

YDB

中 国 通 信 标 准 化 协 会 标 准

YDB 110—2012

增值电信业务系统安全防护定级和评测 实施规范 邮件系统

Implementation Specification of Classified Security Protection and Testing for
Value-added Telecommunication Service System Mail System

2012 - 11 - 13 印发

中国通信标准化协会

目 次

前言.....	II
1 范围.....	1
2 规范性引用文件.....	1
3 术语、定义和缩略语.....	1
3.1 术语和定义.....	1
3.2 缩略语.....	2
4 概述.....	2
4.1 安全防护范围.....	2
4.2 安全风险分析.....	3
4.3 安全防护内容.....	5
5 邮件系统定级实施规范.....	6
5.1 安全等级划分.....	6
5.2 定级要素.....	7
5.3 安全等级的计算方法.....	8
6 安全防护要求.....	8
6.1 第1级要求.....	8
6.2 第2级要求.....	9
6.3 第3.1级要求.....	22
6.4 第3.2级要求.....	31
6.5 第4级要求.....	32
6.6 第5级要求.....	32
7 安全防护评测实施指南.....	32
7.1 第1级要求.....	32
7.2 第2级要求.....	32
7.3 第3.1级要求.....	49
7.4 第3.2级要求.....	63
7.5 第4级要求.....	63
7.6 第5级要求.....	63

YDB 110—2012

前 言

本标准是“增值电信业务系统安全防护定级和评测实施规范”系列实施规范之一，该系列实施规范包含如下实施规范：

- 增值电信业务系统安全防护定级和评测实施规范 门户综合网站系统；
- 增值电信业务系统安全防护定级和评测实施规范 即时通信系统；
- 增值电信业务系统安全防护定级和评测实施规范 网络交易系统；
- 增值电信业务系统安全防护定级和评测实施规范 信息社区服务系统；
- 增值电信业务系统安全防护定级和评测实施规范 邮件系统；
- 增值电信业务系统安全防护定级和评测实施规范 搜索系统；
- 增值电信业务系统安全防护定级和评测实施规范 互联网接入服务系统。

本标准按照GB/T1.1-2009给出的规则起草。

为适应信息通信业发展对通信标准文件的需要，由中国通信标准化协会组织制定“中国通信标准化协会标准”，推荐有关方面参考采用。有关对本标准的建议和意见，向中国通信标准化协会反映。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院。

本标准主要起草人：何友斌、黄晨、鲁冬雪、魏薇、邓东丰、封莎。

增值电信业务系统安全防护定级和评测实施规范 邮件系统

1 范围

本标准规定了邮件系统开展网络安全防护有关系统定级、分等级防护和安全评测等方面的规范性要求。

本标准适用于增值电信企业运营的邮件系统。

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，仅所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。

YD 5098- 2005 通信局(站)防雷与接地工程设计规范

YD 5002 邮电建筑防火设计标准

YD/T 5026- 2005 电信机房铁架安装设计标准

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

邮件系统安全等级 Security Classification of Mail System

邮件系统安全重要程度的表征。重要程度可从邮件系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、业务运营企业造成的损害来衡量。

3.1.2

邮件系统安全等级保护 Classified Security Protection of Mail System

对邮件系统分等级实施安全保护。

3.1.3

邮件系统安全风险 Security Risk of Mail System

人为或自然的威胁可能利用邮件系统中存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

邮件系统资产 Asset of Mail System

邮件系统中具有价值的资源，是安全防护保护的对象。邮件系统中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如邮件系统的主机、网络布局等。

3.1.5

YDB 110—2012

邮件系统威胁 Threat of Mail System

可能导致对邮件系统产生危害的不希望事件潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的邮件系统威胁有光缆中断、设备节点失效、火灾、水灾等等。

3.1.6

邮件系统脆弱性 Vulnerability of Mail System

脆弱性是邮件系统中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危及资产的安全。

3.1.7

邮件系统灾难 Disaster of Mail System

由于各种原因，造成邮件系统故障或瘫痪，使邮件系统支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.8

邮件系统灾准备份 Backup for Disaster Recovery of Mail System

为了邮件系统灾难恢复而对相关网络要素进行备份的过程。

3.1.9

邮件系统灾难恢复 Disaster Recovery of Mail System

为了将邮件系统从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.10

邮件系统安全评测 Security Testing of Mail System

对邮件系统的安全保护能力是否达到相应安全等级的安全防护要求进行衡量。

3.2 缩略语

下列缩略语适用于本标准。

DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
IMAP	Internet Mail Access Protocol	邮件访问协议
POP	Point Of Purchase	邮局协议
SMTP	Simple Mail Transfer Protocol	简单传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议

4 概述

4.1 安全防护范围

邮件系统是指通过互联网建立采用邮件简单传输协议(SMTP)、邮局协议(POP)、邮件访问协议(IMAP)等为用户提供一对一、一对多的邮件编辑、发送、传输、存储、转发、接收的电子信箱业务系统。它通过智能终端、计算机等与互联网结合，利用存储转发方式为用户提供多种类型的信息交换。

邮件系统整体架构包含以下几个关键模块：

- a) 注册登录模块：为新用户提供注册和已注册用户提供服务；
- b) 业务处理模块：为注册用户接收邮件、发送邮件的服务；
- c) 数据存储模块：为注册用户邮件数据存储服务；
- d) 业务安全管理模块：为注册用户恶意代码监控和过滤服务；
- e) 系统安全管理模块：设备配置管理和设备运行状态监控，确保系统运行稳定。

