ICS 35.040
L80

中华人民共和国国家标准

GB/T 22239.1—XXXX

信息安全技术 网络安全等级保护基本要求

第1部分 安全通用要求

Information Security Technology- Baseline for Cybersecurity Classified Protection

Part1： Security General Requirements

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目次

前言

本部分由全国信息安全标准化技术委员会提出。

本部分由全国信息安全标准化技术委员会归口。

本部分起草单位：公安部信息安全等级保护评估中心、国家能源局信息中心、北京网御星云信息技术有限公司。

本部分主要起草人：马力、郭启全、陈广勇、曲洁、葛波蔚、于东升、袁静、陆磊、黎水林、黄顺京、张振峰、尹湘培、申永波、陶源。

引言

国家标准 GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求在开展信息安全等级保护工作的过程中起到了非常重要的作用,被广泛应用于各个行业和领域开展信息安全等级保护的建设整改和等级测评等工作，但是随着信息技术的发展，GB/T 22239-2008 在适用性、时效性、易用性、可操作性上需要进一步完善。

为了适应移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下信息安全等级保护工作的开展，需对 GB/T 22239-2008 进行修订，修订的思路和方法是针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域提出扩展的安全要求。

对 GB/T 22239-2008 的修订完成后，基本要求标准成为由多个部分组成的系列标准，目前主要有六个部分：

——GB/T22239.1-XXXX 信息安全技术 网络安全等级保护基本要求
第 1 部分 安全通用要求；

——GB/T 22239.2-XXXX 信息安全技术 网络安全等级保护基本要求
第 2 部分 云计算安全扩展要求；

——GB/T 22239.3-XXXX 信息安全技术 网络安全等级保护基本要求
第 3 部分 移动互联安全扩展要求；

——GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求
第 4 部分 物联网安全扩展要求；

——GB/T 22239.5-XXXX 信息安全技术 网络安全等级保护基本要求
第 5 部分 工业控制安全扩展要求。

——GB/T 22239.6-XXXX 信息安全技术 网络安全等级保护基本要求
第 6 部分 大数据安全扩展要求。

将来可能会随着技术的变化添加新的部分阐述特定领域的安全扩展要求。

本部分 GB/T 22239.1-XXXX 是对 GB/T 22239-2008 的修订。

在本部分文本中，黑体字表示较低等级中没有出现或增强的要求。

信息安全技术 网络安全等级保护基本要求

第 1 部分 安全通用要求

1 范围

本部分规定了不同等级保护对象的安全通用要求，对于采用移动互联、云计算、大数据、物联网和工业控制等新技术、新应用的保护对象，除使用本部分外还需参考其他的安全扩展要求。

本部分适用于指导分等级的非涉密保护对象的安全建设和监督管理。

2 规范性引用文件

下列文件中的条款通过在本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本部分。

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 25069-2010 信息安全技术术语

3 术语和定义

GB/T 25069-2010和GB 17859-1999确立的以及下列术语和定义适用于本部分。

3.1 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。

4 网络安全等级保护概述

4.1 不同等级的安全保护对象

安全等级保护对象是指等级保护工作中的保护对象，主要包括网络基础设施、信息系统、大数据、云计算平台、物联网、工控系统等；安全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，由低到高划分为五级。

第一级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

安全保护等级如表1所示。

表1　安全保护等级

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.2　不同等级的安全保护能力

不同等级的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，能够发现安全漏洞和安全事件，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，能够发现安全漏洞和安全事件，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）。

4.3　技术要求和管理要求

应依据保护对象的安全保护等级保证它们具有相应等级的安全保护能力，不同安全保护等级的保护对象要求具有不同的安全保护能力。

安全通用要求是针对不同安全保护等级对象应该具有的安全保护能力提出的安全要求，根据实现方式的不同，安全要求分为技术要求和管理要求两大类。技术类安全要求与提供的技术安全机制有关，主要通过部署软硬件并正确的配置其安全功能来实现；管理类安全要求与各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。关于各类安全要求的选择见附录 A。

安全通用要求从各个层面或方面提出了保护对象的每个组成部分应该满足的安全要求，等级保护对象具有的整体安全保护能力通过不同组成部分实现安全要求来保证。除了保证每个组成部分满足安全要求外，还要考虑组成部分之间的相互关系，来保证保护对象整体安全保护能力。关于等级保护对象整体安全保护能力的说明见附录 B。

