

YDB

中国通信标准化协会标准

YDB 106—2012

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

Implementation Specification of Classified Security Protection and
Testing for Value-added Telecommunication Service System
Portal Site 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.....	3
4.2 安全风险分析.....	3
4.3 安全防护内容.....	5
5 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.....	20
6.4 第3.2级要求.....	30
6.5 第4级要求.....	30
6.6 第5级要求.....	30
7 安全防护评测实施指南.....	30
7.1 第1级要求.....	30
7.2 第2级要求.....	30
7.3 第3.1级要求.....	48
7.4 第3.2级要求.....	61
7.5 第4级要求.....	61
7.6 第5级要求.....	61

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：封莎、魏薇、谢玮、魏亮、鲁冬雪、黄晨、祝卓、杨剑锋、邓东丰、许子先、何有斌。

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

1 范围

本标准规定了门户综合网站系统安全防护定级实施规范、安全防护要求和安全防护评测实施指南。
本标准适用于增值电信企业运营的门户综合网站系统。

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- 2005	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

下列术语和定义适用于本标准。

3.1.1

门户综合网站系统安全等级 security classification of portal site system

门户综合网站系统安全重要程度的表征。重要程度可从门户综合网站系统受到破坏后，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

门户综合网站系统安全等级保护 classified security protection of portal site system

对门户综合网站系统分等级实施安全保护。

3.1.3

门户综合网站系统安全风险 security risk of portal site system

人为或自然的威胁可能利用门户综合网站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

门户综合网站系统资产 asset of portal site system

门户综合网站系统中具有价值的资源，是安全防护保护的对象。门户综合网站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，如网站业务系统的主机、网络布局等。

YDB 106—2012

3. 1. 5

门户综合网站系统威胁 threat of portal site system

可能导致对门户综合网站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。常见的门户综合网站系统络威胁有光缆中断、设备节点失效、火灾、水灾等等。

3. 1. 6

门户综合网站系统脆弱性 vulnerability of portal site system

脆弱性是门户综合网站系统中存在的弱点、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

门户综合网站系统灾难 disaster of portal site system

由于各种原因，造成门户综合网站系统故障或瘫痪，使门户综合网站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

门户综合网站系统灾准备份 backup for disaster recovery of portal site system

为了门户综合网站系统灾难恢复而对相关网络要素进行备份的过程。

3. 1. 9

门户综合网站系统灾难恢复 disaster recovery of portal site system

为了将门户综合网站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

门户综合网站系统安全评测 security testing of portal site system

对门户综合网站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。

CVE	Common Vulnerabilities & Exposures	通用漏洞披露
CVNC	China National Vulnerability Database	国家信息安全漏洞共享平台
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transport Protocol	超文本传送协议
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	安全超文本传输协议
IP	Internet Protocol	网际协议
SSL	Secure Sockets Layer	安全套阶层协议
TLS	Transport Layer Security	安全传输层协议
UPS	Uninterruptible Power System	不间断电源

4 概述

4.1 安全防护范围

门户综合网站系统是由计算机及其相关的配套设备、设施、软件构成信息发布平台，按照一定规则对公共互联网用户提供互联网新闻门户服务的信息服务系统，公共互联网用户通过网络可以以查询、浏览等方式获取通过信息发布平台发布的信息。

