ICS 35.020
L 07

MH

中华人民共和国民用航空行业标准

MH/T 0076—2020

民用航空网络安全等级保护基本要求

Baseline for classified protection of cybersecurity in civil aviation

2020－07－20发布　　2020－10－01实施

中国民用航空局　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学、广东机场白云信息科技有限公司、南开大学。

本标准主要起草人：刘春波，麦钊明，隋鬻，罗军，刘哲理，陈光锋，王志，刘超，周景贤，王双，张礼哲，马勇，顾兆军，吕宗平。

引　言

依据GB/T 1.1—2009《标准化工作导则 第一部分：标准的结构和编写》、《中华人民共和国网络安全法》、《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）、《信息安全等级保护管理办法》（公通字〔2007〕43号）、GB/T 22239《信息安全技术 网络安全等级保护基本要求》和《民航网络与信息安全管理暂行办法》（MD-PE-2013-01）、《关于进一步加强民航网络和信息安全工作的通知》（民航人发〔2013〕62号）要求制定本标准。

本标准在GB/T 22239《信息安全技术 网络安全等级保护基本要求》基础上，依据民航行业系统特征，提出和规定了不同安全保护等级保护对象的基本安全保护要求。

本标准是民用航空网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——MH/T 0069 民用航空网络安全等级保护定级指南。

在本标准中，加粗字部分表示较高等级中增加或增强的要求。

民用航空网络安全等级保护基本要求

1 范围

本标准规定了民用航空网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。

本标准适用于指导分等级的非涉密民用航空网络安全等级保护对象的安全建设和监督管理。

注：第五级等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本标准中进行描述。

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 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

MH/T 0069 民用航空网络安全等级保护定级指南

3 术语和定义

GB/T 25069、GB/T 22239和MH/T 0069确立的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 22239中的一些术语和定义。

3.1

网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 22239—2019，术语和定义3.1]

3.2

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

[GB/T 22239—2019，术语和定义3.2]

3.3

（民航）生产网 production network (of civil aviation)

承载民航运输生产业务系统的网络设施。

3.4

办公网 office network

承载办公自动化系统的网络设施。

4 民用航空网络安全等级保护概述

4.1 等级保护对象

等级保护对象是指网络安全等级保护工作中的对象，通常是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统，主要包括基础信息

网络、云计算平台/系统、大数据平台/系统、物联网、工业控制系统以及采用移动互联技术的系统等。等级保护对象根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为五个安全保护等级。

民用航空保护对象的安全保护等级确定方法见MH/T 0069。

4.2 不同级别的安全保护能力

不同级别的等级保护对象应具备的基本安全保护能力如下：

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

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

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

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

第五级安全保护能力：略。

4.3 安全通用要求和安全扩展要求

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

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

本标准根据民用航空行业的实际情况，对GB/T 22239中的安全通用要求进行了细化或增强，对云计算、移动互联、物联网、工业控制系统的安全扩展要求与GB/T 22239一致。对于采用其他特殊技术或处于特殊应用场景的等级保护对象，应在安全风险评估的基础上，针对安全风险采取特殊的安全措施作为补充。

5 第一级安全要求

5.1 安全通用要求

5.1.1 安全物理环境

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

应将设备或主要部件进行固定，并设置明显的不易除去的标识。

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

应设置必要的温湿度调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

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 安全通信网络

5.1.2.1 通信传输

应采用校验技术保证通信过程中数据的完整性。

5.1.2.2 可信验证

可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

5.1.3 安全区域边界

5.1.3.1 边界防护

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

5.1.3.2 访问控制

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。

5.1.3.3 可信验证

可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

5.1.4 安全计算环境

5.1.4.1 身份鉴别

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。

5.1.4.2 访问控制

包括：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在。

5.1.4.3 入侵防范

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。

5.1.4.4 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。

5.1.4.5 可信验证

可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

5.1.4.6 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性。

5.1.4.7 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。

5.1.5 安全管理制度

5.1.5.1 管理制度

应建立日常管理活动中常用的安全管理制度。

5.1.6 安全管理机构

5.1.6.1 岗位设置

应设立系统管理员等岗位，并定义各个工作岗位的职责。

5.1.6.2 人员配备

应配备一定数量的系统管理员。

5.1.6.3 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。

5.1.7 安全管理人员

5.1.7.1 人员录用

应指定或授权专门的部门或人员负责人员录用。

5.1.7.2 人员离岗

应及时终止离岗员工的所有访问权限，收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

5.1.7.3 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。

5.1.7.4 外部人员访问管理

应保证在外部人员访问受控区域前得到授权或审批。

5.1.8 安全建设管理

5.1.8.1 定级和备案

应依据MH/T 0069，以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。

5.1.8.2 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。

5.1.8.3 产品采购和使用

应确保网络安全产品采购和使用符合国家的有关规定；

5.1.8.4 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。

5.1.8.5 测试验收

应进行安全性测试验收。

5.1.8.6 系统交付

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。

5.1.8.7 服务供应商选择

包括：

a) 应确保服务供应商的选择符合国家和行业的有关规定；
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。

5.1.9 安全运维管理

5.1.9.1 环境管理

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) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等方面。