5　第一级安全要求

5.1　技术要求

5.1.1 物理和环境安全

5.1.1.1 物理访问控制

机房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。

5.1.1.2 防盗窃和防破坏

应将机房设备或主要部件进行固定，并设置明显的不易除去的标记。

5.1.1.3 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

5.1.1.4 防火

机房应设置灭火设备。

5.1.1.5 防水和防潮

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

5.1.1.6 温湿度控制

机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内。

5.1.1.7 电力供应

应在机房供电线路上配置稳压器和过电压防护设备。

5.1.2 网络和通信安全

5.1.2.1 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基本业务需要；

b) 应保证接入网络和核心网络的带宽满足基本业务需要。

5.1.2.2 通信传输

应采用校验码技术保证通信过程中数据的完整性。

5.1.2.3 边界防护

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。

5.1.2.4 访问控制

本项要求包括：

a) 应在网络边界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。

5.1.3 设备和计算安全

5.1.3.1 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。

5.1.3.2 访问控制

本项要求包括：

a） 应对登录的用户分配账号和权限；

b） 应重命名默认账号或修改默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在。

5.1.3.3 入侵防范

本项要求包括：

a） 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；

b） 应关闭不需要的系统服务、默认共享和高危端口。

5.1.3.4 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

5.1.4 应用和数据安全

5.1.4.1 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，鉴别信息具有复杂度要求并定期更换；

b） 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

5.1.4.2 访问控制

本项要求包括：

a） 应提供访问控制功能，对登录的用户分配账号和权限；

b） 应重命名应用系统默认账号或修改这些账号的默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在。

5.1.4.3 软件容错

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。

5.1.4.4 数据完整性

应采用校验码技术保证重要数据在传输过程中的完整性。

5.1.4.5 数据备份恢复

应提供重要数据的本地数据备份与恢复功能。

5.2 管理要求

5.2.1 安全策略和管理制度

5.2.1.1 管理制度

应建立日常管理活动中常用的安全管理制度。

5.2.2 安全管理机构和人员

5.2.2.1 岗位设置

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。

5.2.2.2 人员配备

应配备一定数量的系统管理员、网络管理员、安全管理员等。

5.2.2.3 授权和审批

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。

5.2.2.4 人员录用

应指定或授权专门的部门或人员负责人员录用。

5.2.2.5 人员离岗

应及时终止离岗员工的所有访问权限，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。

5.2.2.6 安全意识教育和培训

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。

5.2.2.7 外部人员访问管理

应确保在外部人员访问受控区域前得到授权或审批。

5.2.3 安全建设管理

5.2.3.1 定级

应明确保护对象的边界和安全保护等级。

5.2.3.2 安全方案设计

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。

5.2.3.3 产品采购和使用

应确保信息安全产品采购和使用符合国家的有关规定。

5.2.3.4 工程实施

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。

5.2.3.5 测试验收

应进行安全性测试验收。

5.2.3.6 系统交付

本项要求包括：

a) 应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。

5.2.3.7 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与安全相关的协议，明确约定相关责任。

5.2.4 安全运维管理

5.2.4.1 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。

5.2.4.2 介质管理

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，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。

5.2.4.3 设备维护管理

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。

5.2.4.4 漏洞和风险管理

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。

5.2.4.5 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号管理，对申请账号、建立账号、删除账号等进行控制。

5.2.4.6 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。

5.2.4.7 备份与恢复管理

本项要求包括：

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） 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

5.2.4.8 安全事件处置

本项要求包括：

a） 应报告所发现的安全弱点和可疑事件；

b） 应明确安全事件的报告和处置流程，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。

6 第二级安全要求

6.1 技术要求

6.1.1 物理和环境安全

6.1.1.1 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。**

6.1.1.2 物理访问控制

本项要求包括：

a） 机房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；

6.1.1.3 防盗窃和防破坏

本项要求包括：

a） 应将机房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处，可铺设在地下或管道中。**

6.1.1.4 防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

6.1.1.5 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。**

6.1.1.6 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。**

6.1.1.7 防静电

应安装防静电地板并采用必要的接地防静电措施。

6.1.1.8 温湿度控制

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。

6.1.1.9 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。**

6.1.1.10 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

6.1.2 网络和通信安全

6.1.2.1 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） 应保证接入网络和核心网络的带宽**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网络边界处且没有边界防护措施。**

6.1.2.2 通信传输

应采用校验码技术保证通信过程中数据的完整性。

6.1.2.3 边界防护

应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。

6.1.2.4 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数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。**

6.1.2.5 入侵防范

应在关键网络节点处监视网络攻击行为。

6.1.2.6 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。**

6.1.3 设备和计算安全

6.1.3.1 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。**

6.1.3.2 访问控制

本项要求包括：

a） 应对登录的用户分配账号和权限；

b） 应重命名系统默认账号或修改这些账号的默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在；

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。**

6.1.3.3 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。**

6.1.3.4 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） **应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。**

6.1.3.5　恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

6.1.3.6　资源控制

应限制单个用户或进程对系统资源的最大使用限度。

6.1.4　应用和数据安全

6.1.4.1　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，鉴别信息具有复杂度要求并定期更换；

b）　应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；

c）　**应强制用户首次登录时修改初始口令；**

d）　**用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全。**

6.1.4.2　访问控制

本项要求包括：

a）　应提供访问控制功能，对登录的用户分配账号和权限；

b）　应重命名默认账号或修改默认口令；

c）　应及时删除或停用多余的、过期的账号，避免共享账号的存在。

6.1.4.3　安全审计

本项要求包括：

a）　**应提供安全审计功能，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。**

6.1.4.4　软件容错

本项要求包括：

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内容符合系统设定要求；

b）　**在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施。**

6.1.4.5　资源控制

本项要求包括：

a）　**当通信双方中的一方在一段时间内未作任何响应，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）　**应能够对单个账号的多重并发会话进行限制。**