门户综合网站系统平台提供新闻门户服务，其他业务能力主要通过接口调用其他业务平台业务能力实现，系统功能架构如图1所示。

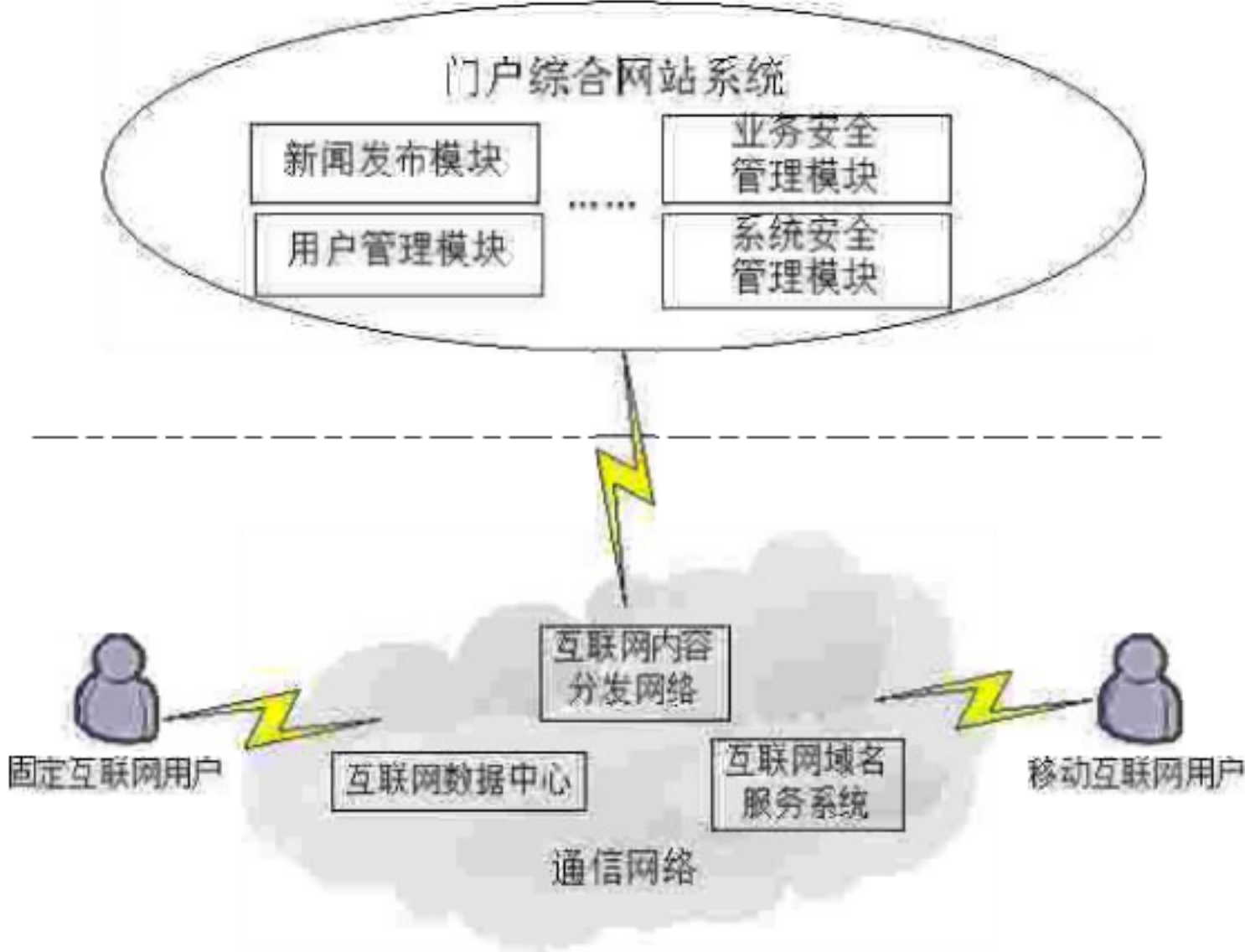


图1 门户综合网站系统功能架构图

门户综合网站系统各模块功能如下：

- a) 用户管理模块主要包括用户注册、认证、权限等子模块，主要是实现用户的注册、登录认证以及用户权限鉴别及管理；
- b) 新闻发布模块主要实现新闻的审核、发布、撤销等功能；
- c) 业务安全管理模块主要包括恶意代码监控和过滤、防篡改和防挂马等模块，主要实现对新闻发布数据中的恶意代码进行扫描，及时有效的发现恶意篡改和挂马等安全问题；
- d) 系统安全管理模块主要包括设备配置管理和设备运行状态监控，主要实现对网络、安全、主机设备的安全配置管理及日常运行状态监控，及时有效的发现系统运行异常，确保系统运行稳定。

本标准主要针对门户综合网站系统平台及其接口提出安全防护要求和检测实施指南，与门户综合网站系统相关的其他业务平台安全防护要求和检测实施指南不属于本标准规定范畴，可参见其他相应增值电信业务实施规范。例如为门户综合网站系统提供域名解析服务的系统、与互联网相关的互联网数据中心、互联网内容分发网络等其他系统的安全防护要求参见相应网络类型的安全防护标准。

4.2 安全风险分析

门户综合网站系统中的重要资产至少应包括：设备硬件，设备软件，重要数据，提供的应用，文档人员等。门户综合网站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	涉及的操作维护终端、服务器和数据库，相关辅助设备（如，安全过滤、入侵检测和防护设备），系统内部网络设备（如，系统内部组网路由器、交换机等设备），系统内部链路。

表 1 (续)

类别	主要资产
软件	相关业务或应用软件、数据库软件、业务控制和运维管理软件等。
数据和信息	保证信息服务业务正常提供的数据和信息（如，业务数据、系统配置数据、管理员操作维护记录、用户信息等）。
业务及应用	门户综合网站系统提供的信息浏览和发布服务。
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）。
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，机房、电力、防火、防水、防静电、温湿度控制等相关设施。