5.1.9.2 介质管理

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

5.1.9.3 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。

5.1.9.4 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。

5.1.9.5 网络和系统安全管理

包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

5.1.9.6 恶意代码防范管理

包括：

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

5.1.9.7 备份与恢复管理

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。

5.1.9.8 安全事件处置

包括：

a) 应及时向网络安全管理部门报告所发现的安全弱点和可疑事件；
b) 应根据行业有关规定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；
c) 收到国家和行业有关部门发出的网络安全风险事件通报后，应及时排查处置并反馈处置情况。

5.2 云计算安全扩展要求

应符合GB/T 22239—2019中6.2的要求。

5.3 移动互联安全扩展要求

应符合GB/T 22239—2019中6.3的要求。

5.4 物联网安全扩展要求

应符合GB/T 22239—2019中6.4的要求。

5.5 工业控制系统安全扩展要求

应符合GB/T 22239—2019中6.5的要求。

6 第二级安全要求

6.1 安全通用要求

6.1.1 安全物理环境

6.1.1.1 物理位置选择

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) **机房外墙壁应没有对外的窗户；否则，应采用双层固定窗，并做密封、防水处理；**
c) **机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，否则应加强防水和防潮措施。**

6.1.1.2 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。

6.1.1.3 防盗窃和防破坏

包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；
b) **应将通信线缆铺设在隐蔽安全处。**

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

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

包括：

a) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下铺有水管的，应采取有效防护措施；

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

应采用防静电地板或地面并采用必要的接地防静电措施。

6.1.1.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内，开机时，机房温度应控制在22 ℃～24 ℃，相对湿度应控制在40%～55%。

6.1.1.9 电力供应

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 安全通信网络

6.1.2.1 网络架构

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，设备 CPU 和内存使用率峰值不大于70%，业务高峰流量不超过设备处理能力的 70%；

b) 应保证网络各个部分的带宽满足业务高峰期需要，各通信链路高峰流量均不大于其带宽的70%；

c) 生产网与互联网、办公网应进行安全隔离，民航单位内部网络应与机场、航空器等公共场所的旅客公共服务网络安全隔离。

d) 应根据承载业务的类型和重要性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；

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

6.1.2.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

6.1.2.3 可信验证

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

6.1.3 安全区域边界

6.1.3.1 边界防护

包括：

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；

应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

6.1.3.2 访问控制

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。**

6.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为，包括但不限于端口扫描、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、网络蠕虫攻击等。

6.1.3.4 恶意代码防范

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。

6.1.3.5 安全审计

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。**

6.1.3.6 可信验证

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

6.1.4 安全计算环境

6.1.4.1 身份鉴别

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，**对于口令的具体要求如下：**
   1) 长度不小于 8 位；
   2) 由大小写字母、数字和特殊字符组成；
   3) 不得与账户名相同；
   4) 不得明文存储；
   5) 至少每半年更换一次；
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，**非法登录次数最多为 5 次，登录失败后锁定时间不少于 10min，登录连接超时不得超过 10 min**；
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。**

6.1.4.2 访问控制

包括：

a) 对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) **应授予管理用户所需的最小权限，实现管理用户的权限分离。**

6.1.4.3 安全审计

包括：

a) 应启用安全审计功能，审计覆盖到每个用户；系统不支持该要求的，应采用第三方安全审计产品实现审计要求；审计内容至少包括用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等重要的用户行为和安全事件；
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 入侵防范

包括：
a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的系统服务、默认共享和高危端口；
c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞或采用其他有效方式进行安全防护。

6.1.4.5 恶意代码防范

包括：
a) 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；
b) 应支持防恶意代码的统一管理。

6.1.4.6 可信验证

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

6.1.4.7 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

6.1.4.8 数据备份恢复

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。

6.1.4.9 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。

6.1.4.10 个人信息保护

本项要求包括：
a) 应仅采集和保存开展民航相关业务必需的旅客等用户的个人信息；
b) 应禁止未授权访问、非法使用和非法转移旅客等用户的个人信息。

6.1.5 安全管理中心

6.1.5.1 系统管理

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

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

6.1.5.2 审计管理

包括：

a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；
c) 应保证审计记录的留存时间符合法律法规要求，满足业务需要。

6.1.6 安全管理制度

6.1.6.1 安全策略

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

6.1.6.2 管理制度

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，覆盖物理环境、通信网络、计算环境、数据、建设和运维等方面；
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。

6.1.6.3 制定和发布

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。

6.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。发生重大变更时，应及时对制度进行修订。

6.1.7 安全管理机构

6.1.7.1 岗位设置

包括：

a) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
b) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

6.1.7.2 人员配备

应配备一定数量的系统管理员、审计管理员、安全管理员等。

6.1.7.3 经费保障

应保障网络和信息系统安全防护加固、安全运维、安全检查、安全测评、系统安全升级改造、网络安全教育培训、网络安全事件应急处置等网络安全方面的经费预算。

6.1.7.4 授权和审批

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。

6.1.7.5 沟通和合作

包括：

a) 应加强各类管理人员之间、组织内部机构之间以及网络安全管理部门内部的合作与沟通，领导班子主要负责人每年至少召集一次网络安全专题会议，网络安全主管领导至少每季度召集一次网络安全会议；
b) 应加强与民用航空监管机构、网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