6.1.4.6　数据完整性

应采用校验码技术保证重要数据在传输过程中的完整性。

6.1.4.7　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。**

6.1.4.8 剩余信息保护

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。

6.1.4.9 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、使用用户个人信息。**

6.2 管理要求

6.2.1 安全策略和管理制度

6.2.1.1 管理制度

本项要求包括：

a） **应对安全管理活动中的主要管理内容建立安全管理制度；**

b） **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。**

6.2.1.2 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。**

6.2.1.3 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。

6.2.2 安全管理机构和人员

6.2.2.1 岗位设置

本项要求包括：

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**定义部门**及各个工作岗位的职责。

6.2.2.2 人员配备

应配备一定数量的系统管理员、网络管理员、安全管理员等。

6.2.2.3 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执行审批过程。**

6.2.2.4 沟通和合作

本项要求包括：

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，定期召开协调会议，共同协作处理信息安全问题；**

b） **应加强与兄弟单位、公安机关、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。**

6.2.2.5　审核和检查

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。

6.2.2.6　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、背景、专业资格和资质等进行审查。

6.2.2.7　人员离岗

应及时终止离岗员工的所有访问权限，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。

6.2.2.8　安全意识教育和培训

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。

6.2.2.9　外部人员访问管理

本项要求包括：

a)　应确保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)　应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、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。

6.2.3　安全建设管理

6.2.3.1　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边界、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)　应确保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。

6.2.3.2　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进行安全方案设计；

c)　**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。**

6.2.3.3　产品采购和使用

本项要求包括：

a)　应确保信息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。**

6.2.3.4　自行软件开发

本项要求包括：

a)　**应确保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） **应确保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。**

6.2.3.5 外包软件开发

本项要求包括：

a） **应在软件交付前检测软件质量和其中可能存在的恶意代码；**

b） **应要求开发单位提供软件设计文档和使用指南。**

6.2.3.6 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） **应制定工程实施方案控制安全工程实施过程。**

6.2.3.7 测试验收

本项要求包括：

a） **在制订测试验收方案，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。**

6.2.3.8 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） **应确保提供建设过程中的文档和指导用户进行运行维护的文档。**

6.2.3.9 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） **应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。**

6.2.3.10 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信息安全相关义务。**

6.2.4 安全运维管理

6.2.4.1 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；

c） **应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等。**

6.2.4.2 资产管理

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。

6.2.4.3 介质管理

本项要求包括：

a) 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，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。**

6.2.4.4 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、涉外维修和服务的审批、维修过程的监督控制等。**

6.2.4.5 漏洞和风险管理

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。

6.2.4.6 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号管理，对申请账号、建立账号、删除账号等进行控制；

c) **应建立网络和系统安全管理制度，对安全策略、账号管理、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。**

6.2.4.7 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。

6.2.4.8 配置管理

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。

6.2.4.9 密码管理

本项要求包括：

a) **应使用符合国家密码管理规定的密码技术和产品；**

b) **应按照国家密码管理的要求开展密码技术和产品的应用。**

6.2.4.10 变更管理

应明确系统变更需求，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。

6.2.4.11 备份与恢复管理

本项要求包括：

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） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

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、备份程序和恢复程序等。**

6.2.4.12 安全事件处置

本项要求包括：

a） 应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。**

6.2.4.13 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。**

6.2.4.14 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。**

7 第三级安全要求

7.1 技术要求

7.1.1 物理和环境安全

7.1.1.1 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。

7.1.1.2 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。

7.1.1.3 防盗窃和防破坏

本项要求包括：

a） 应将机房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处，可铺设在地下或管道中；

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。**

7.1.1.4 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。**

7.1.1.5 防火

本项要求包括：

a） 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。**

7.1.1.6 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。**

7.1.1.7 防静电

本项要求包括：

a） 应安装防静电地板并采用必要的接地防静电措施；

b） **应采用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。**

7.1.1.8 温湿度控制

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。

7.1.1.9 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。**

7.1.1.10 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。**

7.1.2 网络和通信安全

7.1.2.1 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网络边界处且没有边界防护措施；

e） **应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。**

7.1.2.2 通信传输

本项要求包括：

a） 应采用校验码技术**或加解密技术**保证通信过程中数据的完整性；

b） **应采用加解密技术保证通信过程中敏感信息字段或整个报文的保密性**。

7.1.2.3 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防护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限制或检查；**

c) **应能够对内部用户非授权联到外部网络的行为进行限制或检查；**

d) **应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。**

7.1.2.4 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，控制粒度为端口级；

e) **应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。**

7.1.2.5 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和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未知的新型网络攻击的检测和分析；**

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

7.1.2.6 恶意代码防范

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。**

7.1.2.7 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) **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；**

e) **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。**

7.1.2.8 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；**

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。**

7.1.3 设备和计算安全

7.1.3.1 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） **应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。**

7.1.3.2 访问控制

本项要求包括：

a） 应对登录的用户分配账号和权限；

b） 应重命名默认账号或修改默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在；

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） **应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。**

7.1.3.3 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；**

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 。**

7.1.3.4 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） 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

