

密、禁止关键技术扩散和设备行业专用等方面的内容。

## 8 第三级安全要求

### 8.1 安全通用要求

#### 8.1.1 安全物理环境

##### 8.1.1.1 物理位置选择

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。

##### 8.1.1.2 物理访问控制

机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。

##### 8.1.1.3 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识；
- b) 应将通信线缆铺设在隐蔽安全处；
- c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

##### 8.1.1.4 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) 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。

##### 8.1.1.5 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；
- 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。

##### 8.1.1.6 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。

##### 8.1.1.7 防静电

本项要求包括：

- a) 应采用防静电地板或地面并采用必要的接地防静电措施；

- b) 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。

#### 8.1.1.8 温湿度控制

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。

#### 8.1.1.9 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) 应设置冗余或并行的电力电缆线路为计算机系统供电。

#### 8.1.1.10 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。

### 8.1.2 安全通信网络

#### 8.1.2.1 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;
- 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采取可靠的技术隔离手段;
- 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。

#### 8.1.2.2 通信传输

本项要求包括:

- a) 应采用校验技术或密码技术保证通信过程中数据的完整性;
- b) 应采用密码技术保证通信过程中数据的保密性。

#### 8.1.2.3 可信验证

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。

### 8.1.3 安全区域边界

#### 8.1.3.1 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) 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;

- 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；
- d) 应限制无线网络的使用,保证无线网络通过受控的边界设备接入内部网络。

#### 8.1.3.2 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实现基于应用协议和应用内容的访问控制。

#### 8.1.3.3 入侵防范

本项要求包括:

- a) 应在关键网络节点处检测、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检测、防止或限制从内部发起的网络攻击行为;
- c) 应采取技术措施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;
- d) 当检测到攻击行为时,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。

#### 8.1.3.4 恶意代码和垃圾邮件防范

本项要求包括:

- a) 应在关键网络节点处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。

#### 8.1.3.5 安全审计

本项要求包括:

- a) 应在网络边界、重要网络节点进行安全审计,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;
- 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。

#### 8.1.3.6 可信验证

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。

### 8.1.4 安全计算环境

#### 8.1.4.1 身份鉴别

本项要求包括:

- a) 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换;
- b) 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,应采取必要措施防止鉴别信息在网络传输过程中被窃听;
- d) 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密码技术来实现。

#### 8.1.4.2 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) 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;
- 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) 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。

#### 8.1.4.3 安全审计

本项要求包括:

- a) 应启用安全审计功能,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;
- d) 应对审计进程进行保护,防止未经授权的中断。

#### 8.1.4.4 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) 应关闭不需要的系统服务、默认共享和高危端口;
- c) 应通过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) 应能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;
- f) 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。

#### 8.1.4.5 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断。

#### 8.1.4.6 可信验证

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。

#### 8.1.4.7 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传输过程中的完整性,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) 应采用校验技术或密码技术保证重要数据在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。

#### 8.1.4.8 数据保密性

本项要求包括：

- a) 应采用密码技术保证重要数据在传输过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等;
- b) 应采用密码技术保证重要数据在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。

#### 8.1.4.9 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;
- b) 应提供异地实时备份功能,利用通信网络将重要数据实时备份至备份场地;
- c) 应提供重要数据处理系统的冗余,保证系统的高可用性。

#### 8.1.4.10 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或重新分配前得到完全清除;
- b) 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。

#### 8.1.4.11 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) 应禁止未经授权访问和非法使用用户个人信息。

### 8.1.5 安全管理中心

#### 8.1.5.1 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。

#### 8.1.5.2 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) 应通过审计管理员对审计记录应进行分析,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。

### 8.1.5.3 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;
- 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。

### 8.1.5.4 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) 应能够建立一条安全的信息传输路径,对网络中的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) 应能对网络中发生的各类安全事件进行识别、报警和分析。

## 8.1.6 安全管理制度

### 8.1.6.1 安全策略

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。

### 8.1.6.2 管理制度

本项要求包括:

- a) 应对安全管理活动中的各类管理内容建立安全管理制度;
- b) 应对管理人员或操作人员执行的日常管理操作建立操作规程;
- 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。

### 8.1.6.3 制定和发布

本项要求包括:

- 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) 安全管理制度应通过正式、有效的方式发布,并进行版本控制。

### 8.1.6.4 评审和修订

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。

## 8.1.7 安全管理机构

### 8.1.7.1 岗位设置

本项要求包括：

- a) 应成立指导和管理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；
- 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) 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。

### 8.1.7.2 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) 应配备专职安全管理员，不可兼任。

### 8.1.7.3 授权和审批

本项要求包括：

- 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。

### 8.1.7.4 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，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。

### 8.1.7.5 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；
- 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。

## 8.1.8 安全管理人员

### 8.1.8.1 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。

#### 8.1.8.2 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,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。

#### 8.1.8.3 安全意识教育和培训

本项要求包括:

- a) 应对各类人员进行安全意识教育和岗位技能培训,并告知相关的安全责任和惩戒措施;
- b) 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;
- c) 应定期对不同岗位的人员进行技能考核。

#### 8.1.8.4 外部人员访问管理

本项要求包括:

- a) 应在外部人员物理访问受控区域前先提出书面申请,批准后由专人全程陪同,并登记备案;
- b) 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;
- c) 外部人员离场后应及时清除其所有的访问权限;
- d) 获得系统访问授权的外部人员应签署保密协议,不得进行非授权操作,不得复制和泄露任何敏感信息。

### 8.1.9 安全建设管理

#### 8.1.9.1 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。

#### 8.1.9.2 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;
- b) 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;
- c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件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。



### 8.1.9.3 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国家的有关规定；
- b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
- c) 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。

### 8.1.9.4 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,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) 应保证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；
- f) 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；
- g) 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。

### 8.1.9.5 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；
- b) 应保证开发单位提供软件设计文档和使用指南；
- c) 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。

### 8.1.9.6 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；
- c) 应通过第三方工程监理控制项目的实施过程。

### 8.1.9.7 测试验收

本项要求包括：

- a) 应制订测试验收方案,并依据测试验收方案实施测试验收,形成测试验收报告；
- b) 应进行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。

### 8.1.9.8 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) 应对负责运行维护的技术人员进行相应的技能培训；
- c) 应提供建设过程文档和运行维护文档。

#### 8.1.9.9 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;
- 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符合国家有关规定。

#### 8.1.9.10 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) 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;
- c) 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。

#### 8.1.10 安全运维管理

##### 8.1.10.1 环境管理

本项要求包括：

- a) 应指定专门的部门或人员负责机房安全,对机房出入进行管理,定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理;
- b) 应建立机房安全管理制度,对有关物理访问、物品带进出和环境安全等方面的管理作出规定;
- c) 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。

##### 8.1.10.2 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。

##### 8.1.10.3 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) 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。

##### 8.1.10.4 设备维护管理

本项要求包括：

- a) 应对各种设备(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;
- b) 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、维修和服务的审批、维修过程的监督控制等;
- c) 信息处理设备应经过审批才能带离机房或办公地点,含有存储介质的设备带出工作环境时其中重要数据应加密;