ICS 35.240.01
A 90
备案号：50662—2015

YZ

中华人民共和国邮政行业标准

YZ/T 0152—2016

邮政业信息系统安全等级保护基本要求

Basic requirements of classified protection for postal industry information system

2016-11-02 发布　　2017-02-01 实施

国家邮政局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家邮政局提出。

本标准由全国邮政业标准化技术委员会(SAC/TC 462)归口。

本标准起草单位:顺丰速运有限公司、深圳职业技术学院。

本标准主要起草人:田民、刘新凯、谢朝海、黄鹏程、熊莹、潘盛合、彭波、刘玉霞、林苏毅、龙军。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发〔2003〕27号)、《关于信息安全等级保护工作的实施意见》(公通字〔2004〕66号)和《信息安全等级保护管理办法》(公通字〔2007〕43号),制定本标准。

本标准是邮政业信息系统安全等级保护相关系列标准之一。

本标准传承了GB/T 22239—2008以安全保护能力为目标、分级保护的基本编制思路。结合邮政业实际情况,本标准在保留GB/T 22239—2008信息安全类S、服务保证类A、通用安全保护类G三类安全要求的基础上,增加了邮政业增强保护类P的安全要求,并参考行业内一些企事业单位的实践经验,对部分控制项进行了细化。

邮政业信息系统安全等级保护基本要求

1 范围

本标准规定了邮政业不同安全保护等级信息系统的基本保护要求,包括基本技术要求和基本管理要求。

本标准适用于邮政业信息系统的安全建设、安全检查和监督管理。

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/T 5271.8 信息技术 词汇 第8部分:安全(GB/T 5271.8—2001,idt ISO/IEC 2382—8:1998)

GB/T 10757—2011 邮政业术语

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南

GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

YZ/T 0142—2015 邮政业信息系统安全等级保护定级指南

3 术语和定义

GB/T 5271.8、GB 17859—1999 和 YZ/T 0142—2015 界定的以及下列术语和定义适用于本文件。

3.1

业务移动终端 business mobile terminal

邮政行业在提供寄递服务及实施行业管理等过程中使用的智能手机、平板电脑、手持终端等移动设备。

4 邮政业信息系统安全保护能力

4.1 安全保护能力

不同安全保护等级的信息系统应具备与其安全等级相适应的基本安全保护能力。邮政业信息系统各级安全保护能力要求见表1。

表 1　邮政业信息系统各级安全保护能力要求

级别代码	级　　别	要　　求
1	第一级安全保护能力	(1)能够防护系统免受来自个人的、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; (2)在系统遭到损害后,能够恢复部分功能
2	第二级安全保护能力	(1)能够防护系统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; (2)了解系统的安全状态,能够发现重要的安全漏洞和安全事件; (3)在系统遭到损害后,能够在一段时间内恢复部分功能
3	第三级安全保护能力	(1)能够在统一安全策略下,防护系统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; (2)能够发现安全漏洞和安全事件,评估系统的安全状态; (3)在系统遭到损害后,能够较快恢复绝大部分功能
4	第四级安全保护能力	(1)能够在统一安全策略下,防护系统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; (2)能够发现安全漏洞和安全事件,实时动态评估系统的安全状态; (3)在系统遭到损害后,能够迅速恢复所有功能
5	第五级安全保护能力	略

4.2　基本安全要求的四种类型

基本安全要求分为技术要求和管理要求两大类。技术类安全要求主要通过在信息系统中部署软硬件并正确配置其安全功能来实现;管理类安全要求主要通过控制各种角色的活动,并对制度、流程、记录等方面作出规定来实现。

技术要求和管理要求根据保护内容的不同分为四种类型,具体类型见表 2。其中,字母表示安全要求的类型,数字表示适用的安全保护等级。各类安全要求的选择和使用见附录 A。

表 2　基本安全要求的四种类型

类型代码	安全要求的类型名称	用　　途
S	信息安全类	主要用于保障业务信息安全
A	服务保证类	主要用于保障保证系统服务安全
G	通用安全保护类	适用于保障业务信息安全与系统服务安全
P	邮政业增强保护类	邮政业特有的要求,适用于保障业务信息安全与系统服务安全

5 第一级基本要求

5.1 技术要求

5.1.1 物理安全

5.1.1.1 物理访问控制(G1)

机房出入应安排专人负责,控制、鉴别和记录进入机房的人员。

5.1.1.2 防盗窃和防破坏(G1)

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。

5.1.1.3 防雷击(G1)

机房建筑应设置避雷装置。

5.1.1.4 防火(G1)

机房应配置灭火设备。

5.1.1.5 防水和防潮(G1)

a) 应对穿过机房墙壁和楼板的水管增加保护措施;

b) 应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(G1)

机房的温、湿度应控制在设备运行所要求的范围之内。

5.1.1.7 电力供应(A1)

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 网络安全

5.1.2.1 结构安全(G1)

a) 关键网络设备的业务处理能力应满足基本业务需要;

b) 接入网络和核心网络的带宽应满足基本业务需要;

c) 应绘制与当前运行情况相符的网络拓扑结构图。

5.1.2.2 访问控制(G1)

a) 应在网络边界设置访问控制设备,启用访问控制功能;

b) 应根据访问控制列表对源地址、目的地址、源端口、目的端口和协议等进行检查,以允许或拒绝相关数据包出入;

c) 应通过访问控制列表允许或拒绝用户访问系统资源,控制粒度至少为用户组。

5.1.2.3 网络设备防护(G1)

a) 应对登录网络设备的用户进行身份鉴别;

b) 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网络登录连接超时自动退出等措施;

c) 对网络设备进行远程管理时,应采取措施防止用户鉴别信息在网络传输过程中被窃听。

5.1.3 主机安全

5.1.3.1 身份鉴别(S1)

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。

5.1.3.2 访问控制(S1)

a) 应启用访问控制功能,依据安全策略控制用户对系统资源的访问;

b) 应限制默认账户的访问权限,重新命名系统默认账户,修改这些账户的默认口令;

c) 应及时删除多余的、过期的账户,避免共享账户的存在。

5.1.3.3 入侵防范(G1)

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,并及时更新系统补丁。

5.1.3.4 恶意代码防范(G1)

应安装防恶意代码软件,并及时更新防恶意代码软件版本和恶意代码库。

5.1.4 应用安全

5.1.4.1 身份鉴别(S1)

a) 应具有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自动退出等措施;

c) 应启用身份鉴别和登录失败处理功能,并根据安全策略配置相关参数。

5.1.4.2 访问控制(S1)

a) 应具有访问控制功能,控制用户组/用户访问系统功能和用户数据;

b) 应由授权主体配置访问控制策略,并严格限制默认用户的访问权限。

5.1.4.3 通信完整性(S1)

应约定通信会话方式,保证通信过程中数据的完整性。

5.1.4.4 软件容错(A1)

应具有数据有效性检验功能,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应符合系统设定要求。

5.1.5 数据安全及备份恢复

5.1.5.1 数据完整性(S1)

应能够检测到重要用户数据的完整性在传输过程中受到破坏。

5.1.5.2 备份和恢复(A1)

应能够对重要信息进行备份和恢复。

5.2 管理要求

5.2.1 安全管理制度

5.2.1.1 管理制度(G1)

应建立日常管理活动中常用的安全管理制度。

5.2.1.2 制定和发布(G1)

a) 应指定或授权专门的人员负责安全管理制度的制定;

b) 应将安全管理制度以纸质或电子版等方式发布到相关人员手中。

5.2.2 安全管理机构

5.2.2.1 岗位设置(G1)

应设立系统管理员、网络管理员、安全管理员等岗位,并明确各个岗位的职责。

5.2.2.2 人员配备(G1)

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(G1)

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,对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批。

5.2.2.4 沟通和合作(G1)

应加强与同业单位、公安机关、安全机关、运营商等的合作与沟通。

5.2.3 人员安全管理

5.2.3.1 人员录用(G1)

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和专业资格等进行审查,确保其具有基本的专业技术水平和安全管理知识。

5.2.3.2 人员离岗(G1)

a) 应立即终止离岗员工的所有访问权限;
b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

5.2.3.3 安全意识教育和培训(G1)

a) 应对各类人员进行安全意识教育和岗位技能培训;
b) 应告知相关人员安全责任和惩戒措施。

5.2.3.4 外部人员访问管理(G1)

外部人员在访问受控区域前应获得授权或审批。

5.2.4 系统建设管理

5.2.4.1 系统定级(G1)

a) 应明确信息系统的边界和安全保护等级;
b) 应以书面形式说明信息系统确定为某个安全保护等级的方法和理由;
c) 信息系统的定级结果应经过相关部门的批准。

5.2.4.2 安全方案设计(G1)

a) 应根据系统的安全保护等级选择基本安全措施,依据风险分析结果补充和调整安全措施;
b) 应以书面形式描述系统的安全保护要求、保护策略和安全措施等内容,形成系统的安全方案;
c) 应对安全方案进行细化,形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

5.2.4.3 产品采购和使用(G1)

信息系统安全产品的采购和使用应符合国家有关规定。

5.2.4.4 自行软件开发(G1)

a) 开发环境应与实际运行环境物理分开;
b) 软件设计相关文档应由专人负责保管。

5.2.4.5 外包软件开发(G1)

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是否存在恶意代码;
c) 应确保软件开发单位提供软件设计的相关文档和使用指南。

5.2.4.6 工程实施(G1)

应指定或授权专门的部门或人员负责工程实施过程管理。

5.2.4.7 测试验收(G1)

a) 应对系统进行安全性测试验收;
b) 在测试验收前应根据设计方案或合同要求等制订测试验收方案,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。

5.2.4.8 系统交付(G1)

a) 应制定系统交付清单,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进行相应的技能培训;

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。

5.2.4.9 安全服务商选择(G1)

a) 安全服务商的选择应符合国家有关规定;

b) 应与选定的安全服务商签订安全协议,明确约定相关责任。

5.2.5 系统运维管理

5.2.5.1 环境管理(G1)

a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施设备进行维护管理;

b) 应对设备与人员进出机房、服务器的开关等工作进行管理;

c) 应建立机房安全管理制度,对人员进出机房,物品带进、带出机房和机房环境安全等作出规定。

5.2.5.2 资产管理(G1)

应编制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。

5.2.5.3 介质管理(G1)

a) 介质应存放在安全环境中,对各类介质实行有效控制和保护;

b) 应对介质的归档和查询等过程进行记录,并根据介质存档清单定期进行盘点。

5.2.5.4 设备管理(G1)

a) 应指定专门的部门或人员定期对信息系统相关的设备、线路等进行维护管理;

b) 应建立设备安全管理制度,对信息系统中各种软硬件设备的选型、采购、发放和领用等作出规定。

5.2.5.5 网络安全管理(G1)

a) 应指定人员对网络安全进行管理,负责运行日志和网络监控记录的日常维护,以及报警信息分析处理工作;

b) 应定期进行网络系统漏洞扫描,及时对发现的安全漏洞进行修补。

5.2.5.6 系统安全管理(G1)

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,及时对发现的系统安全漏洞进行修补;

c) 应安装最新的系统补丁程序,并在安装系统补丁前对重要文件进行备份。

5.2.5.7 恶意代码防范管理(G1)

应提高所有用户的防病毒意识,告知其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。在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。

5.2.5.8 备份与恢复管理(G1)

a) 应明确需要定期备份的重要业务信息、系统数据及软件系统等;

b) 应规定数据的备份方式、备份频率、存储介质、保存期等。

5.2.5.9 安全事件处置(G1)

a) 应制定安全事件报告和处置管理制度,规定安全事件的现场处理、事件报告和后期恢复等内容;

b) 应报告所发现的安全弱点和可疑事件,且在任何情况下均不应尝试或验证安全弱点。

6 第二级基本要求

6.1 技术要求

6.1.1 物理安全

6.1.1.1 物理位置的选择(G2)

a) 机房和办公场地应选择在具备防震、防风和防雨等能力的建筑内;

b) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明。

6.1.1.2 物理访问控制(G2)

a) 机房出入口应安排专人负责管理。对没有配置电子门禁系统的机房,应有专人值守,对所有进出机房的人员进行控制、鉴别和记录,人员进出记录应至少保存 30 天;对配有电子门禁系统的机房,门禁系统的日志记录应至少保留 30 天;

b) 应采用监控设备将机房人员进出情况传输到值班点,监控记录应至少保留 30 天;

c) 来访人员应经申请和审批后方可进入机房,并限制和监控其活动范围。

6.1.1.3 防盗窃和防破坏(G2)

a) 应将主要设备放置在机房内或其他不易被盗窃和破坏的可控范围内;

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,如粘贴标签或铭牌等;

c) 应将通信线缆铺设在地下或管道中等隐蔽处,强弱电应隔离铺设并进行统一标识;

d) 应对介质进行分类标识和分类存放,存储在介质库或档案室中;

e) 主机房应安装必要的防盗报警装置,当发现异常现象时,可自动报警并保存报警记录。

6.1.1.4 防雷击(G2)

a) 机房建筑应设置避雷装置,防雷击措施至少应包括安装避雷针或避雷器;

b) 机房应设置交流电源地线。

6.1.1.5 防火(G2)

