ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22239—2019
代替 GB/T 22239—2008

信息安全技术
网络安全等级保护基本要求

Information security technology—
Baseline for classified protection of cybersecurity

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》，与 GB/T 22239—2008 相比，主要变化如下：

——将标准名称变更为《信息安全技术　网络安全等级保护基本要求》；

——调整分类为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理；

——调整各个级别的安全要求为安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求和工业控制系统安全扩展要求；

——取消了原来安全控制点的 S、A、G 标注，增加一个附录 A 描述等级保护对象的定级结果和安全要求之间的关系，说明如何根据定级结果选择安全要求；

——调整了原来附录 A 和附录 B 的顺序，增加了附录 C 描述网络安全等级保护总体框架，并提出关键技术使用要求。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：公安部第三研究所(公安部信息安全等级保护评估中心)、国家能源局信息中心、阿里云计算有限公司、中国科学院信息工程研究所(信息安全国家重点实验室)、新华三技术有限公司、华为技术有限公司、启明星辰信息技术集团股份有限公司、北京鼎普科技股份有限公司、中国电子信息产业集团有限公司第六研究所、公安部第一研究所、国家信息中心、山东微分电子科技有限公司、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、浙江大学、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、浙江国利信安科技有限公司、机械工业仪器仪表综合技术经济研究所、杭州科技职业技术学院。

本标准主要起草人：马力、陈广勇、张振峰、郭启全、葛波蔚、祝国邦、陆磊、曲洁、于东升、李秋香、任卫红、胡红升、陈雪鸿、冯冬芹、王江波、张宗喜、张宇翔、毕马宁、沙森森、李明、黎水林、于晴、李超、刘之涛、袁静、霍珊珊、黄顺京、尹湘培、苏艳芳、陶源、陈雪秀、于俊杰、沈锡镛、杜静、周颖、吴薇、刘志宇、宫月、王昱镔、禄凯、章恒、高亚楠、段伟恒、马闽、贾驰千、陆耿虹、高梦州、赵泰、孙晓军、许凤凯、王绍杰、马红霞、刘美丽。

本标准所代替标准的历次版本发布情况为：

——GB/T 22239—2008。

引　言

为了配合《中华人民共和国网络安全法》的实施，同时适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下网络安全等级保护工作的开展，需对 GB/T 22239—2008 进行修订，修订的思路和方法是调整原国家标准 GB/T 22239—2008 的内容，针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

本标准是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：

——GB/T 25058　信息安全技术　信息系统安全等级保护实施指南；

——GB/T 22240　信息安全技术　信息系统安全等级保护定级指南；

——GB/T 25070　信息安全技术　网络安全等级保护安全设计技术要求；

——GB/T 28448　信息安全技术　网络安全等级保护测评要求；

——GB/T 28449　信息安全技术　网络安全等级保护测评过程指南。

在本标准中，**黑体字部分**表示较高等级中增加或增强的要求。

信息安全技术
网络安全等级保护基本要求

1 范围

本标准规定了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 17859 计算机信息系统 安全保护等级划分准则

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069 信息安全技术 术语

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859、GB/T 22240、GB/T 25069、GB/T 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 界定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 31167—2014、GB/T 31168—2014 和 GB/T 32919—2016 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。

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。

3.3

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31167—2014，定义 3.1]

3.4

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络交付云计算的资源。

[GB/T 31167—2014，定义 3.3]

3.5

云服务客户　cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

[GB/T 31168—2014，定义 3.4]

3.6

云计算平台/系统　cloud computing platform/system

云服务商提供的云计算基础设施及其上的服务软件的集合。

3.7

虚拟机监视器　hypervisor

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.8

宿主机　host machine

运行虚拟机监视器的物理服务器。

3.9

移动互联　mobile communication

采用无线通信技术将移动终端接入有线网络的过程。

3.10

移动终端　mobile device

在移动业务中使用的终端设备，包括智能手机、平板电脑、个人电脑等通用终端和专用终端设备。

3.11

无线接入设备　wireless access device

采用无线通信技术将移动终端接入有线网络的通信设备。

3.12

无线接入网关　wireless access gateway

部署在无线网络与有线网络之间，对有线网络进行安全防护的设备。

3.13

移动应用软件　mobile application

针对移动终端开发的应用软件。

3.14

移动终端管理系统　mobile device management system

用于进行移动终端设备管理、应用管理和内容管理的专用软件，包括客户端软件和服务端软件。

3.15

物联网　internet of things

将感知节点设备通过互联网等网络连接起来构成的系统。

3.16

感知节点设备　sensor node

对物或环境进行信息采集和/或执行操作，并能联网进行通信的装置。

3.17

感知网关节点设备　sensor layer gateway

将感知节点所采集的数据进行汇总、适当处理或数据融合，并进行转发的装置。

3.18

工业控制系统　industrial control system

工业控制系统(ICS)是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统(SCADA)、分布式控制系统(DCS)和其他较小的控制系统，如可编程逻辑控制器(PLC)，现已广泛应用在工业部门和关键基础设施中。