门户综合网站系统的脆弱性可以从技术脆弱性和管理脆弱性两个方面考虑。脆弱性识别对象应以资产为核心。门户综合网站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/应用协议存在漏洞，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不够详细； 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、或没有经常更新； 设备重要部件未进行合理备份； 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。

门户综合网站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它物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。门户综合网站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
技术威胁		相关主机和服务、及系统网络设备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。
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、破坏等，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、木马、垃圾电子邮件，利用相关攻击工具恶意消耗应用系统资源，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而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。

门户综合网站系统可能存在的安全脆弱性被利用后会产生很大的安全风险，主要包括以下几个方面：

- 来自内部和外部可能的网络攻击，如 DDOS 攻击、利用系统漏洞进行的各类攻击；
- 网页被篡改或被挂马，成为木马大范围传播的主要途径；
- 相关主机和服务、及系统网络设备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。

这些安全隐患会对门户综合网站系统的业务正常提供构成安全威胁，甚至进一步威胁互联网用户终端的安全。

4.3 安全防护内容

门户综合网站系统的主要功能是进行新闻发布，为用户提供新闻浏览功能，因此保障业务的安全稳定运行至关重要。保障门户综合网站系统的物理环境安全、管理安全等也是安全防护的主要内容。

YDB 106—2012

4.3.1 业务及应用安全

业务及应用安全包括向用户提供的相关业务及应用在实现技术、逻辑、管理和控制等方面的安全要求，主要包括业务逻辑安全、web安全、客户端安全等。

4.3.2 网络安全

网络安全包括网络结构安全、入侵防范、安全审计等方面的安全要求。

4.3.3 设备及软件系统安全

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、中间件在身份鉴别、访问控制、安全审计、入侵防范、资源控制等方面的安全要求。

4.3.4 物理安全

物理安全包括系统所处的物理环境在机房位置、电力供应、防火、防水、防静电、温湿度控制等方面的安全要求。

4.3.5 管理安全

管理安全包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全要求。

5 定级实施规范

5.1 安全等级划分

门户综合网站业务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，对增值电信业务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损害程度，再确定对社会秩序、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。

门户综合网站系统的服务对象范围广泛，数量众多，受到破坏后会对社会秩序、经济运行和公共利益造成较为严重的损害，建议社会影响力赋值为3。

5.2.2 规模和服务范围- R

新闻发布业务的定级对象的规模和服务范围R可根据如下指标确定：规模由日均访问用户数（用R1来表示）和人均页面访问量（用R2来表示）来表示。R取R1和R2中的较大值。定级对象的规模R1赋值如表4所示，R2赋值如表5所示。

表4 规模 R1 赋值表

规模指标	赋值
日均访问用户数在1000万及以下	1
日均访问用户数在1000万以上，1500万及以下	2
日均访问用户数在1500万以上，3000万及以下	3
日均访问用户数在3000万以上，5000万及以下	4
日均访问用户数在5000万以上	5

表5 规模 R2 赋值表

规模指标	赋值
人均页面访问量在10次及以下	1
人均页面访问量在10次以上，20次及以下	2
人均页面访问量在20次以上，50次及以下	3
人均页面访问量在50次以上，100次及以下	4
人均页面访问量在100次以上	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。

门户综合网站系统所提供服务的的重要性一般，被破坏后会对业务运营企业的合法权益造成较大损害，建议所提供服务的的重要性赋值为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：0.4、0.4、0.2，或者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6所示。

表6 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 业务逻辑安全

6.2.1.1.1 身份鉴别

提供用户登录功能的系统应使用专门的登录控制模块对登录用户进行身份标识和鉴别。

应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用。

应采用加密方式存储业务用户的帐号和口令信息。

6.2.1.1.2 访问控制

严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力。如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的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。

6.2.1.1.3 安全审计

审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改帐号信息等行为，以及管理员在业务功能及帐号控制方面的关键操作。