邮件系统功能架构如图1所示。

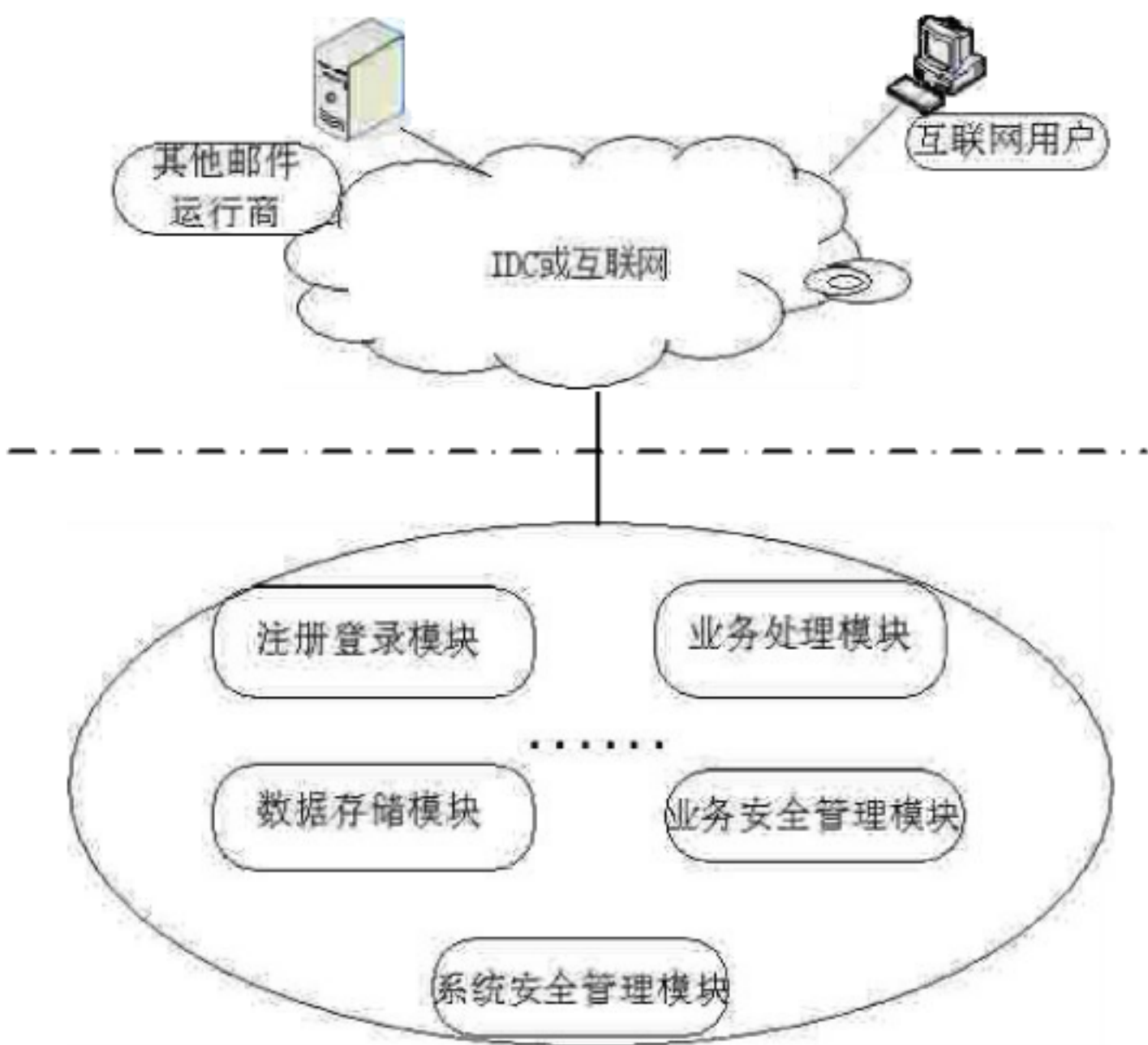


图1 邮件系统功能架构图

4.2 安全风险分析

邮件系统的重要资产至少应包括：

- a) 邮件系统及操作维护终端：如注册登录模块、业务处理模块、数据存储模块、业务安全管理模块及系统安全管理模块等涉及的服务器、数据库和操作维护终端；系统内部网络设备(如系统内部组网路由器、交换机等)、系统内部链路等；
- b) 邮件关键数据：如用户邮件注册信息(用户名、口令等)、用户邮件数据内容、邮件系统服务器的后台管理账户、口令等。

邮件系统相关代表性资产的类别划分如表1所示。

表1 资产类别

类别	主要资产
设备及链路	注册登录模块、发信/收信模块、数据存储模块等涉及的操作维护终端、服务器和数据库，系统内部网络设备（如系统内部组网路由器、交换机等）系统内部链路。
软件	数据库软件、中间件、业务控制和运维管理软件等
数据和信息	保证系统正常提供业务的数据和信息（如用户邮件注册信息、用户邮件数据内容、邮件系统服务器管理账户、口令等）
文档和资料	纸质以及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）。

YDB 110—2012

表 1 (续)

类别	主要资产
人员	相关管理、维护、开发、数据备份人员等。
环境和设施	业务系统和设备所处的物理环境 (如机房、电力、防火、防水、防静电、温湿度控制等相关设施)。

对于邮件系统而言，及时、准确的为用户提供邮件收发服务和用户数据保护服务尤为重要。因此，邮件系统如注册登录模块、业务处理模块、数据存储模块、业务安全管理模块及系统安全管理模块的功能实现、部署、配置、管理等环节对实现邮件系统功能起了直接决定性的作用。

邮件系统面临来自公众互联网和内部网络的各种安全威胁，其最突出安全风险是客户敏感数据信息泄露，包括：邮件内容泄露，邮箱登录用户名和口令被劫持；其次，含恶意代码的标题、正文、附件（图片、文档、视频、音频等）等被恶意传播。这些安全隐患会对邮件系统及时、准确地提供邮件收发服务构成威胁，甚至进一步威胁基础网络和互联网用户终端的安全。

邮件系统的脆弱性包括技术脆弱性和管理脆弱性两个方面，脆弱性识别对象应以资产为核心。邮件系统的脆弱性分析应包括但不限于表2所列范围。

表2 脆弱性类别

类别	对象	主要脆弱性
技术脆弱性	业务及应用	相关服务器未进行合理备份，重要数据未及时进行备份； 相关业务存在漏洞，相关服务器的应用代码存在漏洞、后门； 相关服务器存在过多不必要的开放端口； 相关服务器配置不合理，访问控制策略设置不合理； 相关服务器的日志功能没有启用或日志记录不完整； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷。
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关口令设置不合理、复杂度不够、或没有定期更新； 设备重要部件未进行合理冗余； 相关设备超过使用年限或核心部件老化； 相关设备发生故障后未及时告警。
	物理环境	机房场地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器、主机等设备的保护不符合规范。
管理脆弱性		安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； 安全管理制度方面：管理制度不完善、制度评审和修订不及时等； 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等； 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂家支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善。

邮件系统的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。邮件系统的威胁分析应包括但不限于表3所列范围。

表3 威胁类别

类别		主要威胁
环境威胁	物理环境	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等；意外事故或通讯线路方面的故障。
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击。
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏；攻击者利用非法手段进入机房内部盗窃、破坏、篡改源站内容，攻击者非法物理访问相关设备、存储介质等；攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源；攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据；攻击者利用应用系统扩散病毒、蠕虫，利用相关攻击工具恶意消耗应用系统资源（如DDoS攻击），导致系统能力下降或瘫痪、无法正常提供应用服务；攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失。
	非恶意人员	内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件；内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击；安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件；内部人员由于安全检查不及时不到位导致系统主机(如服务器、网络设备等)使用时间过长或质量问题等导致硬件故障，系统链路发生故障，相关设备的操作系统软件、应用软件运行故障，相关设备数据丢失或系统运行中断，存储介质老化或质量问题等导致不可用，系统不能正常运行。

4.3 安全防护内容

邮件系统的主要功能是为互联网用户提供邮件的写、发、收、存服务，因此保障其业务及应用系统安全运行，防止用户敏感数据泄露至关重要。保障邮件系统网络安全、设备及软件系统安全、管理安全等也是安全防护的主要内容。

4.3.1 业务及应用安全

业务及应用安全包括身份鉴别、访问控制、安全审计、数据安全、资源控制、信息保护、web安全防护、客户端安全、对外能力接口安全、恶意代码防范等方面安全要求。

4.3.2 网络安全

网络安全包括网络结构安全、入侵防范、安全审计等方面安全要求。

4.3.3 设备及软件系统安全

YDB 110—2012

设备及软件系统安全包括网络及安全设备、操作系统、数据库、中间件等方面安全要求。

4.3.4 物理环境安全

物理环境安全包括物理机房位置、机房访问控制等方面的安全要求。

4.3.5 管理安全

管理安全包括安全管理制度、机构、人员等方面的安全要求。

5 邮件系统定级实施规范

5.1 安全等级划分

邮件系统进行安全等级划分的总体原则是：依据定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益以及业务运营企业的合法权益的损害程度，对邮件系统进行安全等级划分，共分为5个等级。

5.1.1 第1级

定级对象受到破坏后，会对其业务运营企业的合法权益造成轻微损害，但不损害国家安全、社会秩序、经济运行和公共利益。

本级由业务运营企业依据国家和通信行业有关标准进行保护。

5.1.2 第2级

定级对象受到破坏后，会对业务运营企业的合法权益产生严重损害，或者对社会秩序、经济运行和公共利益造成轻微损害，但不损害国家安全。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行指导。

5.1.3 第3级

5.1.3.1 第3.1级

定级对象受到破坏后，会对业务运营企业的合法权益产生很严重损害，或者对社会秩序、经济运行和公共利益造成较大损害，或者对国家安全造成轻微损害。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行监督、检查。