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。**

7.1.3.5 恶意代码防范

应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

7.1.3.6　资源控制

本项要求包括：

a）　应限制单个用户或进程对系统资源的最大使用限度；

b）　**应提供重要节点设备的硬件冗余，保证系统的可用性；**

c）　**应对重要节点进行监视，包括监视CPU、硬盘、内存等资源的使用情况；**

d）　**应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。**

7.1.4　应用和数据安全

7.1.4.1　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，鉴别信息具有复杂度要求并定期更换；

b）　应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；

c）　应强制用户首次登录时修改初始口令；

d）　用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；

e）　**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。**

7.1.4.2　访问控制

本项要求包括：

a）　应提供访问控制功能，对登录的用户分配账号和权限；

b）　应重命名默认账号或修改这些账号的默认口令；

c）　应及时删除或停用多余的、过期的账号，避免共享账号的存在；

d）　**应授予不同账号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，客体为文件、数据库表级、记录或字段级；**

g）　**应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。**

7.1.4.3　安全审计

本项要求包括：

a）　应提供安全审计功能，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；**

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。**

7.1.4.4　软件容错

本项要求包括：

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内容符合系统设定要求；

b）　在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；

c） **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。**

7.1.4.5　资源控制

本项要求包括：

a） 当通信双方中的一方在一段时间内未作任何响应，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） 应能够对单个账号的多重并发会话进行限制；

d） **应能够对并发进程的每个进程占用的资源分配最大限额。**

7.1.4.6　数据完整性

本项要求包括：

a） 应采用校验码技术**或加解密技术**保证重要数据在传输过程中的完整性；

b） **应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性。**

7.1.4.7　数据保密性

本项要求包括：

a） **应采用加解密技术保证重要数据在传输过程中的保密性；**

b） **应采用加解密技术保证重要数据在存储过程中的保密性。**

7.1.4.8　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**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热冗余，保证系统的高可用性。**

7.1.4.9　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。**

7.1.4.10　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使用用户个人信息。

7.2　管理要求

7.2.1　安全策略和管理制度

7.2.1.1　安全策略

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。

7.2.1.2　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；

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信息安全管理制度体系。**

7.2.1.3 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。

7.2.1.4 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。

7.2.2 安全管理机构和人员

7.2.2.1 岗位设置

本项要求包括：

a） **应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；

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

7.2.2.2 人员配备

本项要求包括：

a） 应配备一定数量的系统管理员、网络管理员、安全管理员等；

b） **应配备专职安全管理员，不可兼任。**

7.2.2.3 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。**

7.2.2.4 沟通和合作

本项要求包括：

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，定期召开协调会议，共同协作处理信息安全问题；

b） 应加强与兄弟单位、公安机关、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。

7.2.2.5 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。**

7.2.2.6　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）　对被录用人员的身份、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。

7.2.2.7　人员离岗

本项要求包括：

a）　应及时终止离岗员工的所有访问权限，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。

7.2.2.8　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，对信息安全基础知识、岗位操作规程等进行培训。

7.2.2.9　外部人员访问管理

本项要求包括：

a）　应确保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）　应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、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。

7.2.3　安全建设管理

7.2.3.1　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边界、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）　应确保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。

7.2.3.2　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，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。**

7.2.3.3　产品采购和使用

本项要求包括：

a） 应确保信息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。**

7.2.3.4 自行软件开发

本项要求包括：

a） 应确保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） **应确保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） 应确保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） **应确保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） **应确保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。**

7.2.3.5 外包软件开发

本项要求包括：

a） 应在软件交付前检测软件质量和其中可能存在的恶意代码；

b） 应要求开发单位提供软件设计文档和使用指南；

c） 应要求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。

7.2.3.6 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） 应制定工程实施方案控制安全工程实施过程；

c） **应通过第三方工程监理控制项目的实施过程。**

7.2.3.7 测试验收

本项要求包括：

a） 在制订测试验收方案，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。

7.2.3.8 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） 应确保提供建设过程中的文档和指导用户进行运行维护的文档。

7.2.3.9 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） 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

7.2.3.10 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信息安全相关义务；

c） **应定期监视、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。**

7.2.4 安全运维管理

7.2.4.1 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；

c） 应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等。

7.2.4.2 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。**

7.2.4.3 介质管理

本项要求包括：

a） 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，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。

7.2.4.4 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、涉外维修和服务的审批、维修过程的监督控制等；

c） **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，含有存储介质的设备带出工作环境时其中重要数据必须加密；**

d） **含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用。**

7.2.4.5 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。**

7.2.4.6 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号管理，对申请账号、建立账号、删除账号等进行控制；

c） 应建立网络和系统安全管理制度，对安全策略、账号管理、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；**

g） **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；**

h） **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；**

i） **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。**

7.2.4.7 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；

c） **应定期验证防范恶意代码攻击的技术措施的有效性。**

7.2.4.8 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。**

7.2.4.9 密码管理

本项要求包括：

a） 应使用符合国家密码管理规定的密码技术和产品。

7.2.4.10 变更管理

本项要求包括：

a） 应明确变更需求，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） **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；**

c） **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。**

7.2.4.11 备份与恢复管理

本项要求包括：

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） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

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、备份程序和恢复程序等。

7.2.4.12 安全事件处置

本项要求包括：

a） 应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漏的重大安全事件应采用不同的处理程序和报告程序。**