应保护审计记录，保证无法删除、修改或覆盖等。

业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等。

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。

6.2.1.1.4 资源控制

当用户和业务系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。

6.2.1.1.5 信息保护

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。

业务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，并保障存储系统的安全，防止存储过程中泄漏。

应妥善保存存储有用户信息数据的纸质资料、电子介质等。

采取措施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。

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。

关键设备具备一定的灾准备份和恢复的能力,重要部件应采用冗余的方式提供保护。

建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制。

关键数据(如业务数据、应用配置数据、管理员操作维护记录、用户信息等)应有必要的容灾备份。

6.2.1.1.6 恶意代码防范

采用技术或人工手段防止网页被篡改和被挂马。

建立防篡改和防挂马监测及举报受理机制,及时发现问题,一旦发现被篡改或挂马,应能在特定时间内(3小时)反应并处置。

如采用互联网内容分发网络(CDN),如发现网页被篡改或挂马,应要求CDN运营企业在合同约定时间内清除相关数据。

6.2.1.1.7 网站外链控制

通过中转页面形式提供网站外链跳转功能,且中转页面应有显性的免责声明。

确保网站外链不会发生二次对外链接的情况下,方可准予嵌入。

6.2.1.2 Web 安全

6.2.1.2.1 输入验证

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。

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。在服务器端进行输入验证,避免客户端输入验证被绕过。

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。

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。

6.2.1.2.2 身份认证

禁止明文传输用户密码,建议采用SSL加密隧道确保用户密码的传输安全。

禁止在数据库或文件系统中明文存储用户密码,建议采用单向散列值在数据库中存储用户密码,在生成单向散列值过程中加入随机盐值,降低存储的用户密码被字典攻击的风险。

禁止在COOKIE中保存用户密码。

采用图形验证码来增强身份认证安全,防止恶意脚本自动发送身份认证请求来猜测用户认证鉴权性质的信息。要求图形验证码能够抵抗工具的自动识别。

对关键业务操作,例如修改用户认证鉴权信息(如密码、密码取回问题及答案、绑定手机号码等)需要经过二次鉴权,以避免因用户身份被冒用,给用户造成损失。

避免认证错误提示泄露信息,在认证失败时,应向用户提供通用的错误提示信息,不应区分是帐号错误还是密码错误,避免这些错误提示信息被攻击者利用。

支持密码策略设置,从业务系统层面支持强制的密码策略,包括密码长度、复杂度、更换周期等,特别是业务系统的管理员密码。

支持帐号锁定功能，系统应限制连续登录失败次数，在客户端多次尝试失败后，服务器端需要对用户帐号进行短时锁定，且锁定策略支持配置解锁时长。

6.2.1.2.3 访问控制

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。

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。

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。

6.2.1.2.4 会话管理

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。建议会话与IP地址绑定，降低会话被盗用的风险。

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。

确保会话数据的传输安全，防止泄露会话标识。

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。

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。

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。

在涉及到关键业务操作的web页面，应为当前web页面生成一次性随机令牌，作为主会话标识的补充。在执行关键业务前，应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配，以避免跨站请求伪造等攻击。

6.2.1.2.5 数据存储

对于不同安全级别的数据，比如日志记录和业务数据，应采取相应的隔离措施和安全保护措施。

尽量避免存储用户敏感数据，禁止在本地存储用户敏感数据，如用户密码、身份信息等。

避免在代码中硬编码密码，在代码中硬编码密码，即在代码中直接嵌入密码，会导致密码修改困难甚至密码的泄露，建议从配置文件载入密码。

在配置文件中禁止明文存储数据库连接密码、FTP服务密码、主机密码、外部系统接口认证密码等。

6.2.1.2.6 数据传输

应确保敏感信息通信信道的安全，建议在客户端与web服务器之间使用SSL。并正确配置SSL，建议使用SSL 3.0/ TLS 1.0以上版本，对称加密密钥长度不少于128位，非对称加密密钥长度不少于1024位单向散列值位数不小于128位。

6.2.1.2.7 日志记录

日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改帐号信息等行为，以及管理员在业务功能及帐号控制方面的关键操作。

禁止在日志中记录用户密码等敏感信息，如果确实需要记录敏感信息，则应进行模糊化处理。

防止日志欺骗，如果在生成日志时需要引入来自非受信源的数据，则需要进行严格校验，防止日志欺骗攻击。

禁止将日志保存到web目录下，确保日志数据的安全存储并严格限制日志数据的访问权限，建议对日志记录进行签名来实现防篡改。

6.2.1.3 客户端安全

对输入数据做严格验证，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。

确保身份认证模块不能被非法绕过。

软件运行时应对自身进行完整性校验，及时有效的发现是否被恶意修改。

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。

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。

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。

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。

确保软件不非法操作与自身功能不相关的文件。

软件应具有异常处理功能，防止由于软件运行异常导致业务流程中断。

6.2.2 网络安全

6.2.2.1 结构安全

应绘制与当前运行情况相符的系统拓扑结构图。

在满足高峰期流量需求的基础上，合理设计带宽。

应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。

不考虑主动宕机维护的情况，系统年宕机时间不超过8.76小时，可靠性应达到99.9%以上。

6.2.2.2 入侵防范

应在系统边界处监视以下攻击行为：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等。

应在系统边界处部署防火墙等安全防御设备或技术措施，有效抵御和防范各种攻击。

6.2.2.3 安全审计

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）。

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。

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。

6.2.3 设备及软件系统安全

6.2.3.1 网络及安全设备

各类路由器、交换机、宽带接入服务器等网络设备应满足相关行业标准要求，具有进网许可证。

对登录业务平台网络设备（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。

用户的标识应唯一。

用户口令应不小于6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IC无相关性）并定期更换（更新周期不大于90天）。