5.1.3.2 第3.2级

定级对象受到破坏后，会对业务运营企业的合法权益产生特别严重损害，或者对社会秩序、经济运行和公共利益造成严重损害，或者对国家安全造成较大损害。

本级由业务运营企业依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行重点监督、检查。

5.1.4 第4级

定级对象受到破坏后，会对社会秩序、经济运行和公共利益造成特别严重损害，或者对国家安全造成严重损害。

本级由业务运营企业依据国家和通信行业有关标准以及业务的特殊安全要求进行保护,主管部门对其安全等级保护工作进行强制监督、检查。

5.1.5 第5级

定级对象受到破坏后,会对国家安全造成特别严重损害。

本级由业务运营企业依据国家和通信行业有关标准以及业务的特殊安全需求进行保护,主管部门对其安全等级保护工作进行专门监督、检查。

5.2 定级要素

确定定级对象的安全等级应根据如下三个相互独立的定级要素:社会影响力、规模和服务范围和所提供服务的的重要性。

5.2.1 社会影响力-I

定级对象的社会影响力表示其受到破坏后对国家安全、社会秩序、经济运行和公共利益的损害程度。对此定级要素进行赋值时,应先确定对国家安全、社会秩序、经济运行和公共利益的损害程度。定级对象的社会影响力赋值应是对国家安全、社会秩序、经济运行和公共利益的损害程度最严重者。

邮件系统主要为公众用户提供服务,邮件系统被损害后对国家安全不产生影响,对社会秩序、经济运行和公共利益造成轻微损害;邮件系统被破坏后对很多的用户造成影响。综合考虑,建议社会影响力赋值为2。

5.2.2 规模和服务范围-R

定级对象的规模表示其服务的用户数多少,服务范围表示其服务的地区范围大小。邮件可根据其业务特点确定所依据的指标,各指标数值的获取方式,由邮件运营企业提供。

邮件系统的定级对象的规模和服务范围R可根据如下指标确定:规模由其注册用户数(用R1来表示)、活跃用户数(用R2来表示)和人均单日有效浏览时间(用R3来表示)来表示。R取R1、R2和R3的最大值。定级对象的规模R1赋值如表4所示,R2赋值如表5所示,R3赋值如表6所示。

表4 注册用户数赋值表

注册用户数	赋值
注册用户数 1 亿及以下	1
注册用户数 1 亿以上, 3 亿及以下	2
注册用户数 3 亿以上, 5 亿及以下	3
注册用户数 5 亿以上, 10 亿及以下	4
注册用户数 10 亿及以上	5

表5 活跃用户数赋值表

月度覆盖人数	赋值
月度覆盖人数在 1000 万及以下	1
月度覆盖人数在 1000 万以上, 2000 万及以下	2
月度覆盖人数在 2000 万以上, 5000 万及以下	3
月度覆盖人数在 5000 万以上, 10000 万及以下	4
月度覆盖人数在 10000 万及以上	5

表6 人均单日有效浏览时间赋值表

人均单日有效浏览时间(分钟)	赋值
人均单日有效浏览时间在 10 及以下	1
人均单日有效浏览时间在 10 以上，20 及以下	2
人均单日有效浏览时间在 20 以上，50 及以下	3
人均单日有效浏览时间在 50 以上，100 及以下	4
人均单日有效浏览时间在 100 以上	5

5.2.3 所提供服务的的重要性- V

定级对象所提供服务的的重要性表示其提供的服务被破坏后对业务运营企业的合法权益的影响程度，此定级要素可通过定级对象所提供的服务本身的重要性来衡量，如业务的经济价值，业务重要性，对企业自身形象的影响等方面。

邮件系统所提供服务的的重要性一般，被破坏后对业务运营企业的合法权益造成较大损害，建议提供服务的重要性赋值为2。

在确定某一个定级要素的赋值时，无需考虑其他两个定级要素。

5.3 安全等级的计算方法

在完成定级对象的社会影响力I、规模和服务范围R、所提供服务的的重要性V三个定级要素的赋值后，需采用以下公式来计算定级对象的安全等级值：

$$k = \text{Round1}\{\text{Log}_2\{[a \times 2^I + \beta \times 2^R + \gamma \times 2^V]\}\} \dots\dots\dots (1)$$

其中，k代表安全等级值，I代表社会影响力赋值、R代表规模和服务范围赋值、V代表所提供服务的的重要性赋值，Round1{ }表示四舍五入处理，保留1位小数，Log₂[]表示取以2为底的对数，a、β、γ分别表示定级对象的社会影响力、规模和服务范围、所提供服务的的重要性赋值所占的权重，a=0，β=0，γ=0且a+β+γ=1。应根据实际情况确定权重值a、β、γ，建议分别取：1/3、1/3、1/3。

计算所得定级对象的安全等级值与安全等级的映射关系如表7所示。

表7 安全等级值与安全等级的映射关系

安全等级值 k	安全等级
1 ≤ k < 1.5	第 1 级
1.5 ≤ k < 2.5	第 2 级
2.5 ≤ k < 3.3	第 3.1 级
3.3 ≤ k ≤ 4	第 3.2 级
4 < k < 4.5	第 4 级
4.5 ≤ k ≤ 5	第 5 级

6 安全防护要求

6.1 第 1 级要求

6.1.1 业务及应用安全

不作要求。

6.1.2 网络安全

不作要求。

6.1.3 设备及软件系统安全

不作要求。

6.1.4 物理环境安全

不作要求。

6.1.5 管理安全

不作要求。

6.2 第2级要求

6.2.1 业务及应用安全

6.2.1.1 身份鉴别

身份鉴别要求如下：

- a) 邮件系统应提供专用的登录控制模块对登录系统的业务用户进行身份标识和鉴别；
- b) 邮件系统应提供并启用业务用户身份标识唯一性检查的功能，保证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。

6.2.1.2 访问控制

访问控制要求如下：

- a) 邮件系统应提供访问控制功能，依据安全策略控制业务用户、管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户；
- b) 邮件系统应提供并启用业务用户登录认证策略，如防范暴力破解、限定失败登录次数、锁定时间等。

6.2.1.3 安全审计

安全审计要求如下：

- a) 邮件系统应提供覆盖到系统每个业务用户帐号的安全审计功能，至少应能对业务用户关键操作、重要行为、业务资源使用情况、系统重要安全事件等进行审计；
- b) 邮件系统应保证无法删除、修改或覆盖审计记录；
- c) 邮件系统，审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

6.2.1.4 数据安全性

数据安全性要求如下：

- a) 邮件系统对业务用户登录应进行会话初始验证；
- b) 邮件系统应提供用户登陆认证过程数据加密传输功能；
- c) 邮件系统应对邮件内容进行数据保护，采取非明文存储方式；
- d) 邮件系统应防范和过滤垃圾邮件，保证用户邮件的正常使用；

- e) 邮件系统应对邮件发送者进行身份认证,应支持限制和禁止用户未知情情况下自动转发邮件的功能;
- f) 邮件系统应拒绝由未被允许的地址、用户名、子网域发起的邮件服务连接请求;
- g) 邮件系统应拒绝邮件转发次数超过预定上限的邮件的继续转发操作;
- h) 邮件系统应拒绝收信人数量超过预定上限的邮件的发送操作;
- i) 邮件系统应拒绝附件数量超过预定上限的邮件的发送操作;
- j) 邮件系统应拒绝邮件大小超过预定上限的邮件的发送操作;
- k) 邮件系统应对进入邮件服务器的邮件关键信息(如发送地址、接收地址、标题等)是否包含恶意链接及数据进行必要的检测。

6.2.1.5 资源控制

资源控制要求如下:

- a) 邮件系统中通信会话的一方在一段时间内未作任何响应,另一方应能够自动结束会话;
- b) 邮件系统应能够对单个业务用户的多重并发会话进行限制。

6.2.1.6 信息保护

信息保护要求如下:

- a) 邮件系统在获得用户数据信息时,应征得用户同意,并采取传输加密等措施保障相应数据的传输安全,防止传输过程中泄漏会话标识;
- b) 邮件系统发生用户信息泄漏,应依据与用户签订的合同协议对用户进行赔偿;
- c) 邮件系统应采取充分的安全保障措施保障用户数据信息的存储安全,并保障存储设备的安全;
- d) 邮件系统应妥善保存用户信息数据的纸质资料、电子介质等;
- e) 邮件系统在用户申请、审核及投诉处理过程中使用用户数据信息外,不得将用户数据信息用于任何其他用途;
- f) 邮件系统应采取加强对接触到用户数据信息人员的管理,严格控制接触用户信息的人员范围,合理设定用户信息操作权限,防止出现人为信息泄漏事件;
- g) 邮件系统应当明确告知用户收集和处理用户个人信息的方式、内容和用途以及信息泄漏风险,并向用户说明本系统要采取的信息保护措施,不得将用户提交的资料和信息泄露给他人,利用该信息牟利。在与用户签署的相关合同中,应明确规定运营企业对用户信息安全承担保护责任,写明采取的具体信息保护措施;
- h) 邮件系统应对信息安全防护工作进行定期检查或抽查,发现有违规行为时,可以依据相关协议等追究其责任。

6.2.1.7 Web 安全防护

Web安全防护要求如下:

- a) 邮件系统应对所有来源的输入进行验证,默认所有输入都可能包含恶意信息,只要其来源不在可信任的范围之内,就应对输入进行验证并尽量使用白名单验证方法;
- b) 邮件系统应设计一套统一的验证接口,向整个应用系统提供一致的验证方法,并降低开发与代码维护的工作量;
- c) 邮件系统应在服务器端进行输入验证,避免客户端输入验证被绕过;
- d) 邮件系统应对输入内容进行规范化处理后再进行验证,如文件路径、URL 地址等;
- e) 邮件系统应防止关键参数被篡改,关键参数应直接从服务器端提取,避免从客户端输入;

- f) 邮件系统应确保用户不能访问到未授权的功能和数据，未经授权的用户试图访问受限资源时，系统应予以拒绝或提示用户进行身份鉴权；
- g) 邮件系统应在服务器端实现对系统内受限资源的访问控制，避免客户端访问控制被绕过；
- h) 邮件系统应采用统一的访问控制机制，保证整体访问控制策略的一致性。同时应确保访问控制策略不被非法修改；
- i) 邮件系统应确保会话的安全创建，在用户认证成功后，应为用户创建新的会话并释放原有会话，创建的会话标识应满足随机性和长度要求，避免被攻击者猜测（如采用会话与IP地址绑定的方式），降低会话被盗用的风险；
- j) 邮件系统应确保会话数据的存储安全，用户登录成功后所生成的会话数据应存储在服务器端，并确保会话数据不能被非法访问，当更新会话数据时，要对数据进行严格的输入验证，以免会话数据的非法篡改；
- k) 邮件系统应确保会话数据的传输安全，防止泄露会话标识；
- l) 邮件系统应确保会话的安全终止，当用户登录成功并成功创建会话后，应在web应用系统的各个页面提供用户登出功能，登出时应及时删除服务器端的会话数据；当处于登录状态的用户直接关闭浏览器时，需要提示用户执行安全登出或者自动为用户完成登出过程，从而安全的终止本次会话；
- m) 邮件系统应设置合理的会话超时阈值，在合理范围内尽可能减小会话超时阈值，可以降低会话被劫持和重复攻击的风险，超过会话超时阈值后立刻销毁会话，清除会话的信息；
- n) 邮件系统应限制会话并发连接数，限制同一用户的会话并发连接数，避免恶意用户创建多个并发的会话来消耗系统资源，影响业务可用性；
- o) 邮件系统在涉及到关键业务操作的web页面，应为提供保障会话安全的补充机制（如以web页面一次性随机令牌的方式，作为主会话标识的补充）。

6.2.1.8 客户端安全

客户端安全要求如下：

- a) 邮件系统客户端应对输入数据做严格验证；
- b) 邮件系统客户端应确保身份认证模块不能被非法绕过；
- c) 邮件系统客户端软件运行时应自身进行完整性校验，及时有效的发现是否被恶意修改；
- d) 邮件系统客户端应采取会话保护措施防止软件与服务器之间的会话不可被篡改、伪造、重放等；
- e) 邮件系统客户端应确保软件配置信息、用户认证信息等敏感数据采用加密方式存储；
- f) 邮件系统客户端应确保软件内存管理不存在逻辑缺陷，如未释放资源、敏感信息驻留内存等；
- g) 邮件系统客户端应确保软件的用户身份鉴别模块能有效抵抗键盘记录等攻击；
- h) 邮件系统客户端应确保软件不非法操作与自身功能不相关的文件；
- i) 邮件系统客户端软件应具有异常处理功能。

6.2.1.9 对外能力接口安全

对外能力接口安全要求如下：

- a) 邮件系统应提供数据有效性检验功能，保证通过接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- b) 邮件系统接口均必须分别设置专门前置服务器，通过前置服务器的接口应用实现内外系统的交互；
- c) 邮件系统接口数据传输应尽量采用加密方式，原则上要求内外系统交互时，接口报文中的敏感信息应进行加密传输，如接口认证需要的密码等敏感数据；

- d) 邮件系统接口数据传输应进行校验，确保数据在传输过程中的完整性；
- e) 邮件系统接口认证信息必须以密文的形式单独存储在配置文件中；
- f) 邮件系统应对接口的状态和交互过程进行监控，并支持异常恢复。

6.2.1.10 恶意代码防范

恶意代码防范要求如下：

- a) 邮件系统应具备恶意代码过滤功能，应对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行恶意代码检查、屏蔽和删除，防止恶意代码通过业务网络向公众传播；
- b) 邮件系统应将被屏蔽的含有恶意代码相关信息的邮件结果告知邮件用户。

6.2.2 网络安全

6.2.2.1 网络结构安全

网络结构安全要求如下：

- a) 邮件系统应绘制与当前运行情况相符的系统拓扑结构图；
- b) 邮件系统应根据自身应用和服务的特点，在满足高峰期流量需求的基础上，合理设计带宽。

6.2.2.2 入侵防范

邮件系统应在系统边界部署访问控制设备，并启用有效的访问控制策略。

6.2.2.3 安全审计

安全审计要求如下：

- a) 邮件系统应对系统中的重要设备运行状况、网络流量监测信息、系统管理及维护等进行日志记录，并且保留一定期限（至少 180 天）；
- b) 邮件系统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。

6.2.3 设备及软件系统安全

6.2.3.1 网络及安全设备

网络及安全设备要求如下：

- a) 邮件系统各类路由器、交换机等网络设备应满足相关通信行业标准要求，具有进网许可证；
- b) 邮件系统应对登录网络设备（例如路由器、交换机）以及安全设备（例如入侵检测设备、防火墙设备）的用户进行有效的身份标识和鉴别；
- c) 邮件系统中网络及安全设备管理用户的标识应唯一；
- d) 邮件系统中网络及安全设备管理用户口令应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

6.2.3.2 通用主机操作系统

6.2.3.2.1 安全检测

安全检测要求如下：

- a) 应对邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；
- b) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统应遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式（如设置升级服务器）保持系统补丁及时得到更新；
- c) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统应定期进行安全监测，发现并加固操作系统相关漏洞，避免业已发现的漏洞造成安全事件。

6.2.3.2.2 身份鉴别

身份鉴别要求如下：

- a) 应对邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的用户进行身份标识和鉴别；
- b) 应对邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作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) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统的管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于 8 字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于 90 天）。