6.1.7.6 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。

6.1.8 安全管理人员

6.1.8.1 人员录用

包括：

a) 应指定或授权专门的部门或人员负责人员录用；
b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查；
c) 应与系统管理员、审计管理员、安全管理员等关键岗位的人员签署岗位责任协议。

6.1.8.2 人员离岗

应及时终止离岗员工的所有访问权限，收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

6.1.8.3 安全意识教育和培训

包括：

a) 应对各类人员进行安全意识教育和岗位技能培训，并告知人员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，对网络安全基础知识、岗位操作规程等进行培训，在职人员年度人均接受培训时间不少于 4 个学时，网络安全关键岗位人员年度人均接受培训时间不少于 8 个学时。

6.1.8.4 外部人员访问管理

包括：

a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
c) 外部人员离场后应及时清除其所有的访问权限。

6.1.9 安全建设管理

6.1.9.1 定级和备案

包括：

a) 应依据 MH/T 0069，以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
c) 应保证定级结果经过相关部门的批准；
d) 应将备案材料报相应公安机关备案，并将备案结果报所在地民航行政管理机构。

6.1.9.2 安全方案设计

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；涉及关键信息基础设施的，应报民航网络安全管理部门进行网络安全专项审查。**

6.1.9.3 产品采购和使用

包括：

a) 应确保网络安全产品采购和使用符合国家的有关规定；

b) **应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。**

6.1.9.4 自行软件开发

包括：

a) **应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；**

b) **应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。**

6.1.9.5 外包软件开发

包括：

a) **应在软件交付前检测其中可能存在的恶意代码；**

b) **应保证开发单位提供软件设计文档和使用指南。**

6.1.9.6 工程实施

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。**

6.1.9.7 测试验收

包括：

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

b) **应委托专业安全机构进行上线前的安全性测试，并出具安全测试报告；**

c) **应确保系统通过安全性测试后才能接入互联网。**

6.1.9.8 系统交付

包括：

a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b) 应对负责运行维护的技术人员进行相应的技能培训；

c) **应提供建设过程文档和运行维护文档。**

6.1.9.9 等级测评

包括：

a) **应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；**

b) **应在发生重大变更或级别发生变化时进行等级测评；**

c) **应确保测评机构的选择符合国家有关规定。**

6.1.9.10 服务供应商选择

包括：

a) 应确保服务供应商的选择符合国家和行业的有关规定；

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

6.1.10 安全运维管理

6.1.10.1 环境管理

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) 应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等；
c) **应严格控制手机、便携式电脑等电子产品带入机房；**
d) **应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。**

6.1.10.2 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。

6.1.10.3 介质管理

包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
b) **应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；**
c) **应对移动存储介质的安全使用作出规定，避免交叉混用，造成信息泄露和恶意代码传播。**

6.1.10.4 设备维护管理

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

6.1.10.5 漏洞和风险管理

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) **实施漏洞修补前，应对可能的风险进行评估和充分准备，做好数据备份和回退方案；**
c) **漏洞修补后，应进行验证测试。**

6.1.10.6 网络和系统安全管理

包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
c) **应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；**
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。**

6.1.10.7 恶意代码防范管理

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) **应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。**

6.1.10.8 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。

6.1.10.9　密码管理

包括：

a）**应遵循密码相关国家标准和行业标准；**

b）**应使用国家密码管理主管部门认证核准的密码技术和产品。**

6.1.10.10　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。

6.1.10.11　备份与恢复管理

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。**

6.1.10.12　安全事件处置

包括：

a）应及时向网络安全管理部门报告所发现的安全弱点和可疑事件；

b）**应根据行业有关规定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）收到国家和行业有关部门发出的网络安全风险事件通报后，应及时排查处置并反馈处置情况。

6.1.10.13　应急预案管理

包括：

a）**应按照民航网络安全事件应急预案，制定本单位网络安全专项应急预案，纳入本单位总体应急预案体系；**

b）**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，预案应详细，具备可操作性；**

c）**应对系统管理员、审计管理员、安全管理员、业务人员等相关人员进行应急预案培训，并进行应急预案的演练，上述培训和演练应每年至少开展一次。**

6.1.10.14　外包运维管理

包括：

a）**应确保外包运维服务商的选择符合国家和行业的有关规定；**

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。**

6.2　云计算安全扩展要求

应符合GB/T 22239—2019中7.2的要求。

6.3　移动互联安全扩展要求

应符合GB/T 22239—2019中7.3的要求。

6.4　物联网安全扩展要求

应符合GB/T 22239—2019中7.4要求。

6.5　工业控制系统安全扩展要求

应符合GB/T 22239—2019中7.5的要求。

7 第三级安全要求

7.1 安全通用要求

7.1.1 安全物理环境

7.1.1.1 物理位置选择

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) 机房外墙壁应没有对外的窗户；否则，应采用双层固定窗，并做密封、防水处理；
c) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，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

包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；
b) 应将通信线缆铺设在隐蔽安全处；
c) **应设置机房防盗报警系统或设置有专人值守的视频监控系统。**

7.1.1.4 防雷击

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

包括：

a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
c) **应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。**

7.1.1.6 防水和防潮

包括：

a) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下铺有水管的，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的转移与渗透；
d) **应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。**

7.1.1.7 防静电

包括：

a) 应采用防静电地板或地面并采用必要的接地防静电措施；
b) **应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。**