[GB/T 32919—2016，定义 3.1]

4　缩略语

下列缩略语适用于本文件。

AP：无线访问接入点(Wireless Access Point)

DCS：集散控制系统(Distributed Control System)

DDoS：拒绝服务 (Distributed Denial of Service)

ERP：企业资源计划(Enterprise Resource Planning)

FTP：文件传输协议(File Transfer Protocol)

HMI：人机界面(Human Machine Interface)

IaaS：基础设施即服务(Infrastructure-as-a-Service)

ICS：工业控制系统(Industrial Control System)

IoT：物联网(Internet of Things)

IP：互联网协议(Internet Protocol)

IT：信息技术(Information Technology)

MES：制造执行系统(Manufacturing Execution System)

PaaS：平台即服务(Platform-as-a-Service)

PLC：可编程逻辑控制器(Programmable Logic Controller)

RFID：射频识别(Radio Frequency Identification)

SaaS：软件即服务(Software-as-a-Service)

SCADA：数据采集与监视控制系统(Supervisory Control and Data Acquisition System)

SSID：服务集标识(Service Set Identifier)

TCB：可信计算基(Trusted Computing Base)

USB：通用串行总线(Universal Serial Bus)

WEP：有线等效加密(Wired Equivalent Privacy)

WPS：WiFi 保护设置(WiFi Protected Setup)

5　网络安全等级保护概述

5.1　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、大数据应用/平台/资源、物联网(IoT)、工业控制系统和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。

保护对象的安全保护等级确定方法见 GB/T 22240。

5.2 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。

5.3 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，应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 和附录 C。

本标准针对云计算、移动互联、物联网、工业控制系统提出了安全扩展要求。云计算应用场景参见附录 D，移动互联应用场景参见附录 E，物联网应用场景参见附录 F，工业控制系统应用场景参见附录 G，大数据应用场景参见附录 H。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。

6 第一级安全要求

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。

6.1.1.2 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。

6.1.1.3 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。

6.1.1.4 防火

机房应设置灭火设备。

6.1.1.5 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。

6.1.1.6 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。

6.1.1.7 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。

6.1.2 安全通信网络

6.1.2.1 通信传输

应采用校验技术保证通信过程中数据的完整性。

6.1.2.2 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。

6.1.3 安全区域边界

6.1.3.1 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。

6.1.3.2 访问控制

本项要求包括：

a) 应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

6.1.3.3 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。

6.1.4 安全计算环境

6.1.4.1 身份鉴别

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，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。

6.1.4.2 访问控制

本项要求包括：

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。

6.1.4.3 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应关闭不需要的系统服务、默认共享和高危端口。

6.1.4.4 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。

6.1.4.5 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。

6.1.4.6 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。

6.1.4.7 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。

6.1.5 安全管理制度

6.1.5.1 管理制度

应建立日常管理活动中常用的安全管理制度。

6.1.6 安全管理机构

6.1.6.1 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。

6.1.6.2 人员配备

应配备一定数量的系统管理员。

6.1.6.3 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。

6.1.7 安全管理人员

6.1.7.1 人员录用

应指定或授权专门的部门或人员负责人员录用。

6.1.7.2 人员离岗

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

6.1.7.3 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。

6.1.7.4 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。

6.1.8 安全建设管理

6.1.8.1 定级和备案

应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。

6.1.8.2 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。

6.1.8.3 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。

6.1.8.4 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。

6.1.8.5 测试验收

应进行安全性测试验收。

6.1.8.6 系统交付

本项要求包括：

a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b) 应对负责运行维护的技术人员进行相应的技能培训。

6.1.8.7 服务供应商选择

本项要求包括：

a） 应确保服务供应商的选择符合国家的有关规定；

b） 应与选定的服务供应商签订与安全相关的协议，明确约定相关责任。

6.1.9 安全运维管理

6.1.9.1 环境管理

本项要求包括：

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

b） 应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。

6.1.9.2 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。

6.1.9.3 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。

6.1.9.4 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。

6.1.9.5 网络和系统安全管理

本项要求包括：

a） 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；

b） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。

6.1.9.6 恶意代码防范管理

本项要求包括：

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

b） 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

6.1.9.7 备份与恢复管理

本项要求包括：

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式、备份频度、存储介质、保存期等。

6.1.9.8 安全事件处置

本项要求包括：

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） 应明确安全事件的报告和处置流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