机房应配置灭火设备和火灾自动报警系统。当发现火灾隐患时,火灾自动报警系统可自动报警并保存报警记录。

6.1.1.6 防水和防潮(G2)

a) 水管的安装不宜穿过机房屋顶和活动地板下。如不可避免,应采取有效防护措施;

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,如在机房地面修建地漏、泄水槽等。

6.1.1.7 防静电(G2)

a) 关键设备应采取必要的接地防静电措施;

b) 主机房和辅助区内的工作台面应采用导静电或静电耗散材料。

6.1.1.8 温湿度控制(G2)

机房应设置温湿度自动调节设施,使机房温、湿度的变化控制在设备运行所要求的范围之内。设备开机时,机房温度应控制在 18 ~26℃,相对湿度应控制在 30% ~50%。

6.1.1.9 电力供应(A2)

a) 应在机房供电线路上配置稳压器和过电压防护设备;

b) 应具有短期的备用电力供应,至少满足关键设备在断电情况下正常运行 2h 以上。

6.1.1.10 电磁防护(S2)

电源线和通信线缆宜隔离铺设,铺设在不同的桥架或管道中,并使用交叉走线避免并排铺设;如不可避免,应采取相应的屏蔽措施。

6.1.2 网络安全

6.1.2.1 结构安全(G2)

a) 关键网络设备的业务处理能力应具备冗余空间,满足业务高峰期需要,近一年的 CPU 负载均值应小于 60%;

b) 接入网络和核心网络的带宽应满足业务高峰期需要,其占用均值均应低于 60%;

c) 应绘制与当前运行情况相符的网络拓扑结构图,拓扑结构图应包含网络设备名称、线路带宽类型、物理连线标识、设备端口名称、设备管理 IP、接口 IP 和各区域 IP 地址段等;

d) 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。

6.1.2.2 访问控制(G2)

a) 应在网络边界设置访问控制设备,启用访问控制功能;

b) 应能根据会话状态信息,允许或拒绝网络数据流的访问,控制粒度为网段级;

c) 应根据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;

d) 应限制具有拨号访问权限的用户数量。

6.1.2.3 安全审计(G2)

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、用户信息、事件类型、事件是否成功及其他与审计相关的信息。

6.1.2.4 边界完整性检查(S2)

应能够对内部网络中出现的内部用户未经准许私自联到外部网络的行为进行检查,如检查通过双网卡、电话拨号、ADSL 拨号和无线网卡等跨接外部网络的行为。

6.1.2.5 入侵防范(G2)

应在网络边界处监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等行为。

6.1.2.6 网络设备防护(G2)

a) 应对登录网络设备的用户进行身份鉴别,删除默认用户或修改默认用户的口令。根据管理需要新开设用户账号时,不应使用缺省口令、空口令和弱口令;

b) 应对网络设备的管理员登录地址进行限制;

c) 网络设备用户的标识应唯一;

d) 身份鉴别信息应具有不易被冒用的特点。口令应有复杂度要求,包含数字、大写字母、小写字母和特殊字符,且长度应不少于 8 位;口令应定期更换,至少每 90 天更换一次;

e) 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网络登录连接超时自动退出等措施;

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

6.1.3 主机安全

6.1.3.1 身份鉴别(S2)

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,不应使用默认用户和默认口令;

b) 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;

c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点。口令应有复杂度要求,包

含数字、大写字母、小写字母和特殊字符,且长度应不少于8位;口令应定期更换,至少每180天更换一次;

d) 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;

e) 当对服务器进行远程管理时,应采取SSH、HTTPS等必要措施,防止用户鉴别信息在网络传输过程中被窃听。

6.1.3.2 访问控制(S2)

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,关闭系统默认共享功能;

b) 应实现操作系统和数据库系统特权用户的权限分离;

c) 应限制默认账户的访问权限,重新命名系统默认账户,修改这些账户的默认口令,如系统中的administrator账号;

d) 应及时删除多余的、过期的账户,避免共享账户的存在,如禁止多人共用一个相同的管理账户。

6.1.3.3 安全审计(G2)

a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户;

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。如用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、用户登录与退出等操作;

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) 应保护审计记录,避免受到未预期的删除、修改或覆盖等操作,审计记录应至少保存90天。

6.1.3.4 入侵防范(G2)

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及时更新系统补丁。

6.1.3.5 恶意代码防范(G2)

a) 应安装防恶意代码软件,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,可进行统一更新、统一检测和查杀。

6.1.3.6 资源控制(A2)

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功能;

c) 应限制单个用户对系统资源的最大或最小使用限度。

6.1.3.7 业务移动终端安全(P2)

a) 应遵循最小安装的原则,仅安装需要的组件和应用程序,并通过设置服务器等方式及时更新系统补丁;

b) 应通过技术手段,限制用户对不必要功能的使用,关闭非业务所需的无线、蓝牙、GPS等;

c) 应保持安全的业务移动终端运行环境,具有安全输入、安全显示、安全存储等功能。

6.1.4 应用安全

6.1.4.1 身份鉴别(S2)

a) 应具有专用的登录控制模块对登录用户进行身份标识和鉴别;

b) 应具有用户身份标识唯一性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,身份鉴别信息不易被冒用,口令应包含数字、字母和特殊字符,且长度不少于8位,至少每180天更换一次;

c) 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自动退出等措施;

d) 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。

6.1.4.2 访问控制(S2)

a) 应具有访问控制功能,依据安全策略控制用户对文件、数据库表等客体的访问,如控制数据的增加、删除、修改或查询等操作;

b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及相互之间的操作,应在用户界面屏蔽未授权功能的导航;

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。应重新命名默认账户,如admin 等;及时删除或锁定多余无用的账户,如测试用账户等;

d) 应授予不同账户完成各自任务所需的最小权限,并在相互之间形成制约关系。

6.1.4.3 安全审计(G2)

a) 应具有覆盖每个用户的安全审计功能,应对应用系统重要安全事件进行审计,如对用户登录和退出、增加、修改、删除关键数据等操作及系统的异常事件进行日志记录;

b) 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、过程描述和结果等;

c) 应保证无法删除、修改或覆盖审计记录,审计记录应至少保存 90 天。

6.1.4.4 通信完整性(S2)

应采用校验码技术保证通信过程中数据的完整性。

6.1.4.5 通信保密性(S2)

a) 在通信双方建立连接之前,应利用密码技术进行会话初始化验证;

b) 应对通信过程中的整个报文或会话过程进行加密。

6.1.4.6 软件容错(A2)

a) 应具有数据有效性检验功能,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应符合系统设定要求。文件上传时应进行文件格式、内容检查,禁止恶意文件上传;

b) 在故障发生时,应用系统应能够继续提供部分功能,确保能够实施必要的补救措施。

6.1.4.7 资源控制(A2)

a) 当应用系统通信双方中的一方在一段时间内未作出任何响应,另一方应能够自动结束会话,如应用系统可在不超过 60min 的时间内自动终止超时会话;

b) 应能够对系统的最大并发会话连接数进行限制,如在中间件或 WEB 服务器中对最大连接数进行设置;

c) 应能够对单个账户的多重并发会话进行限制。

6.1.5 数据安全及备份恢复

6.1.5.1 数据完整性(S2)

应能够检测到用户鉴别信息和重要业务数据的完整性在传输过程中已经受到破坏,检测范围应包括网络设备操作系统、主机操作系统、数据库管理系统和应用系统的用户鉴别信息和重要业务数据等。

6.1.5.2 数据保密性(S2)

应采用加密或其他保护措施存储用户鉴别信息,保护范围应覆盖网络设备操作系统、主机操作系统、数据库管理系统和应用系统等。

6.1.5.3 备份和恢复(A2)

a) 应能够定期对重要信息进行备份和恢复,备份和恢复范围应覆盖主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置文件和其他重要信息;

b) 应对关键网络设备、通信线路和数据处理系统的硬件进行冗余配置。

6.1.5.4 数据泄露防护(P2)

a) 应明确用户敏感信息的范围,对敏感信息的使用进行授权和审批;

b) 应在关键网络边界和关键应用上对敏感数据进行有效识别,并能够持续地对敏感数据的传输及使用进行监控和保护。

6.2 管理要求

6.2.1 安全管理制度

6.2.1.1 管理制度(G2)

a) 应制定信息系统安全工作的总体方针和安全策略,规定信息系统安全工作的总体目标、范围、原则和安全框架等;

b) 应针对重要的安全管理内容建立安全管理制度,管理制度应包括物理、网络、主机、应用、数据管理等内容;

c) 应建立安全操作规程,范围应覆盖安全主管、安全管理员、网络管理员、主机管理员、安全审计员、数据库管理员、应用管理员和介质管理员等岗位。

6.2.1.2 制定和发布(G2)

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) 应组织相关人员对安全管理制度进行论证和审定,保存安全管理制度评审记录,详细记录相关人员的评审意见;

c) 应将安全管理制度以纸质或电子版等方式发布到相关人员手中。

6.2.1.3 评审和修订(G2)

应每年或当技术基础架构和组织架构等发生变更时,对安全管理制度进行评审,对存在不足或需要改进的内容进行修订。

6.2.2 安全管理机构

6.2.2.1 岗位设置(G2)

a) 应设立负责信息系统安全管理工作的职能部门;

b) 应设立系统管理员、网络管理员、安全管理员等岗位,并明确各个岗位的职责。

6.2.2.2 人员配备(G2)

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) 安全管理员不可兼任网络管理员、系统管理员、数据库管理员等。

6.2.2.3 授权和审批(G2)

a) 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,对系统投入运行、网络系统接入和重要资源的访问、系统变更等关键活动进行审批;

b) 应针对关键活动建立审批流程,并由批准人签字确认。

6.2.2.4 沟通和合作(G2)

a) 应加强管理人员之间、内部组织机构之间以及信息系统安全管理职能部门之间的合作与沟通;

b) 应加强与同业单位、公安机关、安全机关、运营商的合作与沟通,明确合作内容和合作方式。

6.2.2.5 审核和检查(G2)

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。

6.2.3 人员安全管理

6.2.3.1 人员录用(G2)

a) 应指定或授权专门的部门或人员负责人员录用;

b) 应规范人员录用过程,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,重点关注其在原工作单位是否存在信息安全违规和犯罪记录,保存审查和考核结果;

c） 应与从事关键岗位的人员签署保密协议，保密协议应明确保密范围、保密责任、违约责任和有效期限等内容。

6.2.3.2 人员离岗（G2）

a） 应规范人员离岗程序，及时终止离岗员工的所有访问权限，包括但不限于物理访问权限、网络设备访问权限、操作系统访问权限、数据库访问权限、应用系统访问权限、用户终端访问权限等；

b） 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，详细记录交还情况；

c） 应办理严格的调离手续，并保存调离手续记录。

6.2.3.3 人员考核（G2）

应至少每年一次对各个岗位的人员进行安全认知、安全技能及信息系统安全等级保护相关内容的考核。

6.2.3.4 安全意识教育和培训（G2）

a） 应制定安全意识教育和培训计划，内容包括信息系统安全基础知识、岗位操作规程等；

b） 应至少每年一次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；

c） 应告知相关人员安全责任和惩戒措施，对违反安全策略和规定的人员进行惩戒。

6.2.3.5 外部人员访问管理（G2）

外部人员在访问机房、重要服务器或设备区等受控区域前应获得授权或审批，由专人全程陪同或监督，并登记备案。

6.2.4 系统建设管理

6.2.4.1 系统定级（G2）

a） 应明确信息系统的边界和安全保护等级；

b） 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由；

c） 信息系统的定级结果应经过相关部门批准。

6.2.4.2 安全方案设计（G2）

a） 应根据系统的安全保护等级选择基本安全措施，并依据风险分析结果补充和调整安全措施；

b） 应以书面形式描述系统的安全保护要求、保护策略和安全措施等内容，形成系统的安全方案；

c） 应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案；

d） 应组织相关部门和有关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，安全设计方案经过批准后才能正式实施。

6.2.4.3 产品采购和使用（G2）

a） 信息系统安全产品的采购和使用应符合国家有关规定，如根据信息系统安全需求选择使用相应等级的产品；

b） 密码产品的采购和使用应符合国家密码主管部门的要求，如系统中使用的密码产品应具有国家密码主管部门颁发的销售许可证；

c） 应指定或授权专门的部门负责信息系统安全产品采购。

6.2.4.4 自行软件开发（G2）

a） 开发环境应与实际运行环境物理分开；

b） 应制定软件开发管理制度，明确规定开发过程的控制方法和人员行为准则，明确应经过授权、审批的开发活动；

c） 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。

6.2.4.5 外包软件开发（G2）

a） 应根据开发需求检测软件质量，检测范围应包括代码质量、软件功能和性能等；

b） 应在软件安装之前检测软件包中可能存在的恶意代码，并保存恶意代码检测报告；

c） 应确保开发单位提供软件设计的相关文档和使用指南；

d） 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木马；若开发单位未能提供软件源代码，则应要求开发单位提供第三方机构出具的软件源代码审查报告。