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。

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。

当对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。

保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

网络设备的重要部件应采用冗余的方式提供保护。

关键网络设备、重要线路应采用冗余的保护方式。

相关网络关键数据（如网络设备配置数据、网络安全设备配置数据、网络管理员操作维护记录等）应有必要的容灾备份。

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。

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。

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。

定期自检（漏洞扫描、弱口令扫描、基线配置信息等），对主机的端口、弱口令、安全漏洞进行扫描和发现，对已知业务应用漏洞进行扫描和发现，对已知木马进行扫描和发现，对扫描结果进行分析和提交，促进业务安全管理与安全问题的解决。

6.2.3.2 操作系统

6.2.3.2.1 身份鉴别

对登录操作系统的用户进行身份标识和鉴别。

应为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。

操作系统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IC无相关性）并定期更换（更新周期不大于90天）。

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。

当对各类主机进行远程管理时，应采取必要措施，防止鉴别信息在传输过程中被窃听。

6.2.3.2.2 访问控制

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。

及时删除多余的、过期的帐户，避免共享帐户的存在。

实现操作系统和数据库系统特权用户的权限分离。

限制默认帐户的访问权限，修改这些账户的默认口令，条件允许下，应重命名默认账户。

6.2.3.2.3 安全审计

审计范围应覆盖到主机/服务器上的每个操作系统用户和数据库用户。

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。

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。

应保护审计记录，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）。

6.2.3.2.4 入侵防范

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，并通过安全的方式（如，设置升级服务器）保持系统补丁及时得到更新。

6.2.3.2.5 恶意代码防范

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。
支持防恶意代码的统一管理。

6.2.3.2.6 资源控制

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。
根据安全策略设置登录终端的操作超时锁定。
限制单个用户对系统资源的最大或最小使用限度。

6.2.3.2.7 其他

关键主机设备具备一定的灾准备份和恢复的能力，关键设备、重要部件应采用冗余的方式提供保护。
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。

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。

6.2.3.3 数据库

6.2.3.3.1 身份鉴别

应按照用户分配帐号，避免不同用户间共享帐号。
删除与数据库运行、维护等工作无关的帐号。
在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
使用数据库角色来管理对象的权限。

应确保数据库管理员帐号、远程连接帐号口令长度应不小于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ID无相关性）并定期更换（更新周期不大于90天）。

6.2.3.3.2 安全审计

数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐号、登录是否成功、登录时间。

数据库应配置日志功能，记录与数据库相关的安全事件。

6.2.3.3.3 其他安全

数据库应停用不必要的存储过程。
数据库与调用程序之间应使用加密协议通讯。
应确保数据库软件及时升级补丁。

6.2.3.4 中间件

6.2.3.4.1 身份鉴别

实现操作系统和中间件用户的权限分离，中间件应使用独立用户。
应实现中间件用户和应用程序用户的权限分离。

6.2.3.4.2 访问控制

如果中间件启用了SSL，应采用不低于3.0版本的SSL。
中间件使用的操作系统级别的服务用户的权限应遵循最小权限原则。

6.2.3.4.3 安全审计

采用技术手段（如定期运行文件完整性监控软件）及时发现中间件关键系统数据或文件是否被非授权更改并通知相关人员，应至少每周对关键文件进行比较。
应定期（至少每月一次）对中间件安全日志进行审计。