6.2.3.2.3 访问控制

访问控制要求如下：

- a) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应及时删除多余的、过期的账户，避免共享账户的存在；
- c) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应实现操作系统和数据库系统特权用户的权限分离；
- d) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

6.2.3.2.4 安全审计

安全审计要求如下：

- a) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的审计范围应覆盖到主机/服务器上的每个操作系统用户；
- b) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
- c) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的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；

6.2.3.2.5 恶意代码防范

恶意代码防范要求如下：

- a) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应安装防范病毒、木马等恶意代码的软件，并及时更新防恶意代码软件版本和恶意代码库；
- b) 邮件系统中各个功能模块的计算机运维终端、服务器等设备应支持防恶意代码的统一管理。

6.2.3.2.6 资源控制

资源控制要求如下：

- a) 邮件系统中各个功能模块的服务器应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；
- b) 邮件系统中各个功能模块的服务器应根据安全策略设置计算机运维终端的操作超时锁定；
- c) 邮件系统中各个功能模块的服务器应限制单个用户对主机资源的最大或最小使用限度；

6.2.3.2.7 冗余备份

邮件系统中各个功能模块的服务器应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护；

6.2.3.3 数据库及中间件软件

6.2.3.3.1 安全检测

安全检测要求如下：

- a) 应对邮件系统中各个功能模块的数据库及中间件软件进行必要的安全检测，出具安全测试及验收报告并妥善保存，相关设备的安全应满足相应设备技术规范、设备安全要求等行业标准的相关规定；
- b) 邮件系统中各个功能模块的数据库及中间件软件应遵循最小安装的原则，仅安装和开通需要的功能组件和应用程序，并通过安全方式（如设置升级服务器）保持系统补丁及时得到更新；
- c) 应对邮件系统中各个功能模块的数据库及中间件软件应定期进行安全监测，发现并加固操作系统相关漏洞，避免业已发现的漏洞造成安全事件。

6.2.3.3.2 身份鉴别

身份鉴别要求如下：

- a) 应对邮件系统中各个功能模块的数据库及中间件软件的用户进行身份标识和鉴别；
- b) 应对邮件系统中各个功能模块的数据库及中间件软件的不同用户分配不同的用户名，确保用户名具有唯一性；
- c) 应对邮件系统中各个功能模块的数据库及中间件软件的管理用户身份标识应具有不易被冒用的特点，相关用户口令长度应不小于8字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于90天）；

6.2.3.3.3 访问控制

访问控制要求如下：

- a) 邮件系统中各个功能模块的数据库及中间件软件应启用访问控制功能，依据安全策略控制用户对资源的访问；
- b) 邮件系统中各个功能模块的数据库及中间件软件应及时删除多余的、过期的账户，避免共享账户的存在；

- c) 邮件系统中各个功能模块的数据库及中间件软件应实现数据库、中间件特权用户与操作系统的权限分离；
- d) 邮件系统中各个功能模块的数据库及中间件软件应限制默认账户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

6.2.3.3.4 安全审计

安全审计要求如下：

- a) 邮件系统中各个功能模块的数据库及中间件软件的审计范围应覆盖到主机/服务器上的每个操作系统用户；
- b) 邮件系统中各个功能模块的数据库及中间件软件的审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
- c) 邮件系统中各个功能模块的数据库及中间件软件的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。

6.2.3.3.5 资源控制

资源控制要求如下：

- a) 邮件系统中各个功能模块的数据库及中间件软件应通过设定计算机运维终端接入方式、网络地址范围等条件限制管理终端登录；
- b) 邮件系统中各个功能模块的数据库及中间件软件应根据安全策略设置计算机运维终端的操作超时锁定；
- c) 邮件系统中各个功能模块的数据库及中间件软件应限制单个用户对主机资源的最大或最小使用限度。

6.2.3.3.6 冗余备份

邮件系统中各个功能模块的数据库及中间件软件应具备一定的冗余备份，关键设备、重要部件应采用冗余的方式提供保护。

6.2.4 物理环境安全

6.2.4.1 物理位置的选择

物理位置选择要求如下：

- a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
- b) 机房的承重能力应满足机房建筑要求。

6.2.4.2 物理访问控制

物理访问控制要求如下：

- a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员；
- b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

6.2.4.3 防盗窃和防破坏

防盗窃和防破坏要求如下：

- a) 应将主要设备放置在机房内；
- b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记；

- c) 应将室外通信线缆敷设在隐蔽处，可铺设在地下或管道中；
- d) 应对介质分类标识，存储在介质库或档案室中；
- e) 主机房应安装必要的防盗报警设施。

6.2.4.4 防雷击

防雷击要求如下：

- a) 机房建筑应设置避雷装置；
- b) 机房应设置交流电源地线；
- c) 应满足 YD 5098-2005 中相关要求。

6.2.4.5 防火

防火要求如下：

- a) 机房应设置灭火设备和火灾自动报警系统；
- b) 应满足 YD 5002 中相关要求。

6.2.4.6 防水和防潮

防水和防潮要求如下：

- a) 水管安装，不得穿过机房屋顶和活动地板下；
- 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。

6.2.4.7 防静电

关键设备应采用必要的接地防静电措施。

6.2.4.8 温湿度控制

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6.2.4.9 防尘

应采取必要的对机房的防尘措施，出入机房要求使用鞋套，有专人定期对机房进行除尘工作，有条件的设置防尘走廊。

6.2.4.10 电力供应

电力供应要求如下：

- 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，至少满足关键设备在断电情况下的正常运行要求。

6.2.4.11 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

6.2.5 管理安全

6.2.5.1 安全管理制度

6.2.5.1.1 管理制度

管理制度要求如下：

- a) 应制定安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
- b) 应对安全管理活动中重要的管理内容建立安全管理制度；
- c) 应对安全管理人员或操作人员执行的重要管理操作建立操作规程。

6.2.5.1.2 制定和发布

制定和发布要求如下：

- 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；
- c) 应将安全管理制度以某种方式发布到相关人员手中。

6.2.5.1.3 评审和修订

应定期对安全管理制度进行评审，对存在不足或需要改进的安全管理制度进行修订。

6.2.5.2 安全管理机构

6.2.5.2.1 岗位设置

岗位设置要求如下：

- a) 应设立安全主管以及安全管理各方面的负责人岗位，定义各负责人的职责；
- b) 应设立专职的网络安全技术人员，定义有关工作岗位的职责。

6.2.5.2.2 人员配备

应配备一定数量的网络安全管理和技术人员，能满足网络安全工作所需。

6.2.5.2.3 授权和审批

授权和审批要求如下：

- 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、割接、升级和重要资源的访问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。

6.2.5.2.4 沟通和合作

沟通和合作要求如下：

- a) 应加强企业内部人员（如管理人员、技术人员）及机构（如业务部门、安全管理职能部门）之间的合作与沟通；
- b) 应加强与相关外部单位的合作与沟通。

6.2.5.2.5 审核和检查

应由安全管理人员定期进行安全检查，检查内容包括用户帐号、系统漏洞、数据备份等情况。

6.2.5.3 人员安全管理

6.2.5.3.1 人员录用

人员录用要求如下：

- 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，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核；
- c) 应与从事关键岗位的人员签署保密协议。

6.2.5.3.2 人员离岗

人员离岗要求如下：

- a) 应规范人员离岗过程，及时终止离岗员工的所有访问权限；
- b) 对于离岗人员，应取回各种身份证件、钥匙等以及企业提供的软硬件设备；
- c) 对于离岗人员，应办理严格的调离手续。

6.2.5.3.3 人员考核

应定期对各个岗位的人员进行安全技能及安全认知的考核。

6.2.5.3.4 人员和技术支持能力要求

相关网络安全管理和技术人员应通过技能培训和考核。

6.2.5.3.5 安全意识教育和培训

安全意识教育和培训要求如下：

- a) 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；
- b) 应告知人员相关的安全责任和惩戒措施，并对违反违背安全策略和规定的人员进行惩戒；
- c) 应制定安全教育和培训计划，对网络安全基础知识、岗位操作规程等进行培训。