7.1.1.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内，开机时，机房温度应控制在22 ℃～24 ℃，相对湿度应控制在40%～55%。

7.1.1.9 电力供应

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。**

7.1.1.10 电磁防护

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 安全通信网络

7.1.2.1 网络架构

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，设备 CPU 和内存使用率峰值不大于 70%，业务高峰流量不超过设备处理能力的 70%；
b) 应保证网络各个部分的带宽满足业务高峰期需要，各通信链路高峰流量均不大于其带宽的 70%；
c) 生产网与互联网、办公网应进行安全隔离，民航单位内部网络应与机场、航空器等公共场所的旅客公共服务网络安全隔离。
d) 应根据承载业务的类型和重要性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；
e) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
a) **应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。**

7.1.2.2 通信传输

包括：

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

7.1.2.3 可信验证

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

7.1.3 安全区域边界

7.1.3.1 边界防护

包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
b) **应能够对非授权设备私自联到内部网络的行为进行检查或限制；**
c) **应能够对内部用户非授权联到外部网络的行为进行检查或限制；**
d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。

7.1.3.2 访问控制

包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
e) **应对进出网络的数据流实现基于应用协议和应用内容的访问控制；**
f) **应在互联网出口和核心网络接口处限制网络最大流量数及网络连接数；**
g) **重要网段应采取技术手段防止地址欺骗。**

7.1.3.3 入侵防范

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，包括但不限于端口扫描、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、网络蠕虫攻击等；**
b) **应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为，包括但不限于端口扫描、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、网络蠕虫攻击等；**
c) **应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；**
d) **当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。**

7.1.3.4 恶意代码和垃圾邮件防范

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。**

7.1.3.5 安全审计

包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
d) **应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。**

7.1.3.6 可信验证

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

7.1.4 安全计算环境

7.1.4.1 身份鉴别

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，对于口令的具体要求如下：
   1) 长度不小于 8 位；
   2) 由大小写字母、数字和特殊字符组成；
   3) 不得与账户名相同；
   4) 不得明文存储；
   5) 至少每**季度**更换一次；
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，非法登录次数最多为 5 次，登录失败后锁定时间不少于 10 分钟，登录连接超时不得超过 10 分钟；
c) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
d) **应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。**

7.1.4.2 访问控制

包括：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
e) **应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；**
f) **访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；**
g) **应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。**

7.1.4.3 安全审计

包括：

a) 应启用安全审计功能，审计覆盖到每个用户；系统不支持该要求的，应采用第三方安全审计产品实现审计要求；审计内容至少包括用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等重要的用户行为和安全事件；
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。**

7.1.4.4 入侵防范

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) 应对移动存储介质在服务器和终端中的使用进行严格管控；
d) 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；
e) 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；
f) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞或采用其他有效方式进行安全防护；
g) **应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。**

7.1.4.5 恶意代码防范

包括：

a) **应采用免受恶意代码攻击的技术措施或主动免疫可信计算检验机制及时识别入侵和病毒行为，并将其有效阻断；**
b) 应支持防恶意代码的统一管理。

7.1.4.6 可信验证

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

7.1.4.7 数据完整性

包括：

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

7.1.4.8 数据保密性

包括：

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

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

7.1.4.9 数据备份恢复

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。**

7.1.4.10 剩余信息保护

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。**

7.1.4.11 个人信息保护

包括：

a) 应仅采集和保存开展民航相关业务必需的旅客等用户的个人信息；

b) 应禁止未授权访问、非法使用和非法转移旅客等用户的个人信息。

7.1.5 安全管理中心

7.1.5.1 系统管理

包括：

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

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

7.1.5.2 审计管理

包括：

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

b) 应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；

c) 应保证审计记录的留存时间符合法律法规要求，满足业务需要。

7.1.5.3 安全管理

包括：

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

b) **应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。**

7.1.5.4 集中管控

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分析，对异常情况进行告警；**
d) **应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求，满足业务需要；**
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。**

7.1.6 安全管理制度

7.1.6.1 安全策略

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

7.1.6.2 管理制度

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，覆盖物理环境、通信网络、计算环境、数据、建设和运维等方面；
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网络安全管理制度体系。**

7.1.6.3 制定和发布

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。

7.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。发生重大变更时，应及时对制度进行修订。

7.1.7 安全管理机构

7.1.7.1 岗位设置

包括：
a) **应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；**
b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
c) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

7.1.7.2 人员配备

包括：
a) 应配备一定数量的系统管理员、审计管理员、安全管理员等；
b) **应配备专职安全管理员，不可兼任。**

7.1.7.3 经费保障

应保障网络和信息系统安全防护加固、安全运维、安全检查、安全测评、系统安全升级改造、网络安全教育培训、网络安全事件应急处置等网络安全方面的经费预算。

7.1.7.4 授权和审批

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。**

7.1.7.5 沟通和合作

包括：
a) 应加强各类管理人员之间、组织内部机构之间以及网络安全管理部门内部的合作与沟通，领导班子主要负责人每年至少召集一次网络安全专题会议，网络安全主管领导至少每季度召集一次网络安全会议；
b) 应加强与民用航空监管机构、网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

7.1.7.6 审核和检查

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。**

7.1.8 安全管理人员

7.1.8.1 人员录用

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，**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，**与系统管理员、审计管理员、安全管理员等关键岗位的人员签署岗位责任协议。