6.2.4.6 工程实施（G2）

a） 应指定或授权专门的部门或人员负责工程实施过程管理；

b） 应制订详细的工程实施方案，工程实施方案应明确工程时间限制、进度控制和质量控制等内容。

6.2.4.7 测试验收（G2）

a） 应对系统进行安全性测试验收，并保存测试报告；

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，测试验收方案应明确规定参与测试的部门、人员、测试验收内容、现场操作过程等内容，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） 应组织相关部门和人员对测试验收报告进行审定，并签字确认。

6.2.4.8 系统交付（G2）

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进行相应的技能培训；

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。

6.2.4.9 安全服务商选择（G2）

a） 安全服务商的选择应符合国家有关规定；

b） 应与选定的安全服务商签订安全协议，明确约定相关责任、保密范围、有效期限等内容；

c） 选定的安全服务商应提供技术培训和服务承诺，必要时与其签订服务合同，内容包括但不限于技术培训、服务承诺、服务期限等。

6.2.5 系统运维管理

6.2.5.1 环境管理（G2）

a） 应指定专门的部门或人员至少每季度对机房供配电、空调、温湿度控制等设施设备进行维护管理；

b） 应配备机房安全管理人员，对设备与人员进出机房、服务器的开关等工作进行管理；

c） 应建立机房安全管理制度，对有关人员进出机房，物品带进、带出机房和机房环境安全等作出规定；

d） 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还办公室钥匙、登记在办公区接待来访人员情况等。

6.2.5.2 资产管理（G2）

a） 应建立资产管理制度，规定信息系统资产管理的责任部门和人员，规范资产使用和管理行为，明确资产使用、传输、存储、维护以及职责划分等内容；

b） 编制并保存与信息系统相关的资产清单，包括资产的重要程度、价值和类别、责任部门和所处位置等。

6.2.5.3 介质管理（G2）

a） 介质应存放在安全环境中，专人负责保护和管理各类介质；

b） 应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，如粘贴纸质标签等；

c） 应对介质的归档和查询等过程进行记录，每季度根据介质存档清单进行检查；

d） 对需要送出维修或销毁的介质，应清除其中的敏感数据，防止非法泄露相关信息。

6.2.5.4 设备管理（G2）

a） 应指定专门的部门或人员定期对信息系统相关的各种设备、线路等进行维护管理；

b） 应建立设备安全管理制度，对信息系统中各种软硬件设备的选型、采购、发放和领用等作出

规定；

c） 应对服务器、计算机终端、业务移动终端、网络等设备的操作和使用进行规范化管理，按照安全操作规程对主要设备进行启动、停止、加电、断电等操作；

d） 信息处理设备应经过审批才能带离机房或办公地点。

6.2.5.5 网络安全管理（G2）

a） 应指定人员对网络安全进行管理，负责运行日志和网络监控记录的日常维护，以及报警信息分析处理工作；

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，并在更新前对重要文件进行备份；

d） 应定期对网络系统进行漏洞扫描，及时对发现的安全漏洞进行修补。在实施漏洞扫描或漏洞修补前，应对可能的风险进行评估，并做好充分准备，如选择恰当时间、制定数据备份和回退方案。漏洞扫描或漏洞修补后应进行验证测试，以保证网络系统的正常运行；

e） 应定期对网络设备的配置文件进行备份；

f） 所有与外部系统的连接均应获得授权和批准。

6.2.5.6 系统安全管理（G2）

a） 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作出规定；

b） 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，分配信息系统、文件及服务的访问权限；

c） 应定期进行漏洞扫描，及时对发现的系统安全漏洞进行修补。在实施漏洞扫描或漏洞修补前，应对可能的风险进行评估，并做好充分准备，如选择恰当时间、制订数据备份和回退方案。漏洞扫描或漏洞修补后应进行验证测试，以保证系统的正常运行；

d） 应安装最新的系统补丁程序。应首先在测试环境中测试通过系统补丁程序，并对重要文件进行备份后，方可安装系统补丁程序；

e） 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，严禁进行未经授权的操作；

f） 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。

6.2.5.7 恶意代码防范管理（G2）

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或邮件之前，先进行病毒检查，在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） 应制定病毒防范管理制度，对防恶意代码软件的授权使用、恶意代码库的升级等作出明确规定；

c） 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，并及时对截获的危险病毒或恶意代码进行处理。

6.2.5.8 密码管理（G2）

应使用符合国家密码管理规定的密码技术和已获得商用密码产品销售许可证的密码产品。

6.2.5.9 变更管理（G2）

a） 应确认系统的重要变更事项，并制订相应的变更方案，明确变更类型、变更原因、变更过程、变更前评估、回退方式等内容；

b） 系统变更前应获得主管领导的批准，变更实施后应向相关人员通告变更情况。

6.2.5.10 备份与恢复管理（G2）

a） 应明确需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定数据的备份方式、备份频率、存储介质和保存期等；

c） 应根据数据的重要性和数据对系统运行的影响程度,制定数据的备份策略和恢复策略。备份策略应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。

6.2.5.11 安全事件处置(G2)

a） 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、现场处理、事件报告和后期恢复等内容;

b） 应根据国家相关管理部门的计算机安全事件等级划分方法和安全事件对信息系统产生的影响,对信息系统计算机安全事件进行等级划分;

c） 应报告所发现的安全弱点和可疑事件,且在任何情况下均不应尝试或验证安全弱点;

d） 应记录并保存所有报告的安全弱点和可疑事件,分析事件原因,监视事态发展,采取措施避免安全事件发生。

6.2.5.12 应急预案管理(G2)

a） 应制订统一的应急预案框架,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） 在统一的应急预案框架下,分别制订不同事件的应急预案;

c） 应至少每年一次对系统相关人员进行应急预案培训。

7 第三级基本要求

7.1 技术要求

7.1.1 物理安全

7.1.1.1 物理位置的选择(G3)

a） 机房和办公场地应选择在具备防震、防风和防雨等能力的建筑内;

b） 应具有机房或机房所在建筑物符合当地抗震要求的相关证明;

c） 机房场地不宜设在建筑物的高层。如不可避免,应在设备运输、管线铺设等方面采取有效的补救措施;机房场地不宜设在建筑物的地下室,如不可避免,应在管道泄漏和消防排水等方面采取有效的补救措施;机房场地不宜设在用水设备的下层或隔壁,如不可避免,应采取有效措施,防止水漫溢和渗漏。

7.1.1.2 物理访问控制(G3)

a） 机房出入口应安排专人负责管理。对没有配置电子门禁系统的机房,应有专人值守,对所有进出机房的人员进行控制、鉴别和记录,人员进出记录应至少保存 90 天;对配有电子门禁系统的机房,门禁系统的日志记录应至少保留 90 天;

b） 应采用监控设备将机房人员进出情况传输到值班点,监控记录应至少保留 90 天;

c） 来访人员应经申请和审批后方可进入机房,并限制和监控其活动范围;

d） 应对机房进行区域划分管理,区域和区域之间应设置物理隔离装置。在重要区域前应设置交付或安装等过渡区域;

e） 重要区域应配置电子门禁系统,控制、鉴别和记录进入人员,电子门禁系统日志记录应至少保存 90 天。

7.1.1.3 防盗窃和防破坏(G3)

a） 应将主要设备放置在机房内或其他不易被盗窃和破坏的可控范围内;

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,如粘贴标签或铭牌等;

c） 应将通信线缆铺设在地下或管道中等隐蔽处,强弱电应隔离铺设并进行统一标识;

d） 应对介质进行分类标识和分类存放,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。当发现异常现象时，可自动报警并保存报警记录，报警记录应至少保存 90 天；

f） 应对机房设置监控报警系统。当发现异常现象时，可自动报警并保存监控记录、报警记录，监控记录应至少保存 90 天。

7.1.1.4 防雷击（G3）

a） 机房建筑应设置避雷装置，防雷击措施至少应包括安装避雷针或避雷器；

b） 机房应设置交流电源地线；

c） 应设置防雷保安器，防止感应雷。

7.1.1.5 防火（G3）

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） 自动消防系统应有运行记录并定期进行巡检；

c） 机房及相关的工作房间和辅助用房应采用不低于二级耐火等级的建筑材料；

d） 机房应采取区域隔离防火措施，如安装防火门，将重要设备与其他设备隔离开；

e） 机房内所使用的磁带和胶卷等易燃物品，应放置在防火柜内；

f） 机房应设立具有显著标识的消防逃生通道。

7.1.1.6 防水和防潮（G3）

a） 水管的安装不宜穿过机房屋顶和活动地板下。如不可避免，应采取有效防护措施；

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，如在机房地面修建地漏、泄水槽等；

d） 应安装水敏感检测仪表或元件，对机房进行防水检测，异常时报警。

7.1.1.7 防静电（G3）

a） 主要设备应采取必要的接地防静电措施；

b） 主机房和辅助区内的工作台面应采用导静电或静电耗散材料；

c） 机房应采用防静电地板。

7.1.1.8 温湿度控制（G3）

机房应设置温湿度自动调节设施，使机房温、湿度的变化控制在设备运行所要求的范围之内。设备开机时，机房温度应控制在 18 ~ 26℃，相对湿度应控制在 30% ~ 50%。

7.1.1.9 电力供应（A3）

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应具有短期的备用电力供应，如配置 UPS，至少满足主要设备在断电情况下正常运行 2h 以上；

c） 机房供电系统应采用单独的配电柜和独立于一般照明用电的专用供配电线路，配电容量应具备一定余量；

d） 应设置冗余或并行的电力电缆线路为计算机系统供电；

e） 机房供电系统应定期进行巡检，并保存巡检报告。

7.1.1.10 电磁防护（S3）

a） 电源线和通信线缆宜隔离铺设，铺设在不同的桥架或管道中，并使用交叉走线避免并排铺设。如不可避免，应采取相应的屏蔽措施；

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，如将磁介质存放在具有电磁屏蔽功能的容器中。

7.1.2 网络安全

7.1.2.1 结构安全（G3）

a） 主要网络设备的业务处理能力应具备冗余空间，满足业务高峰期需要，关键网络设备近一年的

CPU 负载均值应小于 60%；

b) 接入网络和核心网络的带宽应满足业务高峰期需要，其占用均值均应低于 60%；

c) 应绘制与当前运行情况相符的网络拓扑结构图，拓扑结构图应包含网络设备名称、线路带宽类型、物理连线标识、设备端口名称、设备管理 IP、接口 IP 和各区域 IP 地址段等；

d) 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；

e) 应在业务终端与服务器之间进行路由控制，建立安全的访问路径；

f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术手段隔离；

g) 应根据服务的重要次序指定带宽分配优先级别，网络发生拥堵时应优先保护重要主机。

7.1.2.2 访问控制(G3)

a) 应在网络边界部署访问控制设备，启用访问控制功能；

b) 应根据会话状态信息，允许/拒绝网络数据流的访问，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；

d) 应限制具有拨号访问权限的用户数量；

e) 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；

f) 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；

g) 应限制网络最大流量数及网络连接数；

h) 重要网段应采取技术手段防止地址欺骗；

i) 关键业务应用和网络访问宜使用静态路由。如使用动态路由，应启用路由协议的安全认证机制，并控制路由信息的广播范围。

7.1.2.3 安全审计(G3)

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) 日志记录应包括事件的日期和时间、用户信息、事件类型、事件是否成功及其他相关信息；

c) 应能够对记录数据进行分析，并生成审计报表；

d) 应对日志记录进行保护，避免受到未预期的删除、修改或覆盖等操作，日志记录的保存时间应不少于 180 天。

7.1.2.4 边界完整性检查(S3)

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定位，并对其进行有效阻断；

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

7.1.2.5 入侵防范(G3)

a) 应在网络边界处监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等行为；

b) 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通过声音、短信或邮件等方式进行报警。

7.1.2.6 恶意代码防范(G3)

a) 应在网络边界处对恶意代码进行检测和清除，如部署防病毒网关或 UTM、IPS 的防病毒模块等；

b) 应及时升级维护恶意代码库，并对更新情况进行检测。

7.1.2.7 网络设备防护(G3)

a) 应对登录网络设备的用户进行身份鉴别，删除默认用户或修改默认用户的口令。根据管理需要新开设用户账号时，不应使用缺省口令、空口令和弱口令；

b) 应对网络设备的管理员登录地址进行限制；
c) 网络设备用户的标识应唯一；
d) 身份鉴别信息应具有不易被冒用的特点。口令应有复杂度要求，包含数字、大写字母、小写字母和特殊字符，且长度应不少于8位；口令应定期更换，至少每90天更换一次；
e) 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网络登录连接超时自动退出等措施；
f) 当对网络设备进行远程管理时，应采取SSH、HTTPS等必要措施，防止用户鉴别信息在网络传输过程中被窃听；
g) 主要网络设备应采用两种或两种以上组合的鉴别技术，对同一用户身份进行鉴别；
h) 应实现网络设备特权用户的权限分离。