7.2.4.13 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，并在此框架下制定不同事件的应急预案，包括启动预案的条件、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；

d） **应定期对原有的应急预案重新评估，修订完善。**

7.2.4.14 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） **应确保选择的外包运维服务商在技术和管理方面均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。**

8 第四级安全要求

8.1 技术要求

8.1.1 物理和环境安全

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

本项要求包括：

a） 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；

b） **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。**

8.1.1.3 防盗窃和防破坏

本项要求包括：

a） 应将机房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处，可铺设在地下或管道中；

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） 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） 应安装防静电地板并采用必要的接地防静电措施；

b） 应采用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

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。

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；

d） **应提供应急供电设施。**

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） **应对关键设备或关键区域实施电磁屏蔽。**

8.1.2 网络和通信安全

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网络边界处且没有边界防护措施；

e） 应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性；

f） **应可按照业务服务的重要程度分配带宽，优先保障重要业务。**

8.1.2.2 通信传输

本项要求包括：

a） 应采用校验码技术或加解密技术保证通信过程中数据的完整性；

b） 应采用加解密技术保证通信过程中敏感信息字段或整个报文的保密性；

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） **应基于硬件设备对重要通信过程进行加解密运算和密钥管理。**

8.1.2.3 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防护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限制或检查，**并对其进行有效阻断；**

c） 应能够对内部用户非授权联到外部网络的行为进行限制或检查，**并对其进行有效阻断；**

d） 应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络；

e） **应能够对连接到内部网络的设备进行可信验证，确保接入网络的设备真实可信**。

8.1.2.4 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） **应不允许数据带通用协议通过。**

8.1.2.5 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和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未知的新型网络攻击的检测和分析；

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

8.1.2.6 恶意代码防范

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。

8.1.2.7 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） 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。

8.1.2.8 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；

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。

8.1.3 设备和计算安全

8.1.3.1 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） 应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别。

8.1.3.2 访问控制

本项要求包括：

a） 应对登录的用户分配账号和权限；

b） 应重命名默认账号或修改默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在；

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） **应对所有主体、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。**

8.1.3.3 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、时间、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；

d） 应对审计进程进行保护，防止未经授权的中断；

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。

8.1.3.4 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） 应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；

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。

8.1.3.5 恶意代码防范

应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

8.1.3.6 资源控制

本项要求包括：

a） 应限制单个用户或进程对系统资源的最大使用限度；

b） 应提供重要节点设备的硬件冗余，保证系统的可用性；

c） 应对重要节点进行监视，包括监视CPU、硬盘、内存等资源的使用情况；

d） 应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

8.1.4 应用和数据安全

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，鉴别信息具有复杂度要求并定期更换；

b） 应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；

c） 应强制用户首次登录时修改初始口令；

d） 用户身份鉴别信息丢失或失效时，应采用鉴别信息重置或其他技术措施保证系统安全；

e） 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；

f） **登录用户执行重要操作时应再次进行身份鉴别。**

8.1.4.2 访问控制

本项要求包括：

a） 应提供访问控制功能，对登录的用户分配账号和权限；

b） 应重命名默认账号或修改这些账号的默认口令；

c） 应及时删除或停用多余的、过期的账号，避免共享账号的存在；

d） 应授予不同账号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，客体为文件、数据库表级、记录或字段级；

g） **应对所有主体、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。**

8.1.4.3 安全审计

本项要求包括：

a） 应提供安全审计功能，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、时间、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；

d） 应对审计进程进行保护，防止未经授权的中断；

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。

8.1.4.4 软件容错

本项要求包括：

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内容符合系统设定要求；

b） 在故障发生时，应能够继续提供一部分功能，确保能够实施必要的措施；

c） 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。

8.1.4.5 资源控制

本项要求包括：

a） 当通信双方中的一方在一段时间内未作任何响应，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） 应能够对单个账号的多重并发会话进行限制；

d） 应能够对并发进程的每个进程占用的资源分配最大限额。

8.1.4.6 数据完整性

本项要求包括：

a） 应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性；

b） 应采用校验码技术或加解密技术保证重要数据在存储过程中的完整性；

c） 应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据完整性。

8.1.4.7 数据保密性

本项要求包括：

a） 应采用加解密技术保证重要数据在传输过程中的保密性；

b） 应采用加解密技术保证重要数据在存储过程中的保密性；

c） **应对重要数据传输提供专用通信协议或安全通信协议，避免来自基于通用通信协议的攻击破坏数据保密性。**

8.1.4.8 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热冗余，保证系统的高可用性；

d） **应建立异地灾难备份中心，提供业务应用的实时切换。**

8.1.4.9 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。

8.1.4.10 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信息；

b） 应禁止未授权访问和使用用户信息。

8.2 管理要求

8.2.1 安全策略和管理制度

8.2.1.1 安全策略

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。

8.2.1.2 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；

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信息安全管理制度体系。

8.2.1.3 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。

8.2.1.4 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。

8.2.2 安全管理机构和人员

8.2.2.1 岗位设置

本项要求包括：

a） 应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；

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

8.2.2.2 人员配备

本项要求包括：

a） 应配备一定数量的系统管理员、网络管理员、安全管理员等；

b） 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。**

8.2.2.3 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。

8.2.2.4 沟通和合作

本项要求包括：

a） 应加强与兄弟单位、公安机关、各类供应商、业界专家及安全组织的合作与沟通；

b） 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。

8.2.2.5 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。

8.2.2.6 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） 对被录用人员的身份、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；

d） 应从内部人员中选拔从事关键岗位的人员。

8.2.2.7 人员离岗

本项要求包括：

a） 应及时终止离岗员工的所有访问权限，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。

8.2.2.8 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，对信息安全基础知识、岗位操作规程等进行培训。