6.2.5.3.6 外部人员访问管理

应确保在外部人员访问受控区域前得到授权或审批，批准后由专人全程陪同或监督，并登记备案。

6.2.5.4 安全建设管理

6.2.5.4.1 定级

定级要求如下：

- a) 应明确网络的边界和安全保护等级；
- b) 应以书面的形式说明定级对象确定为某个安全等级的方法和理由；
- c) 应指定专门的人员或部门负责管理定级相关材料，并按主管部门要求及时上报、审批、备案。

6.2.5.4.2 安全方案设计

安全方案设计如下：

- a) 应根据网络的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) 应以书面形式描述对网络的安全保护要求、策略和措施等内容，形成网络的安全方案；
- 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安全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，并且经过批准后，才能正式实施。

6.2.5.4.3 产品采购和使用

产品采购和使用要求如下：

- a) 应确保安全产品采购和使用符合国家的有关规定；
- b) 应确保密码产品采购和使用符合国家密码主管部门的要求；
- c) 应指定或授权专门的部门负责产品的采购。

6.2.5.4.4 自行软件开发

自行软件开发要求如下：

- a) 应确保开发环境与实际运行环境物理分开；
- b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- 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。

6.2.5.4.5 外包软件开发

外包软件开发要求如下：

- a) 应根据开发需求检测软件质量；
- b) 应要求开发单位提供软件设计的相关文档和使用指南；
- c) 应在软件安装之前检测软件包中可能存在的恶意代码。

6.2.5.4.6 工程实施

工程实施要求如下：

- a) 应指定或授权专门的部门或人员负责工程实施过程的管理；
- b) 应制定详细的工程实施方案，控制工程实施过程。

6.2.5.4.7 测试验收

测试验收要求如下：

- 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覆盖网络安全要求的测试验收方案，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。

6.2.5.4.8 交付

交付要求如下：

- a) 应制定网络交付清单，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) 应对负责网络运行维护的技术人员进行相应的技能培训。

6.2.5.4.9 安全服务商的选择

安全服务商的选择要求如下：

- a) 应确保安全服务商的选择符合国家的有关规定；
- b) 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
- c) 应确保选定的安全服务商提供技术支持和服务承诺，必要时与其签订服务合同。

6.2.5.5 安全运维管理

6.2.5.5.1 运行维护能力

运行维护能力要求如下：

- a) 应具有完善运行维护管理制度，管理制度应涵盖业务管理和控制、系统运行、设备操作和维护等方面；
- b) 应按照统一的运行维护要求，对业务及应用系统进行规范化的维护。
- c) 应有业务及应用系统相关介质存取、验证和转储的管理制度，确保有关备份数据、信息的授权访问；
- d) 应保持与其他部门、外部单位间良好的联络和协作能力。

6.2.5.5.2 环境管理

环境管理要求如下：

- a) 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设备设施进行维护管理；
- b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
- c) 应建立机房安全管理制度，对有关机房物理区域访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
- d) 应加强对办公环境的保密性管理，包括工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等内容。

6.2.5.5.3 资产管理

资产管理要求如下：

- a) 应编制与网络相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
- b) 应建立资产安全管理制度，规定资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

6.2.5.5.4 介质管理

介质管理要求如下：

- a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；
- b) 应对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；
- c) 应对需要送出维修或销毁的介质，首先清除其中的敏感数据，防止信息的非法泄漏；
- d) 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管理。

6.2.5.5.5 设备管理

设备管理要求如下：

- a) 应对网络相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
- b) 应建立基于申报、审批和专人负责的设备安全管理制度，对各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；
- c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；
- d) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

6.2.5.5.6 网络安全管理

网络安全管理要求如下：

- a) 应指定人员对网络进行管理,负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作;
- b) 应建立网络安全管理制度,对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面做出规定;

6.2.5.5.7 恶意代码防范管理

恶意代码防范管理要求如下:

- a) 应提高所有人员的恶意代码防范意识,明确移动介质使用、从外部网络接收文件外来设备接入等环节的恶意代码安全检测要求;
- b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录;
- c) 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等做出明确规定。

6.2.5.5.8 密码管理

应使用符合国家密码管理规定的密码技术和产品。

6.2.5.5.9 变更管理

变更管理要求如下:

- a) 应确认网络中要发生重要变更的行为,并制定相应的变更方案;
- b) 网络发生重要变更前,应向主管领导申请,审批后方可实施变更,并在实施后向相关人员通告。

6.2.5.5.10 备份与恢复管理

备份与恢复管理要求如下:

- 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(如增量备份或全备份等)、备份频度(如每日或每周等)、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。

6.2.5.5.11 安全事件处置

安全事件处理要求如下:

- a) 应报告所发现的安全弱点和可疑事件,但任何情况下均不应在生产网络中尝试验证弱点;
- b) 应制定安全事件报告和处置管理制度,明确安全事件类型,规定安全事件的现场处理、事件报告和后期恢复的管理职责;
- c) 应根据安全事件对本网络产生的影响,对本网络安全事件进行等级划分;
- d) 应记录并保存所有发现的安全弱点和可疑事件,分析事件原因,监督事态发展,采取措施避免安全事件发生。

6.2.5.5.12 应急预案管理

应急预案管理要求如下:

- a) 应在统一的应急预案框架下制定不同事件的应急预案,应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容;
- b) 应对相关的人员进行应急预案培训,应急预案的培训应至少每年举办一次。

6.3 第3.1级要求

6.3.1 业务及应用安全

6.3.1.1 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 邮件系统应提供并启用用户身份标识唯一性检查的功能，保证系统中不存在重复用户身份标识；
- b) 邮件系统应提供并启用用户登录认证口令复杂度强度功能，保证业务用户的口令长度不小于8字节，口令应有复杂度要求（使用大写字母、小写字母、数字、标点及特殊字符五种字符中至少二种的组合，且与用户名或身份标识无相关性）并定期更换（更新周期不大于90天）。

6.3.1.2 访问控制

除满足第2级的要求之外，还应满足：

- a) 邮件系统应严格设置业务用户解锁策略，按安全策略要求，被锁定的业务用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定；
- b) 邮件系统应在屏蔽带病毒网页后，为用户发送消息提示。

6.3.1.3 安全审计

除满足第2级的要求之外，还应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

6.3.1.4 数据安全性

除满足第2级的要求之外，还应满足：

- a) 邮件系统应保证采用足够强壮的加密算法保证用户登录认证过程数据不被非授权利用和篡改；
- b) 邮件系统应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据符合系统设定要求，确保非常规数据被过滤；
- c) 邮件系统应对邮件内容进行数据保护，采取非明文存储方式，确保加密或者编码算法不易被破解；
- d) 邮件系统，应能按一定的规则和方式（如黑名单、白名单）对匹配的邮件进行过滤和拦截，并向用户通知有关处理结果。

6.3.1.5 资源控制

除满足第2级的要求之外，还应对通过该平台对外发布的公共信息使用自动程序过滤和人工检查结合的方式进行有害数据检查、屏蔽和删除，防止有害数据通过业务网络向公众传播。

6.3.1.6 信息保护

除满足第2级的要求之外，还应保护系统服务相关信息的安全，避免有关数据被篡改和破坏。

6.3.1.7 Web安全防护

除满足第2级的要求之外，还应在web程序上线前或升级后应进行代码审计，形成报告，并对审计出的问题进行代码升级完善。

6.3.1.8 客户端安全

除满足第2级的要求之外，还应避免使用含有已公开漏洞的开源第三方应用组件及代码（漏洞库可参考CVE、CNC等）。

6.3.1.9 对外能力接口安全

同第2级要求。

6.3.1.10 恶意代码防范

除满足第2级的要求之外，还应禁止不必要的内嵌网络服务，应禁止在用户端自动安装恶意软件和插件。

6.3.2 网络安全

6.3.2.1 网络结构安全

除满足第2级的要求之外，还应满足：

- a) 邮件系统应根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署；
- b) 不考虑主动宕机维护的情况，邮件系统年宕机时间不超过 4.38 小时，可靠性应达到 99.9% 以上；
- c) 邮件系统应具备必要的流量负荷分担设计。