7.1.3 主机安全

7.1.3.1 身份鉴别(S3)

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，不应使用默认用户和默认口令；
b) 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；
c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点。口令应有复杂度要求，包含数字、字母和特殊字符，且长度应不少于10位；口令应定期更换，至少每90天更换一次，至少5次内不能重复；
d) 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；
e) 当对服务器进行远程管理时，应采取SSH、HTTPS等必要措施，防止用户鉴别信息在网络传输过程中被窃听；
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，如通过远程方式登录主机系统时，应采用强化管理的口令、基于生物特征、基于数字证书以及其他具有相应安全强度的两种或两种以上组合鉴别机制进行用户身份鉴别。

7.1.3.2 访问控制(S3)

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，关闭系统默认共享功能；
b) 应实现操作系统和数据库系统特权用户的权限分离；
c) 应限制默认账户的访问权限，重新命名系统默认账户，修改这些账户的默认口令，如系统中的administrator账号；
d) 应及时删除多余的、过期的账户，避免共享账户的存在，如禁止多人共用一个相同的管理账户；
e) 应根据管理用户的角色分配权限，把系统管理员、系统安全员和审计员的权限合理分配给不同特权用户，实现管理用户的权限分离，且仅授予管理用户所需的最小权限；
f) 应对重要信息资源设置敏感标记；
g) 应严格控制用户对设有敏感标记重要信息资源的操作。

7.1.3.3 安全审计(G3)

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；
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。如用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、用户登录与退出等操作；
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) 应保护审计记录，避免受到未预期的删除、修改或覆盖等操作，审计记录应至少保存180天；
e) 应能够对记录数据进行分析，并生成审计报表；
f) 应保护审计进程，避免受到未预期的中断。

7.1.3.4 剩余信息保护(S3)

a) 操作系统和数据库系统的用户鉴别信息所在的存储空间,无论是在硬盘上还是内存中,在被释放或再分配给其他用户前应完全清除。如再次登录系统时不显示前一次登录系统的用户名;

b) 系统内的文件、目录和数据库记录等资源所在的存储空间,在被释放或重新分配给其他用户前应完全清除。如在关闭系统前清除系统的虚拟内存页面。

7.1.3.5 入侵防范(G3)

a) 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及时更新系统补丁;

b) 应能够检测到入侵重要服务器的行为,记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间,并在发生严重入侵事件时使用声音、短信或 Email 等进行报警;

c) 应能够对重要程序的完整性进行检测。在检测到重要程序的完整性受到破坏时,能够采取恢复措施。

7.1.3.6 恶意代码防范(G3)

a) 应安装防恶意代码软件,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,可进行统一更新、统一检测和查杀,且至少每月分析一次日志报告;

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。

7.1.3.7 资源控制(A3)

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功能;

c) 应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,包括服务器的 CPU、硬盘、内存、网络等资源的使用情况;

e) 应在检测到系统的服务水平降低到预先规定的最小值时,采取邮件或短信等方式进行报警。

7.1.3.8 业务移动终端安全(P3)

a) 应遵循最小安装的原则,仅安装需要的组件和应用程序,并通过设置服务器等方式及时更新系统补丁;

b) 应通过技术手段限制用户对不必要功能的使用,关闭非业务所需的无线、蓝牙、GPS 等;

c) 应保持安全的业务移动终端运行环境,具有安全输入、安全显示、安全存储等功能;

d) 系统启动时应直接进入应用程序登录界面,禁止用户直接登录操作系统;

e) 应对业务移动终端上的敏感数据进行加密存储;

f) 应设置业务移动终端日志审计功能,对终端的注册、激活、解除激活等重要操作进行日志记录。

7.1.4 应用安全

7.1.4.1 身份鉴别(S3)

a) 应具有专用的登录控制模块对登录用户进行身份标识和鉴别;

b) 应具有用户身份标识唯一性和用户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,身份鉴别信息不易被冒用,口令应包含数字、字母和特殊字符,长度应不少于 8 位,且至少每 90 天更换一次;

c) 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自动退出等措施;

d) 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;

e) 应采用两种或两种以上组合的鉴别技术,对同一用户身份进行鉴别;

f) 邮政行业核心营运类系统不应通过互联网进行远程管理。

7.1.4.2 访问控制(S3)

a) 应具有访问控制功能,依据安全策略控制用户对文件、数据库表等客体的访问,如数据的增加、删除、修改或查询等操作;

b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及相互之间的操作,应在用户界面屏蔽未授权功能的导航;

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。应重新命名默认账户,如admin 等;及时删除或锁定多余无用的账户,如测试用账户等;

d) 应授予不同账户为完成各自任务所需的最小权限,并在相互之间形成制约关系;

e) 应具有对重要信息资源设置敏感标记的功能,邮政行业核心营运类系统应明确区分客户敏感信息与其他一般信息;

f) 应依据安全策略严格控制用户对重要信息资源的操作,如核心营运类系统应对客户敏感信息设置严格的访问控制策略。

7.1.4.3 安全审计(G3)

a) 应具有覆盖每个用户的安全审计功能,对应用系统重要安全事件进行审计,如对用户登录和退出、增加、修改、删除关键数据等操作及系统的异常事件进行日志记录;

b) 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、过程描述和结果等;

c) 应保证无法单独中断审计进程,无法删除、修改或覆盖审计记录,审计记录应至少保存 180 天;

d) 应具有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。

7.1.4.4 剩余信息保护(S3)

a) 用户鉴别信息所在的存储空间,无论是存放在硬盘还是内存中,在被释放或再分配给其他用户前应完全清除。如再次登录系统时不显示前一次登录系统的用户名、基于 WEB 的应用系统不在客户端上存储用户鉴别信息等;

b) 系统内的文件、目录和数据库记录等资源所在的存储空间,在被释放或重新分配给其他用户前应完全清除。如在用户退出应用系统后,立即清除使用过程中产生的临时文件等。

7.1.4.5 通信完整性(S3)

应采用密码技术保证通信过程中数据的完整性。

7.1.4.6 通信保密性(S3)

a) 在通信双方建立连接之前,应利用密码技术进行会话初始化验证;

b) 应对通信过程中的整个报文或会话过程进行加密。

7.1.4.7 抗抵赖(G3)

a) 应具有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。

7.1.4.8 软件容错(A3)

a) 应具有数据有效性检验功能,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应符合系统设定要求,文件上传时应进行文件格式、内容检查,禁止恶意文件上传;

b) 在故障发生时,应用系统应能够继续提供部分功能,确保能够实施必要的补救措施。

7.1.4.9 资源控制(A3)

a) 当应用系统通信双方中的一方在一段时间内未作出任何响应,另一方应能够自动结束会话,如应用系统可在不超过 15min 的时间内自动终止超时会话;

b) 应能够对系统的最大并发会话连接数进行限制,如在中间件或 WEB 服务器中对最大连接数进行设置;

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） 应能够在检测到系统服务水平降低到预先规定的最小值时进行报警；

g） 应具有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。

7.1.4.10 源代码安全（P3）

a） 应在系统上线前、版本变更后等关键时间节点，检测软件源代码中可能存在的程序缺陷、可能存在的安全漏洞，找出应用系统的安全隐患；

b） 应采取访问控制措施对软件源代码进行控制，防止未授权访问。

7.1.5 数据安全及备份恢复

7.1.5.1 数据完整性（S3）

a） 应能够检测到系统管理数据、用户鉴别信息和重要业务数据的完整性在传输过程中已经受到破坏，并在检测到完整性错误时采取必要的恢复措施；检测范围应包括网络设备操作系统、主机操作系统、数据库管理系统和应用系统的系统管理数据、用户鉴别信息和重要业务数据等；

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

7.1.5.2 数据保密性（S3）

a） 应采用加密或其他保护措施存储系统管理数据、用户鉴别信息和重要业务数据，保护范围应覆盖网络设备操作系统、主机操作系统、数据库管理系统和应用系统等；

b） 应采用加密或其他有效措施传输系统管理数据、用户鉴别信息和重要业务数据，保护范围应覆盖网络设备操作系统、主机操作系统、数据库管理系统和应用系统等。

7.1.5.3 备份和恢复（A3）

a） 应具有本地数据备份与恢复功能，至少每天一次进行完全数据备份，备份介质应场外存放；

b） 应具有异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地，关键数据异地备份传输延迟应控制在15min以内；

c） 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

d） 主要网络设备、通信线路和数据处理系统的硬件应冗余配置，硬件发生故障时应能够自动进行切换；

e） 应根据存储介质的使用寿命，制定存储介质数据恢复计划，避免数据丢失。

7.1.5.4 数据泄露防护（P3）

a） 应明确用户敏感信息的范围，对敏感信息的使用进行授权和审批；

b） 应在网络边界、关键应用、客户端上对敏感数据进行有效识别，并能够及时、持续地对敏感数据的传输及使用进行监控和保护；

c） 应明确不同等级信息系统间的敏感信息传递安全策略，防范敏感信息通过低级别信息系统进行非授权传递。

7.2 管理要求

7.2.1 安全管理制度

7.2.1.1 管理制度（G3）

a） 应制定信息系统安全工作的总体方针和安全策略，规定信息系统安全工作的总体目标、范围、原则和安全框架等；

b） 应针对各类安全管理内容建立安全管理制度，管理制度应包括但不限于物理、网络、主机、应用、

数据、人员、建设和运维等内容；

c） 应建立安全操作规程，范围应覆盖安全主管、安全管理员、网络管理员、主机管理员、安全审计员、数据库管理员、应用管理员和介质管理员等岗位；

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系统安全管理制度体系。

7.2.1.2 制定和发布（G3）

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） 应组织相关人员对制定的安全管理制度进行论证和审定，保存安全管理制度评审记录，详细记录相关人员的评审意见；

c） 应对安全管理制度设定统一格式并进行版本控制；

d） 应注明安全管理制度的发布范围，并记录和保存发布记录；

e） 安全管理制度应通过正式、有效的方式进行发布。

7.2.1.3 评审和修订（G3）

信息系统安全工作领导小组应至少每年，或当技术基础架构和组织架构等发生变更时，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，保存评审记录，并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

7.2.2.1 岗位设置（G3）

a） 应设立负责信息系统安全管理工作的职能部门，以及安全主管、安全管理员等岗位，并明确各个岗位的职责；

b） 应设立系统管理员、网络管理员、数据库管理员等岗位，并明确各个工作岗位的职责；

c） 应成立信息系统安全工作领导小组，负责协调本单位及所辖范围的信息系统安全管理工作，决策本单位及所辖范围的信息系统安全重大事宜。领导小组最高领导应由单位主管领导委任或授权；

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。

7.2.2.2 人员配备（G3）

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） 安全管理员应为专职人员，不可兼任其他岗位；

c） 系统管理、网络管理、数据库管理等关键岗位应至少配备 2 人，实行共同管理。

7.2.2.3 授权和审批（G3）

a） 应根据各个部门和岗位的职责明确授权审批事项、审批部门及批准人。审批事项包括但不限于系统投入运行、网络系统接入和重要资源的访问等重要活动；

b） 应对重要活动建立逐级审批制度，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；

c） 应至少每年一次审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，并保存审查记录；

d） 应记录审批过程并保存审批文档。

7.2.2.4 沟通和合作（G3）

a） 应加强管理人员之间、内部组织机构之间以及信息系统安全管理职能部门之间的合作与沟通，定期或不定期召开协调会议，共同协作处理信息系统安全问题；

b） 应加强与同业单位、公安机关、安全机关、运营商的合作与沟通，以文档形式明确合作内容和合作方式；

c） 应加强与供应商、业界专家、专业安全公司、安全组织的合作与沟通，以文档形式明确合作内容

和合作方式；

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，外联单位应包括公安机关、运营商、供电部门、专业安全公司、安全组织等；

e) 应聘请信息安全专家作为常年安全顾问，指导信息系统安全建设，参与安全规划和安全评审等工作。

7.2.2.5 审核和检查(G3)

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，并保存安全检查记录；

c) 应制定安全检查表格，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，规范安全审核和安全检查工作，定期进行安全审核和安全检查活动。

7.2.3 人员安全管理

7.2.3.1 人员录用(G3)

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，重点关注其在原工作单位是否存在信息安全违规和犯罪记录，保存审查和考核结果；

c) 应签署保密协议，保密协议应明确保密范围、保密责任、违约责任和有效期限等内容；

d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。关键岗位包括但不限于数据库管理员、网络管理员、系统管理员、安全管理员等，安全协议包括但不限于安全责任、违约责任和有效期限等内容。

7.2.3.2 人员离岗(G3)

a) 应严格规范人员离岗程序，及时终止离岗员工的所有访问权限，包括但不限于物理访问权限、网络设备访问权限、操作系统访问权限、数据库访问权限、应用系统访问权限、用户终端访问权限等；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，详细记录交还情况；

c) 应办理严格的调离手续并保存调离手续记录，关键岗位人员须在承诺调离后的保密义务后方可离开。

7.2.3.3 人员考核(G3)

a) 应至少每年一次对各个岗位的人员进行安全认知、安全技能及信息系统安全等级保护相关内容的考核；

b) 应至少每年一次对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，详细记录考核时间、考核内容和考核结果等内容。