8.2.2.9 外部人员访问管理

本项要求包括：

a） 应确保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） 应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、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；

e） 对关键区域或关键系统不允许外部人员访问。

8.2.3 安全建设管理

8.2.3.1 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边界、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） 应确保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。

8.2.3.2 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，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。

8.2.3.3 产品采购和使用

本项要求包括：

a） 应确保信息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；

d） 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。

8.2.3.4 自行软件开发

本项要求包括：

a） 应确保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） 应确保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） 应确保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） 应确保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） 应确保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。

8.2.3.5 外包软件开发

本项要求包括：

a） 应在软件交付前检测软件质量和其中可能存在的恶意代码；

b） 应要求开发单位提供软件设计文档和使用指南；

c） 应要求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。

8.2.3.6 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） 应制定工程实施方案控制安全工程实施过程；

c） 应通过第三方工程监理控制项目的实施过程。

8.2.3.7 测试验收

本项要求包括：

a） 在制订测试验收方案，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。

8.2.3.8 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） 应确保提供建设过程中的文档和指导用户进行运行维护的文档。

8.2.3.9 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） 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

8.2.3.10 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信息安全相关义务；

c） 应定期监视、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。

8.2.4 安全运维管理

8.2.4.1 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；

c） 应不在重要区域接待来访人员和桌面上没有包含敏感信息的纸档文件、移动介质等；

d） 应对出入人员进行相应级别的授权，对进入重要安全区域的人员和活动实时监视等。

8.2.4.2 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。

8.2.4.3 介质管理

本项要求包括：

a) 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，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。

8.2.4.4 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、涉外维修和服务的审批、维修过程的监督控制等；

c) 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，含有存储介质的设备带出工作环境时其中重要数据必须加密；

d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，确保该设备上的敏感数据和授权软件无法被恢复重用。

8.2.4.5 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。

8.2.4.6 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号管理，对申请账号、建立账号、删除账号等进行控制；

c) 应建立网络和系统安全管理制度，对安全策略、账号管理、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；

g) 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；

h) 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；

i) 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。

8.2.4.7 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；

c） 应定期验证防范恶意代码攻击的技术措施的有效性。

8.2.4.8 配置管理

本项要求包括：

a） 应记录和保存系统的基本配置信息，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系统变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

8.2.4.9 密码管理

本项要求包括：

a） 应使用符合国家密码管理规定的密码技术和产品；

8.2.4.10 变更管理

本项要求包括：

a） 应明确变更需求，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） 应建立变更的申报和审批控制程序，依据程序控制系统所有的变更，记录变更实施过程；

c） 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。

8.2.4.11 备份与恢复管理

本项要求包括：

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） 应规定备份信息的备份方式、备份频度、存储介质、保存期等；

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、备份程序和恢复程序等。

8.2.4.12 安全事件处置

本项要求包括：

a） 应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漏的重大安全事件应采用不同的处理程序和报告程序。

8.2.4.13 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，并在此框架下制定不同事件的应急预案，包括启动预案的条件、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；

d） 应定期对原有的应急预案重新评估，修订完善。

8.2.4.14 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） 应确保选择的外包运维服务商在技术和管理方面均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。

9 第五级安全要求

（略）。

附录A
（规范性附录）
安全要求的选择和使用

等级保护对象由于承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同等级的保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的；即使相同等级的保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

保护对象定级后，不同安全保护等级的对象可能形成的定级结果组合见表 A.1。

表A.1 各等级保护对象定级结果组合

安全保护等级	定级结果的组合
第一级	S1A1G1
第二级	S1A2G2，S2A2G2，S2A1G2
第三级	S1A3G3，S2A3G3，S3A3G3，S3A2G3，S3A1G3
第四级	S1A4G4，S2A4G4，S3A4G4，S4A4G4，S4A3G4，S4A2G4，S4A1G4
第五级	S1A5G5，S2A5G5，S3A5G5，S4A5G5，S5A4G5，S5A3G5，S5A2G5，S5A1G5

安全保护措施的选择应依据上述定级结果，本部分中的技术安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；其他通用安全保护类要求（简记为 G），所有管理安全要求均为通用安全保护类要求。

表A.2安全要求及属性标识

技术/管理	分类	安全控制点	属性标识
安全技术要求	物理和环境安全	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G