6.3.2.2 入侵防范

除满足第2级的要求之外，还应在系统边界处对发生的网络入侵行为（包括但不限于端口扫描、强力攻击、木马后门攻击、DoS/DDoS攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击）提供有效的检测能力，当检测到入侵行为时应能记录攻击源IP、攻击类型、攻击目的、攻击时间。

6.3.2.3 安全审计

除满足第2级的要求之外，还应满足：

- a) 邮件系统应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；
- b) 邮件系统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；
- c) 邮件系统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隔离手段；
- d) 邮件系统应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

6.3.3 设备及软件操作系统安全

6.3.3.1 网络及安全设备

除满足第2级的要求之外，还应满足：

- a) 邮件系统网络及安全设备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；
- b) 邮件系统网络及安全设备应通过设定终端接入方式、网络地址范围等条件限制管理终端登录；
- c) 邮件系统网络及安全设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

6.3.3.2 通用主机操作系统

6.3.3.2.1 安全检测

同第2级要求。

6.3.3.2.2 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 邮件系统中各个功能模块的计算机运维终端、服务器等设备的主机操作系统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；
- b) 邮件系统中各个功能模块的计算机运维终端、服务器等设备进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

6.3.3.2.3 访问控制

同第2级要求。

6.3.3.2.4 安全审计

除满足第2级的要求之外，还应满足邮件系统中各个功能模块的计算机运维终端、服务器等设备的审计记录，避免其受到未预期的删除、修改或覆盖等，保留一定期限（至少180天）。

6.3.3.2.5 恶意代码防范

同第2级要求。

6.3.3.2.6 资源控制

除满足第2级的要求之外，还应满足：

- a) 邮件系统应对能够对各模块的服务器进行性能和服务水平监控，监控方式可基于监听、SNMP等网管技术和协议；并设定阈值，在监测到服务水平降低到阈值时进行报警；
- b) 邮件系统中各个功能模块的服务器应保持时间上的同步。

6.3.3.2.7 冗余备份

除满足第2级的要求之外，还应满足：

- a) 邮件系统中各个功能模块的服务器应建立对主机关键数据（如主机配置数据、管理员操作维护记录、用户信息等）和重要信息进行备份和恢复的管理和控制机制；
- b) 邮件系统中相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

6.3.3.3 数据库及中间件软件

6.3.3.3.1 安全检测

同第2级要求。

6.3.3.3.2 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 应对邮件系统中各个功能模块的数据库及中间件软件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;
- b) 应对邮件系统中各个功能模块的数据库及中间件软件进行远程管理时,应采取必要措施,防止鉴别信息在传输过程中被窃听。

6.3.3.3.3 访问控制

同第2级要求。

6.3.3.3.4 安全审计

除满足第2级的要求之外,还应满足邮件系统中各个功能模块的数据库及中间件软件的审计记录,避免其受到未预期的删除、修改或覆盖等,保留一定期限(至少180天)。

6.3.3.3.5 资源控制

除满足第2级的要求之外,还应满足:

- a) 邮件系统中各个功能模块的数据库及中间件软件行性能和服务水平监控,监控方式可基于监听、SNMP等网管技术和协议;并设定阈值,在监测到服务水平降低到阈值时进行报警;
- b) 邮件系统中各个功能模块的数据库及中间件软件应保持时间上的同步。

6.3.3.3.6 冗余备份

除满足第2级的要求之外,还应满足:

- a) 邮件系统中各个功能模块的数据库及中间件软件应建立对主机关键数据(如主机配置数据、管理员操作维护记录、用户信息等)和重要信息进行备份和恢复的管理和控制机制;
- b) 邮件系统中各个功能模块的数据库及中间件软件中相关数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

6.3.4 物理环境安全要求

6.3.4.1 物理位置的选择

除满足第2级的要求之外,还应满足:

- a) 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;
- b) 如果机房有铁架,机房铁架安装应满足 YD/T 5026-2005 要求。

6.3.4.2 物理访问控制

除满足第2级的要求之外,还应满足:

- a) 应对机房划分区域进行管理,区域和区域之间设置物理隔离装置,在重要区域前设置交付或安装等过渡区域;
- b) 重要区域应配置电子门禁系统,控制、鉴别和记录进入的人员。

6.3.4.3 防盗窃和防破坏

除满足第2级的要求之外,还应满足:

- a) 应利用光、电等技术设置机房防盗报警系统;
- b) 应对机房设置监控报警系统。

6.3.4.4 防雷击

除满足第2级的要求之外，还应设置防雷保安器，防止感应雷。

6.3.4.5 防火

除满足第2级的要求之外，还应满足：

- 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) 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

6.3.4.6 防水和防潮

除满足第2级的要求之外，还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。

6.3.4.7 防静电

除满足第2级的要求之外，还应满足：

- a) 主要设备应采用必要的接地防静电措施；
- b) 机房应采用防静电地板。

6.3.4.8 温湿度控制

同第2级要求。

6.3.4.9 防尘

同第2级要求。

6.3.4.10 电力供应

除满足第2级的要求之外，还应满足：

- a) 应设置冗余或并行的电力电缆线路为系统供电；
- b) 应建立备用供电系统。

6.3.4.11 电磁防护

除满足第2级的要求之外，还应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

6.3.4.12 防鼠

信息服务业务系统所处机房应具备防虫防鼠等相关措施，以有效防范鼠虫蚁害。

6.3.5 管理安全要求

6.3.5.1 安全管理制度

6.3.5.1.1 管理制度

除满足第2级的要求之外，还应满足：

- a) 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动；
- b) 应形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。

6.3.5.1.2 制定和发布

除满足第2级的要求之外，还应满足：

- a) 安全管理制度应有统一的格式，并进行版本控制；
- b) 安全管理制度应通过正式、有效的方式发布；
- c) 安全管理制度应注明发布范围，并对收发文进行登记。

6.3.5.1.3 评审和修订

除满足第2级的要求之外，还应满足：

- a) 安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
- b) 应定期或不定期对安全管理制度进行检查和审定。

6.3.5.2 安全管理机构

6.3.5.2.1 岗位设置

除满足第2级的要求之外，还应满足：

- a) 应设立安全管理工作的职能部门；
- b) 应成立指导和管理安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；
- c) 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。

6.3.5.2.2 人员配备

除满足第2级的要求之外，还应满足：

- a) 应配备专职安全管理员，不可兼任；
- b) 关键事务岗位应配备多人共同管理。

6.3.5.2.3 授权和审批

除满足第2级的要求之外，还应满足：

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

6.3.5.2.4 沟通和合作

除满足第2级的要求之外，还应满足：

- a) 各类管理人员之间、组织内部机构之间以及网络安全职能部门内部定期或不定期召开协调会议，共同协作处理网络安全问题；
- b) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- c) 应聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等。

6.3.5.2.5 审核和检查

除满足第2级的要求之外，还应满足：

- a) 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；

- b) 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；
- c) 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，定期按照程序进行安全审核和安全检查活动。

6.3.5.3 人员安全管理

6.3.5.3.1 人员录用

除满足第2级的要求之外，还应满足：

- a) 应严格规范人员录用过程，对被录用人的资质等进行审查；
- b) 应签署保密协议；
- c) 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。