7.2.3.4 安全意识教育和培训(G3)

a) 应对定期开展安全教育和培训进行书面规定，针对不同岗位制定不同的年度培训计划；

b) 应至少每年一次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；

c) 应对安全教育和培训的情况和结果进行记录并归档保存；

d) 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反安全策略和规定的人员进行惩戒；

e) 应每年对专业人员进行信息系统安全技术提升培训，并对培训情况进行记录归档保存；信息系

统安全专业人员晋升时,应进行安全专业技能考核。

7.2.3.5 外部人员访问管理(G3)

a) 对外部人员允许访问的区域、系统、设备、信息等,应进行书面规定并按照规定执行;

b) 外部人员在访问机房、重要服务器或设备区等受控区域前,应先提出书面申请,批准后由专人全程陪同或监督,并登记备案,详细记录外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息;

c) 应禁止外部来访人员的移动设备如 U 盘、移动硬盘、手机等直接接入到系统。

7.2.4 系统建设管理

7.2.4.1 系统定级(G3)

a) 应明确信息系统的边界和安全保护等级;

b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由;

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

d) 信息系统的定级结果应经过相关部门批准。

7.2.4.2 安全方案设计(G3)

a) 应根据系统的安全保护等级选择基本安全措施,并依据风险分析结果补充和调整安全措施;

b) 应根据信息系统的等级划分情况,统一确定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;

c) 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,制定近期和远期安全建设工作计划,计划内容包括但不限于工作目标、建设内容和责任部门等;

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、详细设计方案等文件的合理性和正确性进行论证和审定,并经过批准后才能正式实施;

e) 应根据等级测评、安全评估结果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、详细设计方案等文件。

7.2.4.3 产品采购和使用(G3)

a) 信息系统安全产品的采购和使用应符合国家有关规定,如根据信息系统安全需求选择使用相应等级的产品;

b) 密码产品的采购和使用应符合国家密码主管部门的要求,如系统中使用的密码产品应具有国家密码主管部门颁发的销售许可证;

c) 应指定或授权专门的部门负责信息系统安全产品采购;

d) 应预先对信息系统安全产品进行选型测试,确定产品的候选范围,并定期审定和更新候选产品名单。

7.2.4.4 自行软件开发(G3)

a) 开发环境应与实际运行环境物理分开,开发人员应与测试人员分离;

b) 应制定软件开发管理制度,明确规定开发过程的控制方法和人员行为准则,明确应经过授权、审批的开发活动;

c) 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;

d) 应在软件开发的需求、设计、编码和测试等各个环节,引入安全的开发方法以提高软件安全性,减少软件的安全缺陷和漏洞;

e) 应制定代码编写安全规范,要求开发人员按照规范编写代码;

f) 应对程序资源库的修改、更新、发布进行授权和批准。

7.2.4.5 外包软件开发(G3)

a) 应根据开发需求检测软件质量,检测范围应包括代码质量、软件功能和性能等;

b） 应在软件安装之前检测软件包中可能存在的恶意代码,并保存恶意代码检测报告;
c） 应确保软件开发单位提供软件设计的相关文档和使用指南;
d） 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木马;若开发单位未能提供软件源代码,则应要求开发单位提供第三方机构出具的软件源代码审查报告。

7.2.4.6 工程实施(G3)

a） 应指定或授权专门的部门或人员负责工程实施过程管理;
b） 应制订详细的工程实施方案,工程实施方案应明确工程时间限制、进度控制和质量控制等内容,并要求工程实施单位严格执行工程实施方案;
c） 应制定工程实施管理制度,明确规定实施过程的控制方法和人员行为准则。

7.2.4.7 测试验收(G3)

a） 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,测试验收方案应明确规定参与测试的部门、人员、测试验收内容、现场操作过程等内容,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;
b） 应委托第三方测试机构对系统进行安全性测试,并出具安全性测试报告。报告应具有第三方测试机构的签字和盖章,报告内容应包括但不限于测试时间、测试地点、测试人员、测试对象、测试方法、测试过程、测试中发现的安全问题、整改建议和测试结论;
c） 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;
d） 应对系统测试验收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测试验收的管理,并按照管理规定完成系统测试验收工作。

7.2.4.8 系统交付(G3)

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进行相应的技能培训;
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管理,并按照管理规定完成系统交付工作。

7.2.4.9 系统备案(G3)

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;
b） 应将系统等级结果及相关材料报邮政管理部门备案,并保存相关备案记录;
c） 应将系统等级结果及相关材料报公安机关备案,并保存相关备案记录。

7.2.4.10 等级测评(G3)

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应及时整改;
b） 应在系统发生变更时及时对系统进行等级测评,级别发生变化的应及时进行安全改造,不符合相应等级保护标准要求的应及时整改;
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;
d） 应指定或授权专门的部门或人员负责等级测评管理。

7.2.4.11 安全服务商选择(G3)

a） 安全服务商的选择应符合国家有关规定;
b） 应与选定的安全服务商签订安全协议,明确约定相关责任、保密范围、有效期限等内容;
c） 选定的安全服务商应提供技术培训和服务承诺,必要的与其签订服务合同,内容包括但不限于技术培训、服务承诺、服务期限等;
d） 在与安全服务商签订有效的服务合同之前,应评估安全服务商的引入风险,确保风险在可接受范围内。

7.2.5 系统运维管理

7.2.5.1 环境管理(G3)

a) 应指定专门的部门或人员至少每季度对机房供配电、空调、温湿度控制等设施设备进行维护管理;
b) 应指定专门的部门负责机房安全,配备机房安全管理人员,对设备与人员进出机房、服务器的开关等工作进行管理;
c) 应建立机房安全管理制度,对有关人员进出机房,物品带进、带出机房和机房环境安全等作出规定;
d) 应加强对办公环境的保密性管理,包括工作人员调离办公室应立即交还办公室钥匙、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不放含有敏感信息的纸质文件等。

7.2.5.2 资产管理(G3)

a) 应建立资产管理制度,规定信息系统资产管理的责任部门或人员,规范资产使用和管理行为,明确资产使用、传输、存储、维护以及职责划分等内容;
b) 应编制并保存与信息系统相关的资产清单,包括资产的重要程度、价值和类别、责任部门和所处位置等;
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。

7.2.5.3 介质管理(G3)

a) 应建立介质安全管理制度,对介质的存放环境、使用、维护和销毁等作出规定;
b) 介质应存放在安全环境中,专人负责保护和管理各类介质;
c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行管控,对介质归档和查询等过程进行记录,每季度应根据清单对介质的现状进行检查;
d) 应对存储介质的使用、送出维修及销毁等进行严格管理。对带出工作环境的存储介质应对内容进行加密并进行监控,对需要送出维修或销毁的介质应首先清除介质中的敏感数据,保密性要求较高的存储介质未经批准不应自行销毁;
e) 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;
f) 应对重要介质中的数据和软件采取加密存储,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,如粘贴纸质标签等。

7.2.5.4 设备管理(G3)

a) 应指定专门的部门或人员定期对信息系统相关的各种设备、线路等进行维护管理;
b) 应建立设备安全管理制度,对信息系统各种软硬件设备的选型、采购、发放和领用等作出规定;
c) 应对服务器、计算机终端、业务移动终端、网络等设备的操作和使用进行规范化管理,按照操作规程实现设备的启动、停止、加电、断电等操作;
d) 信息处理设备应经过审批后才能带离机房或办公地点;
e) 应建立机房配套设备的维护管理制度,明确维护人员的责任、涉外维修和服务的审批、维修过程的监督等,并保存设备的涉外维修和服务过程的申请和审批记录。

7.2.5.5 监控管理和安全管理中心(G3)

a) 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;
b) 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,异常时报警,形成记录并妥善保存;

c) 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;

d) 应部署运维审计设备,实现集中账户管理、集中认证、集中授权、集中访问控制、集中安全审计功能。

7.2.5.6 网络安全管理(G3)

a) 应指定人员对网络安全进行管理,负责运行日志和网络监控记录的日常维护,以及报警信息分析处理工作;

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,并在更新前对重要文件进行备份;

d) 应定期对网络系统进行漏洞扫描,及时对发现的安全漏洞进行修补。在实施漏洞扫描或漏洞修补前,应对可能的风险进行评估,做好充分准备,如选择恰当时间、制定数据备份和回退方案。在漏洞扫描或漏洞修补后应进行验证测试,以保证网络系统正常运行;

e) 应实现网络设备的最小服务配置,并对配置文件进行定期离线备份;

f) 所有与外部系统的连接均应得到授权和批准;

g) 应依据安全策略允许或者拒绝便携式和移动式设备接入网络;

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,并保存检查记录。

7.2.5.7 系统安全管理(G3)

a) 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作出规定;

b) 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,分配信息系统、文件及服务的访问权限;

c) 应定期进行漏洞扫描,及时对发现的安全漏洞进行修补。在实施漏洞扫描或漏洞修补前,应对可能的风险进行评估,做好充分准备,如选择恰当时间、制订好数据备份和回退方案。在漏洞扫描或漏洞修补后应进行验证测试,以保证系统的正常运行;

d) 应安装最新的系统补丁程序。应首先在测试环境中测试通过系统补丁程序,并对重要文件进行备份后,方可实施系统补丁程序的安装;

e) 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、参数的设置和修改等内容,严禁进行未经授权的操作;

f) 应定期对运行日志和审计数据进行分析,及时发现异常行为;

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

7.2.5.8 恶意代码防范管理(G3)

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或邮件之前,先进行病毒检查,在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) 应制定病毒防范管理制度,对防恶意代码软件的授权使用、恶意代码库升级等作出明确规定;

c) 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,及时对截获的危险病毒或恶意代码进行处理;

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,及时对主机防病毒产品、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分析处理,并进行书面报告。

7.2.5.9 密码管理(G3)

应建立密码使用管理制度,明确密码产品和技术选型、采购、授权使用、日常维护、废弃等全生命

周期管理内容;应采用符合国家密码管理规定的密码技术和已获得商用密码产品销售许可证的密码产品。

7.2.5.10 变更管理(G3)

a) 应明确系统的重要变更事项并制订相应的变更方案,明确变更类型、变更原因、变更过程、变更前评估、回退方式等内容;

b) 应建立变更管理制度。在变更系统前向主管领导申请,变更和变更方案经过评审、审批后方可实施,并在实施后向相关人员通告变更情况;

c) 应对变更影响进行分析,记录变更实施过程,并妥善保存所有文档和记录;

d) 应建立变更中止与变更失败恢复程序,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。

7.2.5.11 备份与恢复管理(G3)

a) 应明确需要定期备份的重要业务信息、系统数据及软件系统等;

b) 应建立备份与恢复安全管理制度,对备份信息的备份方式、备份频率、存储介质和保存期等作出规定;

c) 应根据数据的重要性和数据对系统运行的影响程度,制定数据的备份策略和恢复策略。备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输的方法;

d) 应建立数据备份和恢复过程控制程序,记录备份过程,所有文件和记录应妥善保存;

e) 应至少每年一次执行恢复程序,检查和测试备份介质的有效性,确保在规定的时间内完成备份恢复。

7.2.5.12 安全事件处置(G3)

a) 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、现场处理、事件报告和后期恢复等内容;

b) 应根据国家相关管理部门的计算机安全事件等级划分方法和安全事件对系统产生的影响,对信息系统计算机安全事件进行等级划分,建立安全事件定级文档,明确安全事件的定义、等级划分原则、等级描述等内容;

c) 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;

d) 应报告所发现的安全弱点和可疑事件,在任何情况下均不应尝试验证安全弱点;

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,明确具体的报告方式、报告内容、报告人员和处理程序等内容。

7.2.5.13 应急预案管理(G3)

a) 应制订统一的应急预案框架,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) 在统一的应急预案框架下,分别制订不同事件的应急预案;

c) 应至少每年一次对系统相关人员进行应急预案培训;

d) 应制定应急保障制度,从人力、技术、设备和财务等方面确保应急预案的执行;

e) 应定期对应急预案进行演练,并保存演练记录,记录应包括应急演练过程、审批过程、相关人员及签字、演练内容及结果等;应根据不同的应急恢复内容,确定演练周期,至少每年演练一次。在演练后对应急预案进行审查,保存审查记录;

f) 应规定应急预案中需要定期审查和更新的内容,并按照执行。

8 第四级基本要求

8.1 技术要求

8.1.1 物理安全

8.1.1.1 物理位置的选择(G4)

a) 机房和办公场地应选择在具备防震、防风和防雨等能力的建筑内;
b) 应具有机房或机房所在建筑物符合当地抗震要求的相关证明;
c) 机房场地不宜设在建筑物的高层。如不可避免,应在设备运输、管线铺设等方面采取有效的补救措施;机房场地不宜设在建筑物的地下室,如不可避免,应在管道泄漏和消防排水等方面采取有效的补救措施;机房场地不宜设在用水设备的下层或隔壁,如不可避免,应采取有效措施,防止水漫溢和渗漏;
d) 机房场地应避开火灾危险程度高的区域,周围50m内不应有加油站、煤气站等建筑。