		温湿度控制	G
		电力供应	A
		电磁防护	S
	网络和通信安全	网络架构	G
		通信传输	G
		边界防护	G
		访问控制	G
		入侵防范	G
		恶意代码防范	G
		安全审计	G
		集中管控	G
	设备和计算安全	身份鉴别	S
		访问控制	S
		安全审计	G
		入侵防范	G
		恶意代码防范	G
		资源控制	A
	应用和数据安全	身份鉴别	S
		访问控制	S
		安全审计	G
		软件容错	A
		资源控制	A
		数据完整性	S
		数据保密性	S
		数据备份恢复	A
		剩余信息保护	S
		个人信息保护	S
安全管理要求	安全策略和管理制度	安全策略	G
		管理制度	G
		制定和发布	G
		评审和修订	G

	安全管理机构和人员	岗位设置	G
		人员配备	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G
		人员录用	G
		人员离岗	G
		安全意识教育和培训	G
		外部人员访问管理	G
	安全建设管理	定级和备案	G
		安全方案设计	G
		产品采购和使用	G
		自行软件开发	G
		外包软件开发	G
		工程实施	G
		测试验收	G
		系统交付	G
		等级测评	G
		服务供应商管理	G
	安全运维管理	环境管理	G
		资产管理	G
		介质管理	G
		设备维护管理	G
		漏洞和风险管理	G
		网络与系统安全管理	G
		恶意代码防范管理	G
		配置管理	G
		密码管理	G
		变更管理	G
		备份与恢复管理	G
		安全事件处置	G
		应急预案管理	G

		外包运维管理	G

对于确定了安全保护等级的保护对象，应依据表 A.1 的定级结果，结合表 A.2 使用安全通用要求，应按照以下过程进行安全要求的选择：

1、根据保护对象的等级选择安全要求，包括技术要求和管理要求。方法是根据本部分，一级选择第一级安全要求，二级选择第二级安全要求，三级选择第三级安全要求，四级选择第四级安全要求，以此作为出发点。

2、根据定级结果，基于表 A.1 和表 A.2 对安全要求进行调整。根据系统服务保证性等级选择相应等级的系统服务保证类（A 类）安全要求；根据业务信息安全性等级选择相应等级的业务信息安全类（S 类）安全要求。

3、针对不同行业或不同对象的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的安全要求或补充安全要求。对于本部分中提出的安全要求无法实现或有更加有效的安全措施可以替代的，可以对安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

总之，保证不同安全保护等级的对象具有相应级别的安全保护能力，是安全等级保护的核心。选用本部分中提供的安全要求是保证保护对象具备一定安全保护能力的一种途径和出发点，在此出发点的基础上，可以参考等级保护的其它相关标准和安全方面的其它相关标准，调整和补充安全要求，从而实现保护对象在满足等级保护安全要求基础上，又具有自身特点的保护。

附录B
（规范性附录）
关于保护对象整体安全保护能力的要求

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。本部分第 4 章提出了不同安全保护等级保护对象的安全保护能力要求，第 5 章到第 9 章分别针对不同安全保护等级保护对象应该具有的安全保护能力提出了相应的安全要求，满足安全通用要求是保证保护对象具有相应等级的安全保护能力的前提。

依据本部分分层面采取各种安全措施时，还应考虑以下总体性要求，保证保护对象的整体安全保护能力。

1、构建纵深的防御体系

本部分从技术和管理两个方面提出安全要求，在采取由点到面的各种安全措施时，在整体上还应保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证保护对象整体的安全保护能力。应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次落实本部分中提到的各种安全措施，形成纵深防御体系。

2、采取互补的安全措施

本部分以安全控制的形式提出安全通用要求，在将各种安全控制落实到特定保护对象中时，应考虑各个安全控制之间的互补性，关注各个安全控制在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，保证各个安全控制共同综合作用于保护对象上，使得保护对象的整体安全保护能力得以保证。

3、保证一致的安全强度

本部分将安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到保护对象的各个层面，在实现各个层面安全功能时，应保证各个层面安全功能实现强度的一致性。应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上消弱。如要实现双因子身份鉴别，则应在各个层面的身份鉴别上均实现双因子身份鉴别；要实现基于标记的访问控制，则应保证在各个层面均实现基于标记的访问控制，并保证标记数据在整个保护对象内部流动时标记的唯一性等。

4、建立统一的支撑平台

本部分针对较高级别的保护对象，提到了使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术或可信技术，为了保证保护对象的整体安全防护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。