6.2.3.4.4 入侵防范

中间件的安装应遵循最小安装的原则。应关闭或限制与系统正常运行无关，但可能造成安全隐患的默认扩展功能，例如示例程序、后台管理、不必要的存储过程等。

应禁用中间件的目录列出功能。

在进行协议级的配置时应禁用中间件不必要的HTTP方法，例如PUT、TRACE、DELETE等，若启用了HTTPS则应禁用HTTP。

应启用必要的语言安全设置，例如PHP语言设置，JAVA语言设置。

对安装时自动生成的帐号（如：演示帐号）须做清理或者修改密码。

配置HTTP服务标识（Service Banner），使其不泄露Web服务器以及操作系统的版本。

6.2.4 物理安全

6.2.4.1 物理位置的选择

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。

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

机房出入口应安排专人值守，控制、鉴别和记录进入的人员。

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

主要设备放置在机房内。

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。

将室外通信线缆敷设在隐蔽处，可铺设在地下或管道中。

应对介质分类标识，存储在介质库或档案室中。

主机房应安装必要的防盗报警设施。

6.2.4.4 防雷击

机房建筑应设置避雷装置。

机房应设置交流电源地线。

应满足YD 5098-2005中相关要求。

6.2.4.5 防火

机房应设置灭火设备和火灾自动报警系统。

6.2.4.6 防水和防潮

水管安装，不得穿过机房屋顶和活动地板下。

采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

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

应在机房供电线路上配置稳压器和过电压防护设备。

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

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。

对安全管理活动中重要的管理内容建立安全管理制度。

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

指定或授权专门的部门或人员负责安全管理制度的制定。

应组织相关人员对制定的安全管理制度进行论证和审定。

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

设立安全主管、安全管理各个方面的负责人岗位，定义各负责人的职责。

设立专职的网络安全技术人员岗位，定义有关工作岗位的职责。

6.2.5.2.2 人员配备

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

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、升级和重要资源访问等关键活动进行审批。

6.2.5.2.4 沟通和合作

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。

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

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

指定或授权专门的部门或人员负责人员录用。

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。

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

应规范人员离岗过程，及时终止离岗员工的所有访问权限。

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。

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

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

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

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。

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。

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

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

明确网络的边界和安全保护等级。

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。

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

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。

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。

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。

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

确保安全产品采购和使用符合国家的有关规定。

确保密码产品采购和使用符合国家密码主管部门的要求。

指定或授权专门的部门负责产品的采购。

自行软件开发应确保开发环境与实际运行环境物理分开。

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。

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。

6.2.5.4.4 外包软件开发

根据开发需求检测软件质量。

应要求开发单位提供软件设计的相关文档和使用指南。

应在软件安装之前检测软件包中可能存在的恶意代码。

6.2.5.4.5 工程实施

指定或授权专门的部门或人员负责工程实施过程的管理。

制定详细的工程实施方案，控制工程实施过程。

6.2.5.4.6 测试验收

对系统进行安全性测试验收。

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。

6.2.5.4.7 交付

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。

对负责网络运行维护的技术人员进行相应的技能培训。

6.2.5.4.8 安全服务商的选择

应确保安全服务商的选择符合国家的有关规定。

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。

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 运行维护管理能力要求

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。

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。

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。

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

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。

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。

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。

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

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。

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

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。

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。

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。

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

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。

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。

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。

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

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。

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作出规定。

6.2.5.5.7 恶意代码防范管理

应提高所有人员的恶意代码防范意识，明确移动存储介质使用、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。

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。

对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定。

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

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。

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

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。

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。

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

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尝试在生产网络中验证弱点。

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。

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。

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。

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 业务逻辑安全

除满足第2级的要求之外，还应满足：

- a) 能根据需要对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护（如进行通信数据加密），并提供业务及应用相关访问、通信等数据的防抵赖功能；

- b) 定义业务水平阈值,能够对业务及应用服务水平进行检测,并具备当服务水平降低到预先规定的阈值时进行告警的功能;
- c) 对业务用户访问和操作的有关环节(如,注册、登录、操作、管理、浏览等)提供有效的保护措施(如,用户注册口令进行强度检查、用户ID检测和帐号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等);
- d) 提供有效的恶意代码检测和过滤技术手段,对业务平台向用户提供的各类信息进行必要的安全检查和过滤;
- e) 重要设备应采用热备份的保护方式进行保护;
- f) 业务及应用应具备必要的流量负荷分担设计;
- g) 业务及应用应具备较好的灾难备份和业务恢复的能力,提供重要服务的业务及应用系统应进行系统级备份,以保证其业务连续性;
- h) 建立对业务及应用全部数据、信息进行备份和恢复的管理和控制机制;
- i) 重要的业务及应用相关数据应进行异地备份;
- j) 应提供数据自动保护功能,当发生故障后应保证系统能够恢复到故障前的业务状态;
- k) 用两种或两种以上组合的鉴别技术实现用户身份鉴别;
- l) 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;
- m) 登录验证模块应能防止身份鉴别暴力攻击。(如登录模块随机验证码验证、并且保证验证码不易被自动预测、识别);
- n) 加强口令复杂度要求,在原基础上还应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合;
- o) 重要服务器用使用资源强制访问控制策略。(如用户、进程、文件内核级保护);
- p) 业务系统管理后台不应暴露给任意用户;管理接口通信内容不应使用明文协议;
- q) 保证系统中使用的第三方软件、运维软件无已知后门、漏洞;
- r) 应拒绝由未被允许的地址、子网域发起的请求(如浏览、发布、评论等),应拒绝以未经授权的方式访问服务器上有限公开的相关内容和资源;
- s) 应建立防篡改和防挂马监测及举报受理机制,及时发现问题,一旦发现被篡改或挂马,应能在特定时间内(1小时)反应并处置。