8.1.1.2 物理访问控制(G4)

a) 机房出入口应安排专人值守并配置电子门禁系统,电子门禁系统的日志记录应至少保留1年;
b) 应采用监控设备将机房人员进出情况传输到值班点,监控记录应至少保留1年;
c) 来访人员应经申请和审批后方可进入机房,并限制和监控其活动范围;
d) 应对机房进行区域划分管理,区域和区域之间应设置物理隔离装置。在重要区域前应设置交付或安装等过渡区域;
e) 重要区域应设置第二道电子门禁系统,控制、鉴别和记录进入人员,电子门禁系统日志记录应至少保存1年。

8.1.1.3 防盗窃和防破坏(G4)

a) 应将主要设备放置在机房内或其他不易被盗窃和破坏的可控范围内;
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,如粘贴标签或铭牌等;
c) 应将通信线缆铺设在地下或管道中等隐蔽处,强弱电应隔离铺设并进行统一标识;
d) 应对介质分类标识和分类存放,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。当发现异常现象时,可自动报警并保存报警记录,报警记录应至少保存1年;
f) 应对机房设置监控报警系统。当发现异常现象时,可自动报警,并保存监控记录和报警记录,监控记录应至少保存1年。

8.1.1.4 防雷击(G4)

a) 机房建筑应设置避雷装置,防雷击措施至少应包括安装避雷针或避雷器;
b) 机房应设置交流电源地线;
c) 应设置防雷保安器,防止感应雷。

8.1.1.5 防火(G4)

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) 自动消防系统应有运行记录并定期进行巡检;
c) 机房及相关的工作房间和辅助房应采用不低于三级耐火等级的建筑材料;
d) 机房应采取区域隔离防火措施,如安装防火门,将重要设备与其他设备隔离开;
e) 机房内所使用的磁带和胶卷等易燃物品,应放置在防火柜内;
f) 机房应设置具有显著标识的消防逃生通道。

8.1.1.6 防水和防潮(G4)

a) 水管的安装不宜穿过机房屋顶和活动地板下。如不可避免,应采取有效防护措施;
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,如在机房地面修建地漏、泄水槽等;
d) 应安装水敏感检测仪表或元件,对机房进行防水检测,发现异常时报警。

8.1.1.7 防静电(G4)

a) 主要设备应采用必要的接地防静电措施;
b) 主机房和辅助区内的工作台面应采用导静电或静电耗散材料;
c) 机房应采用防静电地板;
d) 机房应采用静电消除器等装置,减少静电的产生。

8.1.1.8 温湿度控制(G4)

机房应设置温湿度自动调节设施,使机房温、湿度的变化控制在设备运行所要求的范围之内。设备开机时,机房温度应控制在 18 ~26℃,相对湿度应控制在 30% ~50%。

8.1.1.9 电力供应(A4)

a) 应在机房供电线路上配置稳压器和过电压防护设备;
b) 应具有短期的备用电力供应,如配置 UPS,至少满足主要设备在断电情况下正常运行 2h 以上;
c) 机房供电系统应采用单独的配电柜和独立于一般照明用电的专用供配电线路,配电容量应具备一定余量;
d) 应设置冗余或并行的电力电缆线路为计算机系统供电;
e) 机房供电系统应定期进行巡检,并保存巡检报告。

8.1.1.10 电磁防护(S4)

a) 电源线和通信线缆应隔离铺设,铺设在不同的桥架或管道中,并使用交叉走线避免并排铺设。如不可避免,应采取相应的屏蔽措施;
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) 应对关键区域实施电磁屏蔽。

8.1.2 网络安全

8.1.2.1 结构安全(G4)

a) 主要网络设备的业务处理能力应具备冗余空间,满足业务高峰期需要,关键网络设备近一年的 CPU 负载均值应小于 60%;
b) 接入网络和核心网络的带宽应满足业务高峰期需要,其占用均值均应低于 60%;
c) 应绘制与当前运行情况相符的网络拓扑结构图,拓扑结构图应包含网络设备名称、线路带宽类型、物理连线标识、设备端口名称、设备管理 IP、接口 IP 和各区域 IP 地址段等;
d) 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;
e) 应在业务终端与服务器之间进行路由控制,建立安全的访问路径;
f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统,重要网段与其他网段之间采取可靠的技术手段隔离;
g) 应根据服务的重要次序指定带宽分配优先级别,网络发生拥堵时应优先保护重要主机。

8.1.2.2 访问控制(G4)

a) 应在网络边界部署访问控制设备,启用访问控制功能;
b) 应拒绝带通用协议的数据通过;
c) 应根据数据的敏感标记允许或拒绝数据通过;

d) 应关闭远程拨号访问功能；

e) 关键业务应用和网络访问宜使用静态路由。如果使用动态路由，应启用路由协议的安全认证机制，并控制路由信息的广播范围。

8.1.2.3 安全审计(G4)

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) 日志记录应包括事件的日期和时间、用户信息、事件类型、事件是否成功及其他相关信息；

c) 应能够根据记录数据进行分析，并生成审计报表；

d) 应对日志记录进行保护，避免受到未预期的删除、修改或覆盖等操作，日志记录的保存时间应不少于1年；

e) 应设定审计跟踪极限的阈值，当存储空间接近极限时采取必要措施进行调整，当存储空间被耗尽时终止可审计事件的发生；

f) 应根据信息系统的统一安全策略，实现集中审计，产生日志的机器时钟应与网络服务器的时钟保持同步。

8.1.2.4 边界完整性检查(S4)

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定位，并对其进行有效阻断；

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

8.1.2.5 入侵防范(G4)

a) 应在网络边界处监视端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等行为；

b) 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通过声音、短信或邮件等方式进行报警。

8.1.2.6 恶意代码防范(G4)

a) 应在网络边界处对恶意代码进行检测和清除，如部署防病毒网关或UTM、IPS的防病毒模块等；

b) 应及时升级维护恶意代码库，并对更新情况进行检测。

8.1.2.7 网络设备防护(G4)

a) 应对登录网络设备的用户进行身份鉴别，删除默认用户或修改默认用户的口令。根据管理需要新开设用户账号时，不应使用缺省口令、空口令和弱口令；

b) 应对网络设备的管理员登录地址进行限制；

c) 网络设备用户的标识应唯一；

d) 身份鉴别信息应具有不易被冒用的特点。口令应有复杂度要求，包含数字、大写字母、小写字母和特殊字符，且长度应不少于8位；口令应定期更换，至少每30天更换一次；

e) 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网络登录连接超时自动退出等措施；

f) 当对网络设备进行远程管理时，应采取SSH、HTTPS等必要措施，防止用户鉴别信息在网络传输过程中被窃听；

g) 主要网络设备应采用两种或两种以上组合的鉴别技术，对同一用户身份进行鉴别；

h) 应实现网络设备特权用户的权限分离；

i) 网络设备用户的身份鉴别信息应至少有一种是不可伪造的。

8.1.3 主机安全

8.1.3.1 身份鉴别(S4)

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，不应使用默认用户和默认口令；

b) 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；

c) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点。口令应有复杂度要求,包含数字、字母和特殊字符,且长度应不少于10位;口令应定期更换,至少每30天更换一次,至少5次内不能重复;

d) 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;

e) 当对服务器进行远程管理时,应采取SSH、HTTPS等必要措施,防止用户鉴别信息在网络传输过程中被窃听;

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,且身份鉴别信息应至少有一种是不可伪造的。如通过远程方式登录主机系统时,应采用强化管理的口令、基于生物特征、基于数字证书及其他具有相应安全强度的两种或两种以上组合鉴别机制进行鉴别;

g) 应设置鉴别警示信息,提醒未授权访问可能导致的后果。

8.1.3.2 安全标记(S4)

应对所有主体和客体设置敏感标记。

8.1.3.3 访问控制(S4)

a) 应依据安全策略和所有主体、客体设置的敏感标记控制主体对客体的访问;

b) 主体访问控制的粒度应达到用户级或进程级,客体应达到文件、数据库表、记录和字段级;

c) 应实现操作系统和数据库系统特权用户的权限分离;

d) 应严格限制默认账户的访问权限,重新命名系统默认账户,修改这些账户的默认口令,如系统中的administrator账号;

e) 应及时删除多余的、过期的账户,避免共享账户的存在,如禁止多人共用一个相同的管理账户;

f) 应根据管理用户的角色分配权限,把系统管理员、系统安全员和审计员的权限合理分配给不同特权用户,实现管理用户的权限分离,且仅授予管理用户所需的最小权限。

8.1.3.4 可信路径(S4)

a) 在系统对用户进行身份鉴别时,系统与用户之间应能够建立一条安全的信息传输路径;

b) 在用户对系统进行访问时,系统与用户之间应能够建立一条安全的信息传输路径。

8.1.3.5 安全审计(G4)

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;

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。如用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、用户登录与退出等操作;

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) 应保护审计记录,避免受到未预期的删除、修改或覆盖等操作,审计记录应至少保存1年;

e) 应能够对记录数据进行分析,并生成审计报表;

f) 应保护审计进程,避免受到未预期的中断;

g) 应能够根据信息系统的统一安全策略,实现集中审计。

8.1.3.6 剩余信息保护(S4)

a) 操作系统和数据库系统的用户鉴别信息所在的存储空间,无论是在硬盘上还是内存中,在被释放或再分配给其他用户前应完全清除。如再次登录系统时不显示前一次登录系统的用户名;

b) 系统内的文件、目录和数据库记录等资源所在的存储空间,在被释放或重新分配给其他用户前应完全清除。如在关闭系统前清除系统的虚拟内存页面。

8.1.3.7 入侵防范(G4)

a) 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及时更新系统补丁;

b) 应能够检测到入侵重要服务器的行为,记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间,并在发生严重入侵事件时使用声音、短信或Email等进行报警;

c） 应能够对重要程序的完整性进行检测。在检测到重要程序的完整性受到破坏时，能够采取恢复措施。

8.1.3.8 恶意代码防范（G4）

a） 应安装防恶意代码软件，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，可进行统一更新、统一检测和查杀，且至少每月分析一次日志报告；

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。

8.1.3.9 资源控制（A4）

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功能；

c） 应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，包括服务器的 CPU、硬盘、内存、网络等资源的使用情况；

e） 应在检测到系统的服务水平降低到预先规定的最小值时，采取邮件或短信等方式进行报警。

8.1.3.10 业务移动终端安全（P4）

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置服务器等方式及时更新系统补丁；

b） 应通过技术手段限制用户对不必要功能的使用，关闭非业务所需的无线、蓝牙、GPS 等；

c） 应保持安全的业务移动终端运行环境，具有安全输入、安全显示、安全存储等功能；

d） 系统启动时应直接进入应用程序登录界面，禁止用户直接登录操作系统；

e） 应对业务移动终端上的敏感数据进行加密存储；

f） 应设置业务移动终端日志审计功能，对终端的注册、激活、解除激活等重要操作进行日志记录；

g） 应对业务移动终端进行身份认证，保证终端的合法性；

h） 应采取技术措施对已确认丢失终端的数据进行擦除。

8.1.4 应用安全

8.1.4.1 身份鉴别（S4）

a） 应具有专用的登录控制模块对登录用户进行身份标识和鉴别；

b） 应具有用户身份标识唯一性和用户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，身份鉴别信息不易被冒用，口令应包含数字、字母和特殊字符，长度应不少于 10 位，且至少每 30 天更换一次；

c） 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自动退出等措施；

d） 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；

e） 应采用两种或两种以上组合的鉴别技术，对同一用户身份进行鉴别，且其中一种是不可伪造的；

f） 邮政行业核心营运类系统不应通过互联网进行远程管理。

8.1.4.2 安全标记（S4）

应具有为主体和客体设置安全标记的功能，并在安装后启用；应用系统的设计或验收文档应对其进行描述说明。

8.1.4.3 访问控制（S4）

a） 应具有自主访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问，如数据的增加、删除、修改或查询等操作；

b） 访问控制的覆盖范围应包括与资源访问相关的主体、客体及相互之间的操作，应在用户界面屏蔽未授权的功能导航；

c) 应由授权主体配置访问控制策略,并禁止默认账户的访问;
d) 应授予不同账户为完成各自任务所需的最小权限,并在相互之间形成制约关系;
e) 应具有对重要信息资源设置敏感标记的功能,邮政行业核心营运类系统应明确区分客户敏感信息与其他一般信息;
f) 应通过对主体和客体安全标记的比较,确定授予或拒绝主体对客体的访问。

8.1.4.4 可信路径(S4)

a) 在应用系统对用户进行身份鉴别时,应能够建立一条安全的信息传输路径,并在应用系统的设计或验收文档中对其进行说明;
b) 在用户通过应用系统对资源进行访问时,应用系统应在被访问资源与用户之间建立一条安全的信息传输路径,并在应用系统的设计或验收文档中对其进行说明。

8.1.4.5 安全审计(G4)

a) 应具有覆盖到每个用户的安全审计功能,对应用系统重要安全事件进行审计,如对用户登录与退出、增加、修改、删除关键数据等操作及系统的异常事件提供日志记录;
b) 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、过程描述和结果等;
c) 应保证无法单独中断审计进程,无法删除、修改或覆盖审计记录,并采用日志服务器备份日志文件,审计记录应至少保存 1 年;
d) 应具有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;
e) 应根据统一的安全策略,提供集中审计接口。

8.1.4.6 剩余信息保护(S4)

a) 用户鉴别信息所在的存储空间,无论是存放在硬盘还是内存中,在被释放或再分配给其他用户前应完全清除。如再次登录系统时不显示前一次登录系统的用户名、基于 WEB 的应用系统不在客户端上存储用户鉴别信息等;
b) 系统内的文件、目录和数据库记录等资源所在的存储空间,在被释放或重新分配给其他用户前应完全清除。如在用户退出应用系统后,立即清除使用过程中产生的临时文件等。

8.1.4.7 通信完整性(S4)

应采用密码技术保证通信过程中数据的完整性。

8.1.4.8 通信保密性(S4)

a) 在通信双方建立连接之前,应利用密码技术进行会话初始化验证;
b) 应对通信过程中的整个报文或会话过程进行加密;
c) 应采用硬件设备对重要通信过程进行加解密运算和密钥管理。

8.1.4.9 抗抵赖(G4)

a) 应具有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。

8.1.4.10 软件容错(A4)

a) 应具有数据有效性检验功能,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应符合系统设定要求,文件上传时应进行文件格式、内容检查,禁止恶意文件上传;
b) 应具有自动保护功能,当故障发生时自动保护当前所有状态;
c) 应具有自动恢复功能,当故障发生时立即自动启动新的进程,恢复原来的工作状态。

8.1.4.11 资源控制(A4)

a) 当应用系统通信双方中的一方在一段时间内未作出任何响应,另一方应能够自动结束会话,如应用系统可在不超过 15min 的时间内自动终止超时会话;
b) 应能够对系统的最大并发会话连接数进行限制,如在中间件或 WEB 服务器中对最大连接数进行设置;

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) 应能够在检测到系统服务水平降低到预先规定的最小值时进行报警；
g) 应具有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。

8.1.4.12 源代码安全(P4)

a) 应在系统上线前、版本变更后等关键时间节点，检测软件源代码中可能存在的程序缺陷、可能存在的安全漏洞，找出应用系统的安全隐患；
b) 应采取访问控制措施对软件源代码进行控制，防止未授权访问。

8.1.5 数据安全及备份恢复

8.1.5.1 数据完整性(S4)

a) 应能够检测到系统管理数据、用户鉴别信息和重要业务数据的完整性在传输过程中已经受到破坏，并在检测到完整性错误时采取必要的恢复措施；检测范围应包括网络设备操作系统、主机操作系统、数据库管理系统和应用系统的系统管理数据、用户鉴别信息和重要业务数据等；
b) 应能够检测到系统管理数据、用户鉴别信息和重要业务数据的完整性在存储过程中已经受到破坏，并在检测到完整性错误时采取必要的恢复措施；
c) 应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据的完整性。

8.1.5.2 数据保密性(S4)

a) 应采用加密或其他保护措施存储系统管理数据、用户鉴别信息和重要业务数据，保护范围应覆盖网络设备操作系统、主机操作系统、数据库管理系统和应用系统等；
b) 应采用加密或其他保护措施传输系统管理数据、用户鉴别信息和重要业务数据，保护范围应覆盖网络设备操作系统、主机操作系统、数据库管理系统和应用系统等；
c) 应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据的保密性。

8.1.5.3 备份和恢复(A4)

a) 应具有本地数据备份与恢复功能，至少每天一次进行完全数据备份，备份介质应场外存放；
b) 应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用系统的实时无缝切换；
c) 应具有异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心；
d) 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；
e) 主要网络设备、通信线路和数据处理系统的硬件应冗余配置，硬件发生故障时应能够自动进行切换；
f) 应根据存储介质的使用寿命，制定数据恢复计划，避免数据丢失。

8.1.5.4 数据泄露防护(P4)

a) 应明确用户敏感信息的范围，对敏感信息的使用进行授权和审批；
b) 应在网络边界、关键应用、客户端上对敏感数据进行有效识别，并能够及时、持续地对敏感数据的传输及使用进行监控和保护；
c) 应明确不同等级信息系统间的敏感信息传递安全策略，防范敏感信息通过低级别信息系统进行非授权传递。

8.2 管理要求

8.2.1 安全管理制度

8.2.1.1 管理制度(G4)

a) 应制定信息系统安全工作的总体方针和安全策略,规定信息系统安全工作的总体目标、范围、原则和安全框架等;
b) 应针对各类安全管理内容建立安全管理制度,管理制度应包括但不限于物理、网络、主机、应用、数据、人员、建设和运维等内容;
c) 应建立安全操作规程,范围应覆盖安全主管、安全管理员、网络管理员、主机管理员、安全审计员、数据库管理员、应用管理员和介质管理员等岗位;
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系统安全管理制度体系。

8.2.1.2 制定和发布(G4)

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) 应组织相关人员对制定的安全管理制度进行论证和审定,保存安全管理制度评审记录,详细记录相关人员的评审意见;
c) 应对安全管理制度设定统一格式并进行版本控制;
d) 应注明安全管理制度的发布范围,并记录和保存发布记录;
e) 安全管理制度应通过正式、有效的方式进行发布;
f) 设有密级的安全管理制度,应注明安全管理制度的密级,并进行密级管理。

8.2.1.3 评审和修订(G4)

a) 信息系统安全工作领导小组应至少每年,或当技术基础架构和组织架构等发生变更时,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,保存评审记录,并对存在不足或需要改进的安全管理制度进行修订;
b) 应明确需要定期修订的安全管理制度并注明修订周期,指定部门或人员负责安全管理制度的日常维护;
c) 应根据安全管理制度的相应密级确定评审和修订的人员范围。

8.2.2 安全管理机构

8.2.2.1 岗位设置(G4)

a) 应设立负责信息系统安全管理工作的职能部门,以及安全主管、安全管理员等岗位,并明确各个岗位的职责;
b) 应设立系统管理员、网络管理员、数据库管理员等岗位,并明确各个工作岗位的职责;
c) 应成立信息系统安全工作领导小组,负责协调本单位及所辖范围的信息系统安全管理工作,决策本单位及所辖范围的信息系统安全重大事宜。领导小组最高领导应由单位主管领导委任或授权;
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。

8.2.2.2 人员配备(G4)

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) 安全管理员应为专职人员,不可兼任其他岗位;
c) 网络管理、系统管理、数据库管理等关键岗位应至少配备 2 人,实行共同管理。

8.2.2.3 授权和审批(G4)

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门及批准人。审批事项包括但不限于

系统投入运行、网络系统接入和重要资源的访问等重要活动；

b) 应对重要活动建立逐级审批制度，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；

c) 应至少每年一次审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息，并保存审查记录；

d) 应记录审批过程并保存审批文档。

8.2.2.4 沟通和合作(G4)

a) 应加强管理人员之间、内部组织机构之间以及信息系统安全管理职能部门之间的合作与沟通，定期或不定期召开协调会议，共同协作处理信息系统安全问题；

b) 应加强与同业单位、公安机关、安全机关、运营商的合作与沟通，以文档形式明确合作内容和合作方式；

c) 应加强与供应商、业界专家、专业安全公司、安全组织的合作与沟通，以文档形式明确合作内容和合作方式；

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，外联单位应包括公安机关、运营商、供电部门、专业安全公司、安全组织等；

e) 应聘请信息安全专家作为常年安全顾问，指导信息系统安全建设，参与安全规划和安全评审等工作。

8.2.2.5 审核和检查(G4)

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，并保存安全检查记录；

c) 应制定安全检查表格，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，规范安全审核和安全检查工作，定期进行安全审核和安全检查活动。

8.2.3 人员安全管理

8.2.3.1 人员录用(G4)

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，重点关注其在原工作单位是否存在信息安全违规和犯罪记录，保存审查和考核结果；

c) 应签署保密协议，保密协议应明确保密范围、保密责任、违约责任和有效期限等内容；

d) 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。关键岗位包括但不限于数据库管理员、网络管理员、系统管理员、安全管理员等，安全协议包括但不限于安全责任、违约责任和有效期限等内容。

8.2.3.2 人员离岗(G4)

a) 应制定有关管理规范，严格规范人员离岗程序，及时终止离岗员工的所有访问权限，包括但不限于物理访问权限、网络设备访问权限、操作系统访问权限、数据库访问权限、应用系统访问权限、用户终端访问权限等；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，详细记录交还情况；

c) 应办理严格的调离手续并保存调离手续记录，关键岗位人员须在承诺调离后的保密义务后方可离开。

8.2.3.3 人员考核(G4)

a) 应至少每年一次对各个岗位的人员进行安全认知、安全技能及信息系统安全等级保护相关内容的考核;
b) 应至少每年一次对关键岗位的人员进行全面、严格的安全审查和技能考核;
c) 应建立保密制度,并定期或不定期地对保密制度执行情况进行检查或考核;
d) 应对考核结果进行记录并保存,详细记录考核时间、考核内容和考核结果等内容。

8.2.3.4 安全意识教育和培训(G4)

a) 应对定期开展安全教育和培训进行书面规定,针对不同岗位制定不同的年度培训计划;
b) 应至少每年一次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;
c) 应对安全教育和培训的情况和结果进行记录并归档保存;
d) 应对安全责任和惩戒措施进行书面规定并告知相关人员,对违反安全策略和规定的人员进行惩戒;
e) 应每年对专业人员进行信息系统安全技术提升培训,并对培训情况进行记录归档保存;信息系统安全专业人员晋升时,应进行安全专业技能考核。

8.2.3.5 外部人员访问管理(G4)

a) 对外部人员允许访问的区域、系统、设备、信息等,应进行书面规定并按照规定执行;
b) 外部人员在访问机房、重要服务器或设备区等受控区域前,应先提出书面申请,批准后由专人全程陪同或监督,并登记备案,详细记录外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息;
c) 应禁止外部来访人员的移动设备如 U 盘、移动硬盘、手机等直接接入到系统;
d) 关键区域不应允许外部人员访问。

8.2.4 系统建设管理

8.2.4.1 系统定级(G4)

a) 应明确信息系统的边界和安全保护等级;
b) 应以书面的形式说明信息系统确定为某个安全保护等级的方法和理由;
c) 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定;
d) 信息系统的定级结果应经过相关部门批准。

8.2.4.2 安全方案设计(G4)

a) 应根据系统的安全保护等级选择基本安全措施,并依据风险分析结果补充和调整安全措施;
b) 应根据信息系统的等级划分情况,统一确定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;
c) 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,制定近期和远期安全建设工作计划,计划内容包括但不限于工作目标、建设内容和责任部门等;
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、详细设计方案等文件的合理性和正确性进行论证和审定,并经过批准后才能正式实施;
e) 应根据等级测评、安全评估结果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、详细设计方案等文件。

8.2.4.3 产品采购和使用(G4)

a) 信息系统安全产品的采购和使用应符合国家有关规定,如根据信息系统安全需求选择使用相应等级的产品;
b) 密码产品的采购和使用应符合国家密码主管部门的要求,如系统中使用的密码产品应具有国家密码主管部门颁发的销售许可证;

c) 应指定或授权专门的部门负责信息系统安全产品采购;
d) 应预先对信息系统安全产品进行选型测试,确定产品的候选范围,并定期审定和更新候选产品名单;
e) 应委托专业测评单位对重要信息系统安全产品进行专项测试,根据测试结果选用产品。

8.2.4.4 自行软件开发(G4)

a) 开发环境应与实际运行环境物理分开,开发人员应与测试人员分离;
b) 应制定软件开发管理制度,明确规定开发过程的控制方法和人员行为准则,明确应经过授权、审批的开发活动;
c) 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;
d) 应在软件开发的需求、设计、编码和测试等各个环节,引入安全的开发方法以提高软件安全性,减少软件的安全缺陷和漏洞;
e) 应制定代码编写安全规范,要求开发人员按照规范编写代码;
f) 应对程序资源库的修改、更新、发布进行授权和批准;
g) 开发人员应为专职人员,开发人员的开发活动应受到有效的安全监控。

8.2.4.5 外包软件开发(G4)

a) 应根据开发需求检测软件质量,检测范围应包括代码质量、软件功能和性能等;
b) 应在软件安装之前检测软件包中可能存在的恶意代码,应保存恶意代码检测报告;
c) 应确保软件开发单位提供软件设计的相关文档和使用指南;
d) 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木马和隐蔽信道;若开发单位未能提供软件源代码,则应要求开发单位提供第三方机构出具的软件源代码审查报告。