7.1.8.2 人员离岗

包括：
a) 应及时终止离岗员工的所有访问权限，收回各种身份证件、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。**

7.1.8.3 安全意识教育和培训

包括：
a) 应对各类人员进行安全意识教育和岗位技能培训，并告知人员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，对网络安全基础知识、岗位操作规程等进行培训，在职人员年度人均接受培训时间不少于 4 个学时，网络安全关键岗位人员年度人均接受培训时间不少于 8 个学时，**关键信息基础设施运营者的网络安全关键岗位人员年度人均接受培训时间不少于 24 个学时**；
c) **应定期对不同岗位的人员进行技能考核；**
d) **网络安全专业技术岗位人员中，获得网络安全专业资质人员占比达到 60%或虽未达到 60%但逐年提高。**

7.1.8.4 外部人员访问管理

包括：
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
c) 外部人员离场后应及时清除其所有的访问权限；
d) **获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。**

7.1.9 安全建设管理

7.1.9.1 定级和备案

包括：
a) 应依据 MH/T 0069，以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
a) 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；
b) 应保证定级结果经过相关部门的批准；
c) 应将备案材料报相应公安机关备案，并将备案结果报所在地民航行政管理机构。

7.1.9.2 安全方案设计

包括：
a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；涉及关键信息基础设施的，应报民航网络安全管理部门进行网络安全专项审查。

7.1.9.3 产品采购和使用

包括：
a) 应确保网络安全产品采购和使用符合国家的有关规定；
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
c) **应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。**

7.1.9.4 自行软件开发

包括：
a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b) **应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；**
c) **应制定代码编写安全规范，要求开发人员参照规范编写代码；**
d) **应具备软件设计的相关文档和使用指南，并对文档使用进行控制；**
e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
f) **应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；**
g) **应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。**

7.1.9.5 外包软件开发

包括：
a) 应在软件交付前检测其中可能存在的恶意代码；
b) 应保证开发单位提供软件设计文档和使用指南；
c) **应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。**

7.1.9.6 工程实施

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。**

7.1.9.7 测试验收

包括：

a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
b) 应委托专业安全机构进行上线前的安全性测试，并出具安全测试报告，**安全测试报告应包含密码应用安全性测试相关内容；**
c) 应确保系统通过安全性测试后才能接入互联网。

7.1.9.8 系统交付

包括：

a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
b) 应对负责运行维护的技术人员进行相应的技能培训；
c) 应提供建设过程文档和运行维护文档。

7.1.9.9 等级测评

包括：

a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
b) 应在发生重大变更或级别发生变化时进行等级测评；
c) 应确保测评机构的选择符合国家有关规定。

7.1.9.10 服务供应商选择

包括：

a) 应确保服务供应商的选择符合国家和行业的有关规定；
b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
c) **应定期监视、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。**

7.1.10 安全运维管理

7.1.10.1 环境管理

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，**对机房设施定期巡检**；
b) **应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；**
c) 应严格控制手机、便携式电脑等电子产品带入机房；
d) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。

7.1.10.2 资产管理

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。**

7.1.10.3 介质管理

包括：

a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
c) 应对移动存储介质的安全使用作出规定，避免交叉混用，造成信息泄露和恶意代码传播。

7.1.10.4 设备维护管理

包括：

a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
b) 应**建立**配套设施、软硬件维护**方面的管理制度，对其维护进行有效的管理**，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
c) **信息处理设备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，保证该设备上的敏感数据和授权软件无法被恢复重用。**

7.1.10.5 漏洞和风险管理

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) 实施漏洞修补前，应对可能的风险进行评估和充分准备，做好数据备份和回退方案；
c) 漏洞修补后，应进行验证测试；
d) **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。**

7.1.10.6 网络和系统安全管理

包括：

a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
f) **应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；**
g) **应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；**
h) **应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；**
i) **应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；**
j) 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。

7.1.10.7 恶意代码防范管理

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) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
d) **应定期验证防范恶意代码攻击的技术措施的有效性。**

7.1.10.8 配置管理

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。**

7.1.10.9 密码管理

包括：

a) 应遵循密码相关国家标准和行业标准；
b) 应使用国家密码管理主管部门认证核准的密码技术和产品。

7.1.10.10 变更管理

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。**

7.1.10.11 备份与恢复管理

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。

7.1.10.12 安全事件处置

包括：

a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；
b) 应根据行业有关规定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) 收到国家和行业有关部门发出的网络安全风险事件通报后，应及时排查处置并反馈处置情况；
e) **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。**

7.1.10.13 应急预案管理

包括：

a) 应按照民航网络安全事件应急预案，制定本单位网络安全专项应急预案，纳入本单位总体应急预案体系；
b) **应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；**
c) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
d) 应对系统管理员、审计管理员、安全管理员、业务人员等相关人员进行应急预案培训，并进行应急预案的演练，上述培训和演练应每年至少开展一次；
e) **应定期对原有的应急预案重新评估，修订完善。**

7.1.10.14 外包运维管理

包括：

a) 应确保外包运维服务商的选择符合国家和行业的有关规定；
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) **选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；**
d) **应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。**