6.3.1.2 Web 安全

除满足第2级的要求之外,还应满足:

- a) 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;
- b) 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、CNVD等)。

6.3.1.3 客户端安全

除满足第2级的要求之外,还应满足:

- a) 客户端软件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;
- b) 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、CNVD等)。

6.3.2 网络安全

6.3.2.1 结构安全

除满足第2级的要求之外,还应满足:

- a) 避免将重要设备部署在网络边界处且直接连接外部网络/系统，重要网段与其他网段之间采取可靠的技术隔离手段；
- b) 系统应具有过负荷保护功能，确保系统在过负荷时，重要业务能正常运行；
- c) 不考虑主动宕机维护的情况，系统年宕机时间不超过 4.38 小时，可靠性应达到 99.95% 以上；
- d) 具备必要的流量负荷分担设计；
- e) 保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

6.3.2.2 入侵防范

除满足第2级的要求之外，还应满足当检测到入侵行为时，应记录攻击源IP、攻击类型、攻击目的地址、攻击时间，在发生严重入侵事件时应提供报警。

6.3.2.3 安全审计

除满足第2级的要求之外，还应满足：

- a) 能根据记录数据进行分析，并生成审计报告；
- b) 保护审计记录，保证无法删除、修改或覆盖等。

6.3.3 设备及软件系统安全

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) 重要设备、线路应采用热备份的保护方式进行保护；
- b) 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) 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) 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；
- e) 定期自检(漏洞扫描、弱口令扫描、基线配置信息等)；
- f) 加强口令复杂度要求，在原基础上还应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合；
- g) 应能采取有效手段(如，IP地址与mac地址绑定等)防止地址欺骗及嗅探攻击；
- h) 网络能有效防止非法接入。

6.3.3.2 操作系统

6.3.3.2.1 身份鉴别

除满足第2级的要求之外，还应满足：

- a) 应采用两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴别；
- b) 重要主机应使用安全性较高的身份鉴别措施(如，数字证书等)对用户进行身份鉴别。

6.3.3.2.2 访问控制

除满足第2级的要求之外，还应满足：

- a) 应根据最小权限分配原则，按设备相关各类管理、维护帐号的角色分配权限，实现管理帐号与操作、维护帐号的权限分离；

- b) 应对重要信息资源设置敏感标记；
- c) 应依据安全策略严格控制有关用户对有敏感标记重要信息资源的操作。

6.3.3.2.3 安全审计

除满足第2级的要求之外，还应满足：

- a) 应能根据记录数据进行分析，并生成审计报表；
- b) 应保护审计进程，避免受到未预期的中断。

6.3.3.2.4 入侵防范

除满足第2级的要求之外，还应满足：

- a) 应对重要服务器进行入侵行为的监测，能够记录入侵的源IP、攻击的类型、攻击的目的地址、攻击的时间，并在发生严重入侵事件时提供告警；
- b) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

6.3.3.2.5 恶意代码防范

除满足第2级的要求之外，还应满足主机防恶意代码产品应使用与网络/系统防恶意代码产品不同的恶意代码库。

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) 应对重要服务器进行性能监测，包括监测服务器的CPU、硬盘、内存、网络等资源的使用情况；
- b) 应能够对服务器、数据库等系统的服务水平设定告警阈值，当监测到服务水平降低到阈值时应能进行告警。

6.3.3.2.7 其他

重要设备应采用热备份的保护方式进行保护。

系统应有必要的流量负荷分担设计。

系统应具备较好的灾后备份和业务恢复的能力，提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。

应建立对主机全部数据、信息进行备份和恢复的管理和控制机制。

重要的主机相关数据应进行异地备份。

应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。

登录验证模块应能防止身份鉴别暴力攻击（如，使用随机验证码验证并保证验证码不易被自动预测、识别）。

加强口令复杂度要求，在原基础上还应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合。

重要服务器用使用资源强制访问控制策略。（如用户、进程、文件内核级保护）。

6.3.3.3 数据库

同第2级要求。

6.3.3.4 中间件

同第2级要求。

6.3.4 物理安全

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 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。

6.3.4.9 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。

6.3.4.10 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

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 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。

6.3.5.4.6 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。

6.3.5.4.7 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。

6.3.5.4.8 安全服务商的选择

同第2级要求。

6.3.5.4.9 等级评测

除满足第2级的要求之外，还应满足：

- 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，如变化较为频繁应至多每半年进行等级评测，发现级别发生变化时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档文件。

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作出规定，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、维护和销毁等方面作出规定；
- 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 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。

6.3.5.5.7 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。

6.3.5.5.8 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。

6.3.5.5.9 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。

6.3.5.5.10 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。

6.3.5.5.11 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3.1级要求。

6.5 第4级要求

同第3.2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

7.2.1.1 业务逻辑安全

7.2.1.1.1 身份鉴别

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，检查验证系统是否提供了专门的登录控制模块对登录用户进行身份标识和鉴别。

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，检查用户身份鉴别信息复杂度检查功能、技术手段及有关措施启用、实施情况，检查或测试验证是否能保证系统中身份鉴别信息不易被冒用。

访谈相关技术和管理人员，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，检查是否采用加密方式存储系统业务用户的帐号和口令。

7.2.1.1.2 访问控制

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，检查或测试验证是否严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

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，检查或测试验证是否严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力。如限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的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。

7.2.1.1.3 安全审计

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，对审计功能和审计记录进行测试，验证审计范围是否覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、异常修改帐号信息等，管理员的业务功能及帐号控制方面的关键操作。

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，对审计功能和审计记录进行测试，验证是否保证无法删除、修改或覆盖审计记录。

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、相关审计记录，访谈审计相关工作流程、审计文件及结果记录要求，检查验证业务相关审计记录的内容是否至少包括事件日期、时间、发起者信息、类型、描述和结果等。

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，对审计功能和审计记录进行测试，验证是否对审计记录数据进行统计、查询、分析及生成审计报表。

7.2.1.1.4 资源控制

应访谈相关技术人员，检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档，检查或测试验证系统能否在用户和业务系统通信双方中的一方在一段时间内未作任何响应时，自动结束会话。

7.2.1.1.5 信息保护

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证在获得用户数据信息时，是否征得用户同意，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。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证业务系统是否采取充分的安全保障措施保障用户数据信息的存储安全，并保障存储系统的安全，防止存储过程中泄漏。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证是否妥善保存存储有用户信息数据的纸质资料、电子介质等。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证是否采取措施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。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证是否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，是否将用户提交的资料和信息泄露给他人。

访谈相关技术人员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其它文档，检查验证系统是否具备一定的灾备份和恢复的能力，检查验证关键设备、重要线路是否采用冗余的保护方式。

访谈相关技术人员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其它文档，检查验证是否建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制。

访谈相关技术人员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其它文档，检查验证相关业务及应用的关键数据（如业务数据、计费数据、系统配置数据、管理员操作维护记录、用户信息等）是否有必要的容灾备份。

7.2.1.1.6 恶意代码防范

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，检查验证门户综合网站系统是否采用技术或人工手段防止网页被篡改和被挂马。

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，检查验证门户综合网站系统是否建立防篡改和防挂马监督举报机制，及时发现问题，一旦发现被篡改或挂马，是否能在特定时间内（3小时）反应并处置。

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，检查验证门户综合网站系统如采用互联网内容分发网络（CDN），是否参照互联网内容分发网络安全防护定级和评测实施规范。

7.2.1.1.7 网站外链控制

访谈相关技术人员，并检查业务设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其它文档，检查验证是否通过中转页面形式提供网站外链跳转功能，且中转页面应有显性的免责声明。

访谈相关技术人员，并检查业务设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其它文档，是否采取有效手段确保网站外链不会发生二次对外链接的情况下，才准予嵌入，并使用二次外链的链接进行嵌入测试，以验证该防护手段的有效性。

7.2.1.2 Web 安全

7.2.1.2.1 输入验证

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证系统是否对所有来源的输入进行验证并使用白名单验证方法，并使用渗透测试工具进行扫描验证。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证系统是否具备统一的验证接口，向整个应用系统提供一致的验证方法，并使用渗透测试工具进行扫描验证。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证系统是否在服务器端进行输入验证，并使用渗透测试工具进行扫描验证，并使用渗透测试工具进行扫描验证。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证系统是否对输入内容进行规范化处理后再进行验证，并使用渗透测试工具进行扫描验证。

访谈相关技术人员，并检查业务设计/验收文档、系统安全策略、业务运营商提供的其它文档，检查验证系统是否采用有效手段防止关键参数被篡改，并通过修改数据包，并使用渗透测试工具进行扫描验证。

7.2.1.2.2 身份认证