6.2 云计算安全扩展要求

6.2.1 安全物理环境

6.2.1.1 基础设施位置

应保证云计算基础设施位于中国境内。

6.2.2 安全通信网络

6.2.2.1 网络架构

本项要求包括：

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b） 应实现不同云服务客户虚拟网络之间的隔离。

6.2.3 安全区域边界

6.2.3.1 访问控制

应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。

6.2.4 安全计算环境

6.2.4.1 访问控制

本项要求包括：

a） 应保证当虚拟机迁移时，访问控制策略随其迁移；

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

6.2.4.2 数据完整性和保密性

应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。

6.2.5 安全建设管理

6.2.5.1 云服务商选择

本项要求包括：

a） 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；

b） 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；

c） 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。

6.2.5.2 供应链管理

应确保供应商的选择符合国家有关规定。

6.3 移动互联安全扩展要求

6.3.1 安全物理环境

6.3.1.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

6.3.2 安全区域边界

6.3.2.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入安全网关设备。

6.3.2.2 访问控制

无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符。

6.3.3 安全计算环境

6.3.3.1 移动应用管控

应具有选择应用软件安装、运行的功能。

6.3.4 安全建设管理

6.3.4.1 移动应用软件采购

应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名。

6.4 物联网安全扩展要求

6.4.1 安全物理环境

6.4.1.1 感知节点设备物理防护

本项要求包括：

a) 感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

b) 感知节点设备在工作状态所处物理环境应能正确反映环境状态(如温湿度传感器不能安装在阳光直射区域)。

6.4.2 安全区域边界

6.4.2.1 接入控制

应保证只有授权的感知节点可以接入。

6.4.3 安全运维管理

6.4.3.1 感知节点管理

应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护。

6.5 工业控制系统安全扩展要求

6.5.1 安全物理环境

6.5.1.1 室外控制设备物理防护

本项要求包括：

a) 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固；箱体或装置具有透风、散热、防盗、防雨和防火能力等；

b) 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

6.5.2 安全通信网络

6.5.2.1 网络架构

本项要求包括：

a) 工业控制系统与企业其他系统之间应划分为两个区域，区域间应采用技术隔离手段；

b) 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术隔离手段。

6.5.3 安全区域边界

6.5.3.1 访问控制

应在工业控制系统与企业其他系统之间部署访问控制设备，配置访问控制策略，禁止任何穿越区域边界的 E-Mail、Web、Telnet、Rlogin、FTP 等通用网络服务。

6.5.3.2 无线使用控制

本项要求包括：

a) 应对所有参与无线通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

b) 应对无线连接的授权、监视以及执行使用进行限制。

6.5.4 安全计算环境

6.5.4.1 控制设备安全

本项要求包括：

a) 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

b) 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作。

7 第二级安全要求

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

本项要求包括：

a) **机房场地应选择在具有防震、防风和防雨等能力的建筑内；**

b) **机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。**

7.1.1.2 物理访问控制

机房出入口应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。

7.1.1.3 防盗窃和防破坏

本项要求包括：

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。**

7.1.1.4 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。

7.1.1.5 防火

本项要求包括：

a) **机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；**

b) **机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。**

7.1.1.6 防水和防潮

本项要求包括：

a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

b) **应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。**

7.1.1.7 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。

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。

7.1.1.9 电力供应

本项要求包括：

a) 应在机房供电线路上配置稳压器和过电压防护设备；

b) 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

7.1.1.10 电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

7.1.2 安全通信网络

7.1.2.1 网络架构

本项要求包括：

a) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b) 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。

7.1.2.2 通信传输

应采用校验技术保证通信过程中数据的完整性。

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

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。

7.1.3.2 访问控制

本项要求包括：

a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；

d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。

7.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为。

7.1.3.4 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。

7.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

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

本项要求包括：

a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

7.1.4.2 访问控制

本项要求包括：

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。

7.1.4.3 安全审计

本项要求包括：

a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.1.4.4 入侵防范

本项要求包括：

a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应关闭不需要的系统服务、默认共享和高危端口；

c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d) 应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。

7.1.4.5 恶意代码防范

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

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

应采用校验技术保证重要数据在传输过程中的完整性。

7.1.4.8 数据备份恢复

本项要求包括：

a) 应提供重要数据的本地数据备份与恢复功能；

b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。

7.1.4.9 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。

7.1.4.10 个人信息保护

本项要求包括：

a) 应仅采集和保存业务必需的用户个人信息；

b) 应禁止未授权访问和非法使用用户个人信息。

7.1.5 安全管理中心

7.1.5.1 系统管理

本项要求包括：

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

本项要求包括：

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。

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，阐明机构安全工作的总体目标、范围、原则和安全框架等。