7.2 云计算安全扩展要求

应符合GB/T 22239—2019中8.2的要求。

7.3 移动互联安全扩展要求

应符合GB/T 22239—2019中8.3的要求。

7.4 物联网安全扩展要求

应符合GB/T 22239—2019中8.4的要求。

7.5 工业控制系统安全扩展要求

应符合GB/T 22239—2019中8.5的要求。

8 第四级安全要求

8.1 安全通用要求

8.1.1 安全物理环境

8.1.1.1 物理位置选择

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) 机房外墙壁应没有对外的窗户；否则，应采用双层固定窗，并做密封、防水处理；
c) 机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁，否则应加强防水和防潮措施。

8.1.1.2 物理访问控制

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

包括：

a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识；
b) 应将通信线缆铺设在隐蔽安全处；
c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

8.1.1.4 防雷击

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

包括：

a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
c) 应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

8.1.1.6 防水和防潮

包括：

a) 与机房设备无关的水管不得穿过机房屋顶和活动地板下；机房屋顶和活动地板下铺有水管的，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的转移与渗透；
d) 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

8.1.1.7 防静电

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) 应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

8.1.1.8 温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内，开机时，机房温度应控制在22℃-24℃，相对湿度应控制在40%-55%。

8.1.1.9 电力供应

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

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 安全通信网络

8.1.2.1 网络架构

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，设备 CPU 和内存使用率峰值不大于70%，业务高峰流量不超过设备处理能力的 70%；
b) 应保证网络各个部分的带宽满足业务高峰期需要，各通信链路高峰流量均不大于其带宽的 70%；
c) 生产网与互联网、办公网应进行安全隔离，民航单位内部网络应与机场、航空器等公共场所的旅客公共服务网络安全隔离。
d) 应根据承载业务的类型和重要性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；
e) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。
f) 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；
g) **应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

包括：

a) 应采用密码技术保证通信过程中数据的完整性；
b) 应采用密码技术保证通信过程中数据的保密性；
c) **应在通信前基于密码技术对通信的双方进行验证或认证；**
d) **应基于硬件密码模块对重要通信过程进行密码运算和密钥管理。**

8.1.2.3 可信验证

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

8.1.3 安全区域边界

8.1.3.1 边界防护

包括：

a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制；
c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制；
d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络；
e) **应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断；**
f) **应采用可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信。**

8.1.3.2 访问控制

包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
e) **应在网络边界通过通信协议转换或通信协议隔离等方式进行数据交换。**
f) 应在互联网出口和核心网络接口处限制网络最大流量数及网络连接数；
g) 重要网段应采取技术手段防止地址欺骗。

8.1.3.3 入侵防范

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，包括但不限于端口扫描、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、网络蠕虫攻击等；
b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为，包括但不限于端口扫描、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、网络蠕虫攻击等；
c) 采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

8.1.3.4 恶意代码和垃圾邮件防范

包括：

a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

8.1.3.5 安全审计

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。

8.1.3.6 可信验证

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

8.1.4 安全计算环境

8.1.4.1 身份鉴别

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，对于口令的具体要求如下：
   1) 长度不小于 8 位；
   2) 由大小写字母、数字和特殊字符组成；
   3) 不得与账户名相同；
   4) 不得明文存储；
   5) 至少每季度更换一次；
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，非法登录次数最多为 5 次，登录失败后锁定时间不少于 10 分钟，登录连接超时不得超过 10 分钟；
c) 当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

8.1.4.2 访问控制

包括：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
g) **应对主体、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

包括：

a) 应启用安全审计功能，审计覆盖到每个用户；系统不支持该要求的，应采用第三方安全审计产品实现审计要求；审计内容至少包括用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等重要的用户行为和安全事件；
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。

8.1.4.4 入侵防范

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) **应关闭或拆除主机的软盘驱动、光盘驱动、USB 接口、串行口等，确需保留的应严格管理；**
d) 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；
e) 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；
f) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞或采用其他有效方式进行安全防护；
g) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

8.1.4.5 恶意代码防范

包括：

a) **应采用主动免疫可信计算检验机制及时识别入侵和病毒行为，并将其有效阻断。**
b) 应支持防恶意代码的统一管理。

8.1.4.6 可信验证

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

8.1.4.7 数据完整性

包括：

a) 应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
b) 应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
c) **在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。**

8.1.4.8 数据保密性

包括：

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

8.1.4.9 数据备份恢复

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。**

8.1.4.10 剩余信息保护

包括：

a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

8.1.4.11 个人信息保护

包括：

a) 应仅采集和保存开展民航相关业务必需的旅客等用户的个人信息；
b) 应禁止未授权访问、非法使用和非法转移旅客等用户的个人信息。

8.1.5 安全管理中心

8.1.5.1 系统管理

包括：

a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

8.1.5.2 审计管理

包括：

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

b) 应通过安全审计员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等；
c) 应保证审计记录的留存时间符合法律法规要求，满足业务需要。

8.1.5.3 安全管理

包括：
a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

8.1.5.4 集中管控

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分析，对异常情况进行告警；
d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求，满足业务需要；
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；
g) **应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。**

8.1.6 安全管理制度

8.1.6.1 安全策略

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

8.1.6.2 管理制度

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，覆盖物理环境、通信网络、计算环境、数据、建设和运维等方面；
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网络安全管理制度体系。