6.3.5.3.2 人员离岗

除满足第2级的要求之外，还应满足关键岗位人员离岗须承诺调离后的保密义务后方可离开。

6.3.5.3.3 人员考核

除满足第2级的要求之外，还应满足：

- a) 应对关键岗位的人员进行全面、严格的安全审查和技能考核；
- b) 应对考核结果进行记录并保存。

6.3.5.3.4 人员和技术支持能力

同第2级要求。

6.3.5.3.5 安全意识教育和培训

除满足第2级的要求之外，还应满足：

- a) 应对安全责任和惩戒措施进行书面规定；
- b) 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划；
- 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。

6.3.5.3.6 外部人员访问管理

除满足第2级的要求之外，还应满足：

- a) 应确保在外部人员访问受控区域前先提出书面申请；
- b) 对外部人员允许访问的区域、网络、设备、信息等内容应进行书面的规定，并按照规定执行。

6.3.5.4 安全建设管理

6.3.5.4.1 定级

除满足第2级的要求之外，还应满足：

- a) 应组织相关部门和有关安全技术专家对网络定级结果的合理性和正确性进行论证和审定；
- b) 应将网络的定级结果分级上报至全国或地区的主管部门，主管部门对定级结果审批。

6.3.5.4.2 安全方案设计

除满足第2级的要求之外，还应满足：

- a) 应指定和授权专门的部门对网络的安全建设进行总体规划,制定近期和远期的安全建设工作计划;
- b) 应根据网络的等级划分情况,统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案,并形成配套文件;
- c) 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定,并且经过批准后,才能正式实施;
- d) 应根据等级评测、安全评估的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、详细设计方案等相关配套文件。

6.3.5.4.3 产品采购和使用

除满足第2级的要求之外,还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。

6.3.5.4.4 自行软件开发

除满足第2级的要求之外,还应满足:

- a) 应确保开发人员和测试人员分离,测试数据和测试结果受到控制;
- b) 应制定代码编写安全规范,要求开发人员参照规范编写代码;
- c) 应确保对程序资源库的修改、更新、发布进行授权和批准。

6.3.5.4.5 外包软件开发

同第2级要求。

6.3.5.4.6 工程实施

除满足第2级的要求之外,还应满足:

- a) 要求工程实施单位能正确地执行安全工程过程;
- b) 应制定工程实施方面的管理制度,明确说明实施过程的控制方法和人员行为准则。

6.3.5.4.7 测试验收

除满足第2级的要求之外,还应满足:

- a) 应对系统测试验收的控制方法和人员行为准则进行书面规定;
- b) 应指定或授权专门的部门负责系统测试验收的管理,并按照管理规定的要求完成系统测试验收工作。

6.3.5.4.8 交付

除满足第2级的要求之外,还应满足:

- a) 应对网络交付的控制方法和人员行为准则进行书面规定;
- b) 应指定或授权专门的部门负责网络交付的管理工作,并按照管理规定的要求完成交付工作;
- c) 在网络正式投入使用前,应根据实际情况进行试运行,试运行期间应提供相关应急预防措施;
- d) 在网络正式投入使用后,应对开发、建设过程中涉及安全要求的配置、口令等内容重新修改、设定。

6.3.5.4.9 安全服务商的选择

同第2级要求。

6.3.5.4.10 等级评测

等级评测要求如下：

- a) 在网络运行过程中，应至少每年对网络进行一次等级评测，发现不符合相应等级保护标准要求的及时整改；
- b) 应在网络发生变更时及时对网络进行等级评测，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
- c) 应选择具有国家相关技术资质和安全资质的评测单位进行等级评测；
- d) 应指定或授权专门的部门或人员负责等级评测的管理。

6.3.5.5 安全运维管理

6.3.5.5.1 环境管理

除满足第2级的要求之外，还应满足：

- a) 应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理。
- b) 工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸质文件。

6.3.5.5.2 资产管理

除满足第2级的要求之外，还应满足：

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

6.3.5.5.3 介质管理

除满足第2级的要求之外，还应满足：

- a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面做出规定；
- b) 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；
- c) 应对存储介质的使用过程进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准不得自行销毁；
- d) 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；
- e) 应对重要介质中的数据和软件采取加密存储。

6.3.5.5.4 设备管理

除满足第2级的要求之外，还应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。

6.3.5.5.5 网络安全管理

同第2级要求。

6.3.5.5.6 系统安全管理

除满足第2级的要求之外，还应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

6.3.5.5.7 恶意代码防范

除满足第2级的要求之外，还应定期检查网络内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

6.3.5.5.8 密码管理

除满足第2级的要求之外，还应建立密码使用管理制度。

6.3.5.5.9 变更管理

除满足第2级的要求之外，还应满足：

- a) 应建立变更管理制度，变更和变更方案需有评审过程；
- b) 应建立变更申报和变更审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；
- c) 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

6.3.5.5.10 备份与恢复管理

除满足第2级的要求之外，还应满足：

- a) 应建立备份与恢复管理相关的安全管理制度；
- b) 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；
- c) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

6.3.5.5.11 安全事件处置

除满足第2级的要求之外，还应满足：

- a) 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；
- b) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；
- c) 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。

6.3.5.5.12 应急预案管理

除满足第2级的要求之外，还应满足：

- a) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；
- b) 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；
- c) 应规定应急预案需要定期审查和根据实际情况更新等内容，并按照执行。

6.4 第3.2级要求

同第2级要求。

6.5 第4级要求

同第2级要求。

6.6 第5级要求

待补充。

7 安全防护评测实施指南

7.1 第1级要求

7.1.1 业务及应用安全

不作要求。

7.1.2 网络安全

不作要求。

7.1.3 设备及软件系统安全

不作要求。

7.1.4 物理环境安全

不作要求。

7.1.5 管理安全

不作要求。

7.2 第2级要求

7.2.1 业务及应用安全检测要求

7.2.1.1 身份鉴别

身份鉴别要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供专用的登录控制模块对登录系统的业务用户进行身份标识和鉴别；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供并启用业务用户身份标识唯一检查功能，保证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。

7.2.1.2 访问控制

访问控制要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供访问控制功能，是否依据安全策略控制业务用户、管理用户对系统文件、数据库表等客体的访问，控制粒度为单个用户；

- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供并启用业务用户登录认证策略，如防范暴力破解、限定失败登录次数、锁定时间等。

7.2.1.3 安全审计

安全审计要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供覆盖到系统每个业务用户帐号的安全审计功能，至少应能对业务用户关键操作、重要行为、业务资源使用情况、系统重要安全事件等进行审计；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否保证无法删除、修改或覆盖审计记录；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统审计记录的内容是否至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

7.2.1.4 数据安全性

数据安全性要求如下：

- a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统业务用户登录是否进行会话初始验证；
- b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否提供用户登录认证过程数据加密传输功能；
- c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否对邮件内容进行数据保护，采取非明文存储方式；
- d) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否能够防范和过滤垃圾邮件，保证用户邮件的正常使用；
- e) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否对邮件发送者进行身份认证，应支持限制和禁止自动转发邮件的功能；
- f) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否拒绝由未被允许的地址、用户名、子网域发起的邮件服务连接请求；
- g) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否拒绝邮件转发次数超过预定上限的邮件的继续转发操作；
- h) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否拒绝收信人数量超过预定上限的邮件的发送操作；
- i) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否拒绝附件数量超过预定上限的邮件的发送操作；
- j) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否拒绝邮件大小超过预定上限的邮件的发送操作；
- k) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查邮件系统是否对进入邮件服务器的邮件相关的关键信息（如发送地址、接收地址、标题、内容、附件等）是否包含恶意链接及数据进行必要的检测。

7.2.1.5 资源控制

资源控制要求如下：