8.2.4.6 工程实施(G4)

a) 应指定或授权专门的部门或人员负责工程实施过程管理;
b) 应制订详细的工程实施方案,工程实施方案应明确工程时间限制、进度控制和质量控制等内容,并要求工程实施单位严格执行工程实施方案;
c) 应制定工程实施管理制度,明确规定实施过程的控制方法和人员行为准则;
d) 应通过第三方工程监理监控项目的实施过程。

8.2.4.7 测试验收(G4)

a) 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,测试验收方案应明确规定参与测试的部门、人员、测试验收内容、现场操作过程等内容,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;
b) 应委托第三方测试机构对系统进行安全性测试,并出具安全性测试报告。报告应具有第三方测试机构的签字和盖章,报告内容应包括但不限于测试时间、测试地点、测试人员、测试对象、测试方法、测试过程、测试中发现的安全问题、整改建议和测试结论;
c) 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;
d) 应对系统测试验收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测试验收的管理,并按照管理规定完成系统测试验收工作。

8.2.4.8 系统交付(G4)

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进行相应的技能培训;
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管理,并按照管理规定完成系统交付工作。

8.2.4.9 系统备案(G4)

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;
b) 应将系统等级结果及相关材料报邮政管理部门备案,并保存相关备案记录;
c) 应将系统等级结果及相关材料报公安机关备案,并保存相关备案记录。

8.2.4.10 等级测评(G4)

a) 在系统运行过程中,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;
b) 应在系统发生变更时及时对系统进行等级测评,级别发生变化的应及时进行安全改造,不符合相应等级保护标准要求的应及时整改;
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;
d) 应指定或授权专门的部门或人员负责等级测评管理。

8.2.4.11 安全服务商选择(G4)

a) 安全服务商的选择应符合国家有关规定;
b) 应与选定的安全服务商签订安全协议,明确约定相关责任、保密范围、有效期限等内容;
c) 选定的安全服务商应提供技术培训和服务承诺,必要的与其签订服务合同,内容包括但不限于技术培训、服务承诺、服务期限等;
d) 在与安全服务商签订有效的服务合同之前,应评估安全服务商的引入风险,确保风险在可接受范围内。

8.2.5 系统运维管理

8.2.5.1 环境管理(G4)

a) 应指定专门的部门或人员至少每季度对机房供配电、空调、温湿度控制等设施设备进行维护管理;
b) 应指定专门的部门负责机房安全,配备机房安全管理人员,对设备与人员进出机房、服务器的开关等工作进行管理;
c) 应建立机房安全管理制度,对有关人员进出机房,物品带进、带出机房和机房环境安全等作出规定;
d) 应加强对办公环境的保密性管理,包括工作人员调离办公室应立即交还办公室钥匙、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不放含有敏感信息的纸质文件等;
e) 应对机房和办公环境实行统一安全管理,对出入人员进行相应级别的授权,实时监视和记录进入重要安全区域的活动。

8.2.5.2 资产管理(G4)

a) 应建立资产管理制度,规定信息系统资产管理的责任部门或人员,规范资产使用和管理行为,明确资产使用、传输、存储、维护以及职责划分等内容;
b) 应编制并保存与信息系统相关的资产清单,包括资产的重要程度、价值和类别、责任部门和所处位置等;
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。

8.2.5.3 介质管理(G4)

a) 应建立介质安全管理制度,对介质的存放环境、使用、维护和销毁等作出规定;
b) 介质应存放在安全环境中,专人负责保护和管理各类介质;
c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行管控,对介质归档和查询等过程进行记录,每季度应根据清单对介质的现状进行检查;

d) 应对存储介质的使用、送出维修以及销毁等进行严格管理。重要数据的存储介质带出工作环境应对内容进行加密并进行监控,对于需要送出维修或销毁的介质应采用多次读写方式覆盖、清除敏感或秘密数据,销毁无法执行删除操作的受损介质,保密性要求较高的信息存储介质应获得批准并在双人监控下才能销毁,销毁记录应妥善保存;

e) 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;

f) 应对重要介质中的数据和软件采取加密存储,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,如粘贴纸质标签等。

8.2.5.4 设备管理(G4)

a) 应指定专门的部门或人员定期对信息系统相关的各种设备、线路等进行维护管理;

b) 应建立设备安全管理制度,对信息系统各种软硬件设备的选型、采购、发放和领用等作出规定;

c) 应对服务器、计算机终端、业务移动终端、网络等设备的操作和使用进行规范化管理,按照操作规程实现设备的启动、停止、加电、断电等操作;

d) 信息处理设备应经过审批后才能带离机房或办公地点;

e) 应建立机房配套设备的维护管理制度,明确维护人员的责任、涉外维修和服务的审批、维修过程的监督等,并保存设备的涉外维修和服务过程的申请和审批记录。

8.2.5.5 监控管理和安全管理中心(G4)

a) 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;

b) 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,发现异常时报警,形成记录并妥善保存;

c) 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;

d) 应部署运维审计设备,实现集中账户管理、集中认证、集中授权、集中访问控制、集中安全审计功能。

8.2.5.6 网络安全管理(G4)

a) 应指定人员对网络安全进行管理,负责运行日志和网络监控记录的日常维护,以及报警信息的分析处理工作;

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,并在更新前对重要文件进行备份;

d) 应定期对网络系统进行漏洞扫描,及时对发现的安全漏洞进行修补。在实施漏洞扫描或漏洞修补前,应对可能的风险进行评估,做好充分准备,如选择恰当时间、制定数据备份和回退方案。在漏洞扫描或漏洞修补后应进行验证测试,以保证网络系统正常运行;

e) 应实现网络设备的最小服务配置,并对配置文件进行定期离线备份;

f) 所有与外部系统的连接均应得到授权和批准;

g) 应禁止便携式和移动式设备接入网络;

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,并保存检查记录;

i) 应严格控制网络管理用户的授权,授权应有两人在场并经双方认可后方可操作,操作过程应保留不可更改的日志记录。

8.2.5.7 系统安全管理(G4)

a) 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作出规定;

b) 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,分配信息系统、文件及服务的访问

权限；

c） 应定期进行漏洞扫描，及时对发现的安全漏洞进行修补。在实施漏洞扫描或漏洞修补前，应对可能的风险进行评估，做好充分准备，如选择恰当时间、制订好数据备份和回退方案。在漏洞扫描或漏洞修补后应进行验证测试，以保证系统的正常运行；

d） 应安装最新的系统补丁程序。应首先在测试环境中测试通过系统补丁程序，并对重要文件进行备份后，方可实施系统补丁程序的安装；

e） 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、参数的设置和修改等内容，严禁进行未经授权的操作；

f） 应定期对运行日志和审计数据进行分析，及时发现异常行为；

g） 应指定专人对系统进行安全管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应遵循最小授权原则；

h） 应对系统资源的使用进行预测，以确保充足的处理速度和存储容量。管理人员应随时注意处理器、存储设备和输入设备等系统资源的使用情况。

8.2.5.8 恶意代码防范管理（G4）

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或邮件之前，先进行病毒检查，在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） 应制定病毒防范管理制度，对防恶意代码软件的授权使用、恶意代码库升级等作出明确规定；

c） 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，及时对截获的危险病毒或恶意代码进行处理；

d） 应至少每月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，及时对主机防病毒产品、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分析处理，并进行书面报告。

8.2.5.9 密码管理（G4）

应建立密码使用管理制度，明确密码产品和技术选型、采购、授权使用、日常维护、废弃等全生命周期管理内容；应采用符合国家密码管理规定的密码技术和已获得商用密码产品销售许可证的密码产品。

8.2.5.10 变更管理（G4）

a） 应明确系统的重要变更事项并制订相应的变更方案，明确变更类型、变更原因、变更过程、变更前评估、回退方式等内容；

b） 应建立变更管理制度。在变更系统前向主管领导申请，变更和变更方案经过评审、审批后方可实施，并在实施后向相关人员通告变更情况；

c） 应对变更影响进行分析，记录变更实施过程，并妥善保存所有文档和记录；

d） 应建立变更中止与变更失败恢复程序，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） 应定期检查变更申报审批程序的执行情况，对系统现状与文档记录的一致性进行评估。

8.2.5.11 备份与恢复管理（G4）

a） 应明确需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应建立备份与恢复安全管理制度，对备份信息的备份方式、备份频率、存储介质和保存期等作出规定；

c） 应根据数据的重要性和数据对系统运行的影响程度，制定数据的备份策略和恢复策略。备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和数据离站运输的方法；

d） 应建立数据备份和恢复过程控制程序，记录备份过程。对需要加密或进行数据隐藏处理的备份数据，在进行备份和加密操作时，应要求两名工作人员在场。所有文件和记录应妥善保存；

e) 应至少每年一次执行恢复程序,检查和测试备份介质的有效性,确保在规定的时间内完成备份恢复;

f) 应根据信息系统的备份要求,制订相应的灾难恢复计划,并对其进行测试以确保各个恢复规程的正确性和计划整体的有效性。测试内容包括运行系统恢复、备用系统性能测试、通信连接、人员协调等,根据测试结果对不适用的规定进行修改或更新。

8.2.5.12 安全事件处置(G4)

a) 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、现场处理、事件报告和后期恢复等内容;

b) 应根据国家相关管理部门的计算机安全事件等级划分方法和安全事件对系统产生的影响,对信息系统计算机安全事件进行等级划分,建立安全事件定级文档,明确安全事件的定义、等级划分原则、等级描述等内容;

c) 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;

d) 应报告所发现的安全弱点和可疑事件,在任何情况下均不应尝试验证安全弱点;

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,明确具体的报告方式、报告内容、报告人员和处理程序等内容;

g) 发生可能涉及国家秘密的重大失密、泄密事件,应按照相关规定及时向保密等部门汇报;

h) 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。

8.2.5.13 应急预案管理(G4)

a) 应制订统一的应急预案框架,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) 在统一的应急预案框架下,分别制订不同事件的应急预案;

c) 应至少每年一次对系统相关人员进行应急预案培训;

d) 应制定应急保障制度,从人力、设备、技术和财务等方面确保应急预案的执行;

e) 应定期对应急预案进行演练,并保存演练记录,记录应包括应急演练过程、审批过程、相关人员及签字、演练内容及结果等;应根据不同的应急恢复内容,确定演练周期,至少每年演练一次。在演练后对应急预案进行审查,保存审查记录;

f) 应规定应急预案中需要定期审查和更新的内容,并按照执行;

g) 应根据信息系统的变更情况定期对原有的应急预案进行重新评估、修订完善,并保存评估和修订记录。

9 第五级基本要求

略。

附 录 A
（规范性附录）
基本要求的选择和使用

A.1 概述

不同安全保护等级的信息系统，对业务信息的安全性要求和系统服务的连续性要求可能存在差异，其安全保护等级由业务信息安全等级和系统服务保证等级较高者决定。因此，对某个定级后的信息系统的安全要求可以有多种组合。

A.2 定级组合

信息系统定级后，不同安全保护等级的信息系统可能形成的定级结果组合见表 A.1。

表 A.1 信息系统可能形成的定级结果组合

安全保护等级	信息系统可能形成的定级结果组合
第一级	S1A1G1P1
第二级	S1A2G2P2，S2A2G2P2，S2A1G2P2
第三级	S1A3G3P3，S2A3G3P3，S3A3G3P3，S3A2G3P3，S3A1G3P3
第四级	S1A4G4P4，S2A4G4P4，S3A4G4P4，S4A4G4P4，S4A3G4P4，S4A2G4P4，S4A1G4P4

本标准中的每级安全等级保护的基本安全要求按照业务信息安全等级和系统服务保证等级相同的情况来组织，即针对 S1A1G1P1、S2A2G2P2、S3A3GP33 和 S4A4G4P4 的情况给出。

A.3 选择和使用

对于确定了安全保护等级的信息系统，选择和使用基本安全要求时，可以按照以下过程进行：

a) 明确信息系统应该具有的安全保护能力，根据信息系统的安全保护等级选择基本安全要求，包括技术要求和管理要求。根据本标准，一级系统选择第一级基本安全要求，二级系统选择第二级基本安全要求，三级系统选择第三级基本安全要求，四级系统选择第四级基本安全要求，以此作为出发点；

b) 根据信息系统的定级结果对基本安全要求进行调整。根据系统服务安全等级选择相应等级的系统服务保证类（A 类）基本要求；根据业务信息安全等级选择相应等级的业务信息安全类（S 类）基本要求；

c) 针对信息系统的不同特点，分析可能在某些方面存在的特殊安全保护能力要求，由此选择较高级别的基本安全要求或补充基本安全要求；

d) 本标准中提出的基本安全要求无法实现的或另有更加有效的安全措施可以替代的，可以对基本安全要求进行调整，调整的原则是保证不降低信息系统的整体安全保护能力。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[5] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
[6] GB/T 202282—2006 信息安全技术 信息系统安全工程管理要求
[7] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型
[8] GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件
[9] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件
[10] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[11] SP 800-53 Recommended Security Controls for Federal Information Systems
[12] SP 800-82 Guide to Industrial Control Systems (ICS) Security
[13] SP 800-124 Rev.1 Guidelines for Managing the Security of Mobile Devices in the Enterprise