8.1.6.3 制定和发布

包括：
a) 应指定或授权专门的部门或人员负责安全管理制度的制定；
b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。

8.1.6.4 评审和修订

应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。发生重大变更时，应及时对制度进行修订。

8.1.7 安全管理机构

8.1.7.1 岗位设置

包括：
a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；

b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
c) 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

8.1.7.2 人员配备

包括：
a) 应配备一定数量的系统管理员、审计管理员、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。**

8.1.7.3 经费保障

应保障网络和信息系统安全防护加固、安全运维、安全检查、安全测评、系统安全升级改造、网络安全教育培训、网络安全事件应急处置等网络安全方面的经费预算。

8.1.7.4 授权和审批

包括：
a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

8.1.7.5 沟通和合作

包括：
a) 应加强各类管理人员之间、组织内部机构之间以及网络安全管理部门内部的合作与沟通，领导班子主要负责人每年至少召集一次网络安全专题会议，网络安全主管领导至少每季度召集一次网络安全会议；
b) 应加强与民用航空监管机构、网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

8.1.7.6 审核和检查

包括：
a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

8.1.8 安全管理人员

8.1.8.1 人员录用

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，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，与系统管理员、审计管理员、安全管理员等关键岗位的人员签署岗位责任协议；
d) **应从内部人员中选拔从事系统管理员、审计管理员、安全管理员等关键岗位的人员。**

8.1.8.2 人员离岗

包括：

a) 应及时终止离岗员工的所有访问权限，收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。

8.1.8.3 安全意识教育和培训

包括：
a) 应对各类人员进行安全意识教育和岗位技能培训，并告知人员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，对网络安全基础知识、岗位操作规程等进行培训，在职人员年度人均接受培训时间不少于 4 个学时，网络安全关键岗位人员年度人均接受培训时间不少于 8 个学时，关键信息基础设施运营者的网络安全关键岗位人员年度人均接受培训时间不少于 24 个学时。
c) 应定期对不同岗位的人员进行技能考核；
d) 网络安全专业技术岗位人员中，获得网络安全专业资质人员占比达到 60%或虽未达到 60%但逐年提高。

8.1.8.4 外部人员访问管理

包括：
a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
c) 外部人员离场后应及时清除其所有的访问权限；
d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
e) **对关键区域或关键系统不允许外部人员访问。**

8.1.9 安全建设管理

8.1.9.1 定级和备案

包括：
a) 应依据 MH/T 0069，以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
a) 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；
b) 应保证定级结果经过相关部门的批准；
c) 应将备案材料报相应公安机关备案，并将备案结果报所在地民航行政管理机构。

8.1.9.2 安全方案设计

包括：
a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码相关内容，并形成配套文件；
c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施；涉及关键信息基础设施的，应报民航网络安全管理部门进行网络安全专项审查。

8.1.9.3 产品采购和使用

包括：
a) 应确保网络安全产品采购和使用符合国家的有关规定；
b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；
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。**

8.1.9.4 自行软件开发

包括：

a） 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
c） 应制定代码编写安全规范，要求开发人员参照规范编写代码；
d） 应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
e） 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
f） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
g） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

8.1.9.5 外包软件开发

包括：

a） 应在软件交付前检测其中可能存在的恶意代码；
b） 应保证开发单位提供软件设计文档和使用指南；
c） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

8.1.9.6 工程实施

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。

8.1.9.7 测试验收

包括：

a） 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
b） 应委托专业安全机构进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容；
c） 应确保系统通过安全性测试后才能接入互联网。

8.1.9.8 系统交付

包括：

a） 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
b） 应对负责运行维护的技术人员进行相应的技能培训；
c） 应提供建设过程文档和运行维护文档。

8.1.9.9 等级测评

包括：

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
b） 应在发生重大变更或级别发生变化时进行等级测评；
c） 应确保测评机构的选择符合国家有关规定。

8.1.9.10 服务供应商选择

包括：

a） 应确保服务供应商的选择符合国家和行业的有关规定；
b） 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
c） 应定期监视、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。

8.1.10 安全运维管理

8.1.10.1 环境管理

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，对机房设施定期巡检；
b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；
c) 应严格控制手机、便携式电脑等电子产品带入机房；
d) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等；
e) **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。**

8.1.10.2 资产管理

包括：
a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

8.1.10.3 介质管理

包括：
a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录；
c) 应对移动存储介质的安全使用作出规定，避免交叉混用，造成信息泄露和恶意代码传播。

8.1.10.4 设备维护管理

包括：
a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
c) 信息处理设备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，保证该设备上的敏感数据和授权软件无法被恢复重用。

8.1.10.5 漏洞和风险管理

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) 实施漏洞修补前，应对可能的风险进行评估和充分准备，做好数据备份和回退方案；
c) 漏洞修补后，应进行验证测试；
d) 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。

8.1.10.6 网络和系统安全管理

包括：
a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

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

8.1.10.7 恶意代码防范管理

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) 应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
d) 应定期验证防范恶意代码攻击的技术措施的有效性。

8.1.10.8 配置管理

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。

8.1.10.9 密码管理

包括：
a) 应遵循密码相关国家标准和行业标准；
b) 应使用国家密码管理主管部门认证核准的密码技术和产品；
c) **应采用硬件密码模块实现密码运算和密钥管理。**

