或合同要求等制定测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。
c） 应对系统测试验收的控制方法和人员行为准则进行书面规定。
d） 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作。
e） 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

A.4.8 系统交付

系统交付应满足如下要求：
a） 应制定详细的系统交付清单，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） 应对负责系统运行维护的技术人员每年进行相应的技能培训，对安全教育和培训的情况和结果进行记录并归档保存。
c） 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。
d） 应对系统交付的控制方法和人员行为准则进行书面规定。
e） 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

A.4.9 系统备案

系统备案应满足如下要求：
a） 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用。
b） 应将系统等级及相关材料报系统主管部门备案，电力企业汇总系统等级及相关信息报电力行业网络与信息安全领导小组办公室备案。
c） 跨电力公司联网运行，且由电力行业网络与信息安全领导小组办公室统一确定安全等级的信息系统，领导小组办公室负责统一向公安部办理备案手续。电力公司内部跨省联网运行，且由公司责任部门统一确定安全等级的信息系统，由公司责任部门负责统一向公安部办理备案手续。其他信息系统由运营使用单位直接向当地市级以上公安机关备案，跨省联网运行的信息系统，在各地运行、应用的分支系统，向当地市级以上公安机关备案。

A.4.10 系统测评

系统测评应满足如下要求：
a） 在系统运行过程中，应至少每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。
b） 应在系统发生变更时及时对系统进行等级测评，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，经电力行业信息安全测评中心批准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。

A.4.11 安全服务商选择

安全服务商选择应满足如下要求：
a） 应选择符合国家及行业有关规定的安全服务商开展安全服务。
b） 应与选定的安全服务商签订安全协议，明确安全责任。
c） 应与服务商签订安全服务合同，明确技术支持和服务承诺。

A.5 系统安全运维管理

A.5.1 环境管理

环境管理应满足如下要求：

a） 应指定专门的部门或人员定期对机房供配电、空调及温度、湿度控制等设施进行维护管理。

b） 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理。

c） 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。

d） 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸质文件等。

A.5.2 资产管理

资产管理应满足如下要求：

a） 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。

b） 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

c） 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。

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

A.5.3 介质管理

介质管理应满足如下要求：

a） 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面做出规定。

b） 应建立移动存储介质安全管理制度，对移动存储介质的使用进行管控。

c） 应确保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。

d） 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，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点。

e） 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁。

f） 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。

g） 对重要数据或软件采用加密介质存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

A.5.4 设备管理

设备管理应满足如下要求：

a） 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理，每年至少维护一次。

b） 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理。

c） 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员

的责任、涉外维修和服务的审批、维修过程的监督控制等。

d） 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动（停止）、加电（断电）等操作。

e） 应确保信息处理设备必须经过审批才能带离机房或办公地点。

A.5.5 监控管理和安全管理中心

监控管理和安全管理中心应满足如下要求：

a） 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存。

b） 应组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施。

c） 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

A.5.6 网络安全管理

网络安全管理应满足如下要求：

a） 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

b） 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定。

c） 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份。

d） 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞及时修补。

e） 应实现设备的最小服务配置，并对配置文件进行定期离线备份。

f） 应保证所有与外部系统的连接均得到授权和批准。

g） 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入。

h） 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

A.5.7 系统安全管理

系统安全管理应满足如下要求：

a） 应根据业务需求和系统安全分析确定系统的访问控制策略。

b） 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

c） 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

d） 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面做出具体规定。

e） 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

f） 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

g） 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

A.5.8 恶意代码防范管理

恶意代码防范管理应满足如下要求：

a） 应提高所有用户的防病毒意识，及时告知防病毒软件版本。在读取移动存储设备上的数据以及网络上接收文件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查。
b） 应指定专人对网络和主机进行恶意代码检测并保存检测记录。
c） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等做出明确规定。
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、防病毒网关上截获的危险病毒或恶意代码进行及时分析处理并报告。

A.5.9 密码管理

密码管理应满足如下要求：
应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

A.5.10 变更管理

变更管理应满足如下要求：
a） 应确认系统中要发生的变更，并制定变更方案。
b） 应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告。
c） 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录。
d） 应建立中止变更并从失败变更中恢复的文件化程序，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。

A.5.11 备份与恢复管理

备份与恢复管理应满足如下要求：
a） 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。
b） 应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范。
c） 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，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。
d） 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。
e） 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

A.5.12 安全事件处置

安全事件处置应满足如下要求：
a） 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点。
b） 应制定安全事件报告和处置管理制度，明确安全事件的类型，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。
c） 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。
d） 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度以及处理方法等。
e） 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，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。

f） 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。

A.5.13 应急预案管理

应急预案管理应满足如下要求：

a） 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。

b） 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。

c） 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。

d） 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期。

e） 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

中 华 人 民 共 和 国
电 力 行 业 标 准
用电信息安全防护技术规范
DL / T 1527 — 2016
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）
北京九天众诚印刷有限公司印刷
*
2016 年 6 月第一版　　2016 年 6 月北京第一次印刷
880 毫米×1230 毫米　16 开本　1.5 印张　43 千字
印数 0001—1000 册
*
统一书号 155123・3054　定价 **13.00** 元

中国电力出版社官方微信　　掌上电力书屋

刮开涂层
查询真伪

155123.3054