5、进行集中的安全管理

本部分针对较高级别的保护对象，提到了构建安全管理中心，实现集中的安全管理、安全监控和安

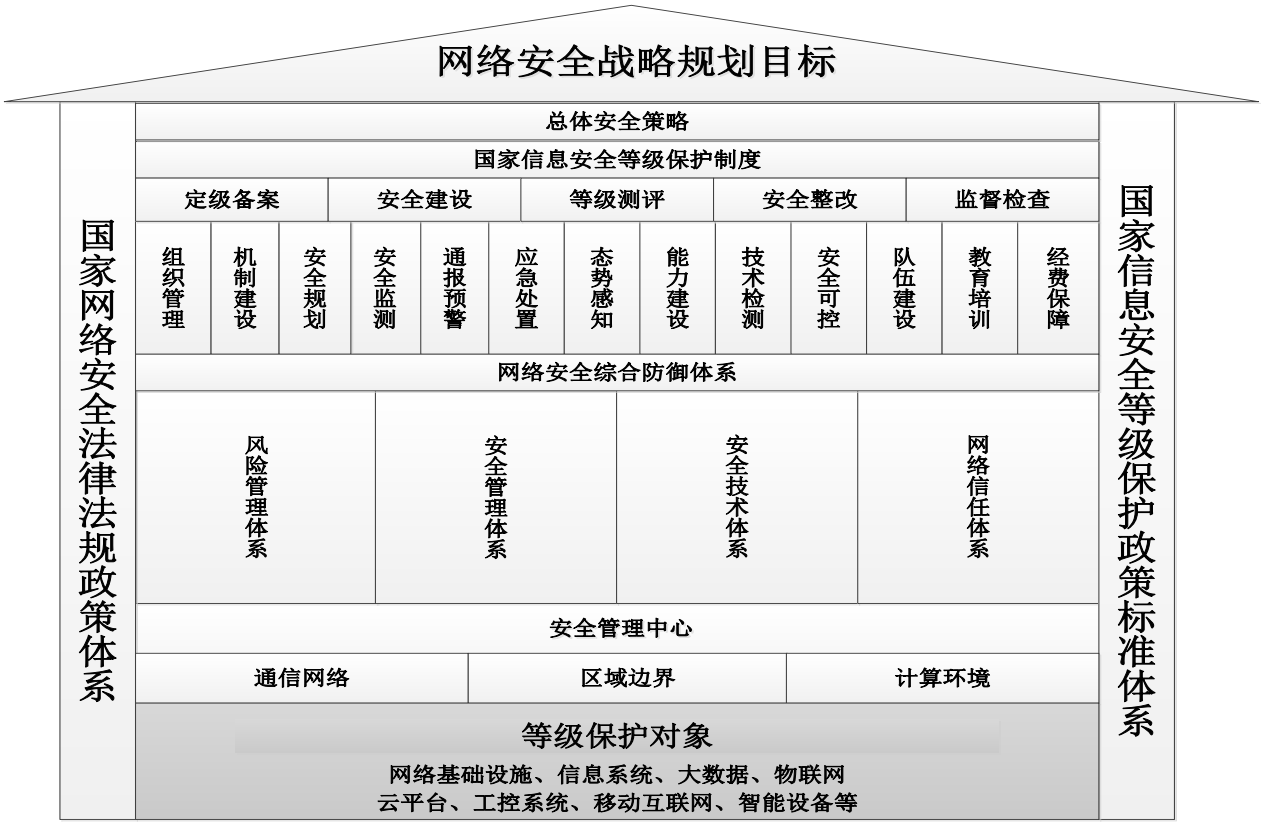
全审计等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制在可控情况下发挥各自的作用，应建立集中的管控中心，集中管理保护对象中的各个安全控制组件，支持统一安全管理。

附录C

（资料性附录）

等级保护安全框架和关键技术

在开展网络安全等级保护工作中应首先明确等级保护对象，等级保护对象包括网络基础设施、信息系统、大数据、云计算平台、物联网、工控系统等；确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。应依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、教育培训和经费保障等工作。



图C.1 等级保护安全框架

应在较高级别等级保护对象的安全建设和安全整改中注重使用一些关键技术：

1、可信计算技术

应针对计算资源构建保护环境，以可信计算基(TCB)为基础，实现软硬件计算资源可信；针对信息资源构建业务流程控制链，以访问控制为核心，实行主体按策略规则访问客体，实现数据信息访问可控；

强调最小权限管理，尤其是高等级保护对象实行三权分离管理体制，构建以可信技术为基础的等级保护核心技术体系。

2、强制访问控制

应确保在高等级保护对象中使用强制访问控制机制，强制访问控制机制需要总体设计、全局考虑，在通信网络、操作系统、应用系统各个方面实现访问控制标记和策略，进行统一的主客体安全标记，安全标记随数据全程流动，并在不同访问控制点之间实现访问控制策略的关联，构建各个层面强度一致的访问控制体系。

3、审计追查技术

应立足于现有的大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术，解决海量数据处理瓶颈，通过对审计数据快速提取，满足信息处理中对于检索速度和准确性的需求；同时，还应建立事件分析模型，发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查。

4、结构化保护技术

应通过良好的模块结构与层次设计等方法来保证具有相当的抗渗透能力，为安全功能的正常执行提供保障。高等级保护对象应确保安全功能可以形式表述、不可被篡改、不可被绕转，隐蔽信道不可被利用，通过保障安全功能的正常执行，使系统具备源于自身结构的、主动性的防御能力，利用可信技术实现结构化保护。

5、多级互联技术

应在保证各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互。随着对结构网络化和业务应用分布化动态性要求越来越高，多级互联技术应在不破坏原有等级保护对象正常运行和安全的前提下，实现不同级别之间的多级安全互联、互通和数据交换。

参考文献

[1] ISO/IEC 27000-2013 信息安全管理体系 概述和术语
[2] ISO/IEC 27001-2013 信息安全管理体系 要求
[3] ISO/IEC 27002-2013 信息安全管理实用规则
[4] ISO/IEC 27003-2013 信息安全管理体系实施指南
[5] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[6] GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
[7] NIST Special Publication 800-53 联邦信息系统和组织的安全和隐私控制