8.1.10.10 变更管理

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。

8.1.10.11 备份与恢复管理

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。

8.1.10.12 安全事件处置

包括：
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；
b) 应根据行业有关规定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) 收到国家和行业有关部门发出的网络安全风险事件通报后，应及时排查处置并反馈处置情况；

e) 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；
f) **应建立联合防护和应急机制，负责处置跨单位安全事件。**

8.1.10.13 应急预案管理

包括：

a) 应按照民航网络安全事件应急预案，制定本单位网络安全专项应急预案，纳入本单位总体应急预案体系；
b) 应规定统一的应急预案框架，具体包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
c) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
d) 应对系统管理员、审计管理员、安全管理员、业务人员等相关人员进行应急预案培训，并进行应急预案的演练，上述培训和演练应每年至少开展一次；
e) 应定期对原有的应急预案重新评估，修订完善；
f) **应建立重大安全事件的跨单位联合应急预案，并进行应急预案的演练。**

8.1.10.14 外包运维管理

包括：

a) 应确保外包运维服务商的选择符合国家和行业的有关规定；
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) 选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

8.2 云计算安全扩展要求

应符合GB/T 22239—2019中9.2的要求。

8.3 移动互联安全扩展要求

应符合GB/T 22239—2019中9.3的要求。

8.4 物联网安全扩展要求

应符合GB/T 22239—2019的9.4的要求。

8.5 工业控制系统安全扩展要求

应符合GB/T 22239—2019的9.5的要求。

9 第五级安全要求

略。

附 录 A
（规范性附录）
关于安全通用要求和安全扩展要求的选择和使用

由于等级保护对象承载的业务不同，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。

不同级别的等级保护对象，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；即使相同级别的等级保护对象，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。

等级保护对象定级后，可能形成的定级结果组合见表A.1。

表A.1 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	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A4，S5A3，S5A2，S5A1

安全保护措施的选择应依据上述定级结果，本标准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）；其他安全保护类要求（简记为G）。本标准中所有安全管理要求和安全扩展要求均标注为G。安全要求及属性标识见表A.2。

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	安全物理环境	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

表 A.2 （续）

技术/管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	电磁防护	S
	安全通信网络	网络架构	G
		通信传输	G
		可信验证	S
	安全区域边界	边界防护	G
		访问控制	G
		入侵防范	G
		可信验证	S
		恶意代码防范	G
		安全审计	G
	安全计算环境	身份鉴别	S
		访问控制	S
		安全审计	G
		可信验证	S
		入侵防范	G
		恶意代码防范	G
		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
	安全管理中心	系统管理	G
		审计管理	G
		安全管理	G
		集中管控	G
安全管理要求	安全管理制度	安全策略	G
		管理制度	G
		制定和发布	G

表 A.2 （续）

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全管理制度	评审和修订	G
	安全管理机构	岗位设置	G
		人员配备	G
		经费保障	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G
	安全管理人员	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

表 A.2 （续）

技术/管理	分类	安全控制点	属性标识
安全管理要求	安全运维管理	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

对于确定了级别的等级保护对象，应依据表A.1的定级结果，结合表A.2使用安全要求，应按照以下过程进行安全要求的选择：

a) 根据等级保护对象的级别选择安全要求。方法是根据本标准，第一级选择第一级安全要求，第二级选择第二级安全要求，第三级选择第三级安全要求，第四级选择第四级安全要求，以此作为出发点。

b) 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级别的系统服务保证类（A 类）安全要求；根据业务信息安全性等级选择相应级别的业务信息安全类（S 类）安全要求；根据系统安全等级选择相应级别的安全通用要求（G 类）和安全扩展要求（G 类）。

c) 根据等级保护对象采用新技术和新应用的情况，选用相应级别的安全扩展要求作为补充。采用云计算技术的选用云计算安全扩展要求，采用移动互联技术的选用移动互联安全扩展要求，物联网选用物联网安全扩展要求，工业控制系统选用工业控制系统安全扩展要求。

d) 针对不同对象的特点，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其他标准的补充安全要求。对于本标准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。选用本标准中提供的安全技术要求和安全管理要求是保证等级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，从而实现等级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）
关于等级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。本标准第4章提出了不同级别的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的对象应该具有的安全保护能力提出了相应的安全通用要求和安全扩展要求，满足等级保护基本要求是保证等级保护对象具有相应级别的安全保护能力的前提。

依据本标准分层面采取各种安全措施时，还应考虑以下总体性要求，保证等级保护对象的整体安全保护能力：

a) 构建纵深的防御体系

本标准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，保证等级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标准中提到的各种安全措施，形成纵深防御体系；

b) 采取互补的安全措施

本标准以安全控制的形式提出安全要求，在将各种安全控制落实到特定等级保护对象中时，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等级保护对象上，使得等级保护对象的整体安全保护能力得以保证；

c) 保证一致的安全强度

本标准将安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到等级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。例如，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等级保护对象内部流动时标记的唯一性等；

d) 建立统一的支撑平台

本标准针对较高级别的等级保护对象，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，为了保证等级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；

e) 进行集中的安全管理

本标准针对较高级别的等级保护对象，提到了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，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

参 考 文 献

[1] 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

[2] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[3] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南

[4] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations