



中华人民共和国国家标准

GB/T 37939—2026

代替 GB/T 37939—2019

网络安全技术 网络存储安全技术要求

Cybersecurity technology—Technical requirements for network storage security

2026-05-25 发布

2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 概述 2

6 安全功能要求 2

 6.1 总则 2

 6.2 通用要求 2

 6.3 访问安全 3

 6.4 系统安全 3

 6.5 数据安全 4

 6.6 管理安全 7

7 安全保障要求..... 13

 7.1 总则 13

 7.2 通用要求 13

 7.3 开发 13

 7.4 指导性文档 15

 7.5 生存周期管理 15

 7.6 测试 17

 7.7 脆弱性评定 17

附录 A（资料性） 安全功能要求能力说明 19

附录 B（资料性） 安全功能要求与安全保障要求对应章条 20

参考文献 22

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 37939—2019《信息安全技术 网络存储安全技术要求》，与 GB/T 37939—2019 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 删除了“产品描述”一章(见 2019 年版的第 5 章)；
- b) 在“通用要求”中增加了符合 GB 42250—2022 的具体要求(见 6.2、7.2)；
- c) 更改了“访问控制”第一级、第二级、第三级的安全功能要求(见 6.3.2, 2019 年版的 6.1.2.2、6.2.2.2、6.3.2.2)；
- d) 删除了“概述”(见 2019 年版的 6.1.1、6.2.1、6.3.1)；
- e) 更改了“设备可靠运行支持”第二级、第三级的安全功能要求(见 6.4.1.2、6.4.1.3, 2019 年版的 6.2.3.1、6.3.3.1)；
- f) 更改了“软件及软件运行安全”第一级、第二级、第三级的安全功能要求(见 6.4.3, 2019 年版的 6.1.3.3、6.2.3.4、6.3.3.4)；
- g) 更改了“安全加固”第二级、第三级的安全功能要求(见 6.4.5, 2019 年版的 6.2.3.5、6.3.3.5)；
- h) 增加了“资源隔离”第二、三级的安全功能要求(见 6.4.7)；
- i) 增加了“硬件可靠性”第三级的安全功能要求(见 6.4.9)；
- j) 更改了“存储数据的完整性”第二级、第三级的安全功能要求(见 6.5.1.1.2、6.5.1.1.3, 2019 年版的 6.2.4.1.1、6.3.4.1.1)；
- k) 更改了“数据保密性”第二级、第三级的安全功能要求(见 6.5.2.1.2、6.5.2.1.3, 2019 年版的 6.2.4.2、6.3.4.2.1)；
- l) 更改了“剩余信息保护”第三级的安全功能要求(见 6.5.2.2, 2019 年版的 6.3.4.2.2)；
- m) 更改了“数据冗余”第一级、第二级、第三级的安全功能要求(见 6.5.3.3, 2019 年版的 6.1.4.3.3、6.2.4.3.3、6.3.4.3.3)；
- n) 增加了“链路断开”第三级的安全功能要求(见 6.5.3.4)；
- o) 更改了“高可用”第三级的安全功能要求(见 6.5.3.5, 2019 年版的 6.3.4.3.4)；
- p) 更改了“口令安全管理”第一级、第二级、第三级的安全功能要求(见 6.6.2.2, 2019 年版的 6.1.5.2.2、6.2.5.2.2、6.3.5.2.2)；
- q) 删除了“密码算法”第一级、第二级的安全功能要求，更改了第三级的安全功能要求(见 6.6.4, 2019 年版的 6.1.5.4、6.2.5.4、6.3.5.4)；
- r) 更改了“审计数据产生”第二级、第三级的安全功能要求(见 6.6.5.1.2, 2019 年版的 6.2.5.5.1、6.3.5.5.1)；
- s) 更改了“审计数据存储”第一级、第二级、第三级的安全功能要求(见 6.6.5.3, 2019 年版的 6.1.5.5.3、6.2.5.5.3、6.3.5.5.3)；
- t) 更改了“配置管理范围”第一级、第二级、第三级的安全保障要求(见 7.5.2, 2019 年版的 7.1.3.2、7.2.3.2、7.3.3.2)；
- u) 删除了“开发安全”(见 2019 年版的 7.2.3.4、7.3.3.4)；
- v) 增加了“开发者环境安全”(见 7.5.4)；
- w) 删除了“生命周期定义”(见 2019 年版的 7.2.3.5、7.3.3.5)；

- x) 增加了“开发生存周期”(见 7.5.5);
- y) 更改了“工具和技术”第三级的安全保障要求(见 7.5.6,2019 年版的 7.3.3.6);
- z) 更改了“深度”第二级、第三级的安全保障要求(见 7.6.2,2019 年版的 7.2.4.2、7.3.4.2);
- aa) 删除了“代码测试”(见 2019 年版的 7.1.4.4、7.2.4.5、7.3.4.5);
- ab) 更改了“脆弱性评定”第一级、第二级、第三级的安全保障要求(见 7.7,2019 年版的 7.1.5、7.2.5、7.3.5)。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中国电子技术标准化研究院、华为技术有限公司、公安部第三研究所、华中科技大学、桂林电子科技大学、中国移动信息技术有限公司、浪潮电子信息产业股份有限公司、深信服科技股份有限公司、南方电网数字电网集团信息通信科技有限公司、新华三技术有限公司、中国科学院信息工程研究所、中国科学院软件研究所、陕西省网络与信息安全测评中心、上海市信息安全测评认证中心、中国软件评测中心、长扬科技(北京)股份有限公司、郑州信大捷安信息技术股份有限公司、联想(北京)有限公司、兴唐通信科技有限公司、北京时代新威信息技术有限公司、上海观安信息技术股份有限公司、浙江大华技术股份有限公司、山东商业职业技术学院、大唐高鸿信安(浙江)信息科技有限公司、天津天复检测技术有限公司、山东中网云安智能科技有限公司、北京数安行科技有限公司。

本文件主要起草人:李琳、孟凡辉、陈妍、李彦峰、章倩、王孝丰、冯轶、邢希双、蒋涛涛、黄国栋、张天洁、刘清林、赵新强、王惠莅、王芳、李春海、曹雅琴、吴敬征、刘玉岭、朱雪峰、李霖琦、靳倩、徐佟海、刘心宇、凌祥、秦巍、熊娇、陈新军、张璐、赵华、刘为华、杨利锋、蔡子凡、黄国强、王文君、张浩、卢国庆、刘海洁、张宇、刘俊、杨亚楠、苏昭宇、李鹏、陈强、安健、刘玉红。

本文件及其所代替文件的历次版本发布情况为:

——2019 年首次发布为 GB/T 37939—2019;

——本次为第一次修订。

网络安全技术 网络存储安全技术要求

1 范围

本文件规定了网络存储的安全功能要求、安全保障要求。
本文件适用于网络存储的设计、开发、测试与评估。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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—2022 信息安全技术 术语
GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

3 术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

网络存储 network storage

通过网络为企业提供数据存储和访问服务的设备。

注:网络存储通常包括块存储设备、文件存储设备、对象存储设备等。

3.2

对象存储 object based storage

基于对象的方式提供数据访问的存储架构。

注:一个对象通常包括数据、描述该对象的元数据和该对象的唯一标识符。

3.3

镜像 mirroring

实时地将一个逻辑盘卷上的数据复制到若干个逻辑盘卷上。

3.4

敏感数据 sensitive data

一旦泄露、非法提供或滥用可能危害网络安全的数据。

注:网络关键设备常见的敏感数据包括口令、密钥、关键配置信息等。

[来源:GB 40050—2021,3.4]

4 缩略语

下列缩略语适用于本文件。

CER:证书(Certificate)

CPU:中央处理器(Central Processing Unit)

DER:可辨别编码规则(Distinguished Encoding Rules)

JKS:Java 密钥库(Java KeyStore)

- PEM:增强隐私的电子邮件(Privacy Enhanced Mail)
- PKCS#12:公钥密码标准第12号(Public-Key Cryptography Standards #12)
- RAID:独立磁盘冗余阵列(Redundant Array of Independent Disks)
- URL:统一资源定位符(Uniform Resource Locator)
- WORM:一次写多次读(Write Once Read Many)

5 概述

网络存储安全技术要求包括安全功能要求和产品全生存周期过程的安全保障要求两个方面。网络存储安全功能框架见图1,包括访问安全、系统安全、数据安全和管理安全等方面;网络存储安全保障要求包括开发、指导性文档、生存周期管理、测试、脆弱性评定等方面。

根据不同应用场景需求的差异,结合网络存储产品安全功能的强弱和安全保障要求的高低,本文件将安全功能要求和安全保障要求各自划分为三个级别,分别是第一级、第二级和第三级,“宋体加粗”字表示较低等级中没有出现或增强的要求。

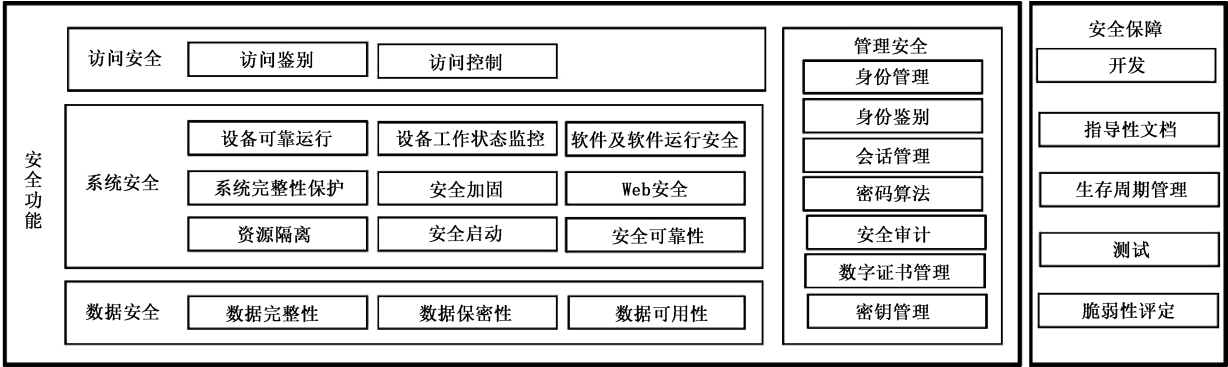


图 1 网络存储安全技术要求框架

6 安全功能要求

6.1 总则

第一级安全功能要求提出了网络存储应具备的基本安全功能。与第一级安全功能相比,第二级安全功能增强了系统安全中系统完整性保护、安全加固和 Web 安全等方面的要求,增强了数据安全中传输数据的完整性、处理数据的完整性等方面的要求,增强了管理安全中账号安全管理、鉴别机制、审计内容和数字证书等方面的要求。与第二级安全功能相比,第三级安全功能增强了系统安全中系统完整性保护、安全启动、硬件可靠性等方面的要求,增强了数据安全中数据完整性、数据保密性和高可用等方面的要求,增强了管理安全中会话管理、鉴别机制管理、口令安全管理、登录身份鉴别、数字证书和密钥管理等方面的要求。各等级网络存储安全功能要求能力说明见附录 A。

本章中没有明确具体级别的要求章条,则表示第一级、第二级、第三级均应符合该章条的要求;有明确具体级别的要求章条,则对应具体级别应符合该章条的要求。不同级别安全功能要求的对应章条见附录 B 中的表 B.1。

6.2 通用要求

应符合 GB 42250—2022 中第 5 章规定的标识和鉴别、自身访问控制、自身安全审计、通信安全、支撑系统安全、产品升级、用户信息安全和密码等方面的要求。

6.3 访问安全

6.3.1 访问鉴别

应对访问网络存储的应用进行鉴别,符合以下要求:

- a) 对应用提供唯一标识,并将标识和与其相关的所有可审计事件相关联;
- b) 鉴别信息应非明文存储,且鉴别数据不被未经授权查阅和篡改;
- c) 不存在能绕过鉴别机制的访问方式。

6.3.2 访问控制

应按访问控制安全策略进行设计,实现策略控制下的访问控制功能,符合以下要求:

- a) 访问控制的策略范围包含与资源访问相关的主体、客体及它们之间的操作;
- b) 对资源进行访问的内容、操作权限不超出预设的范围,符合最小特权原则;
- c) 服务器与存储连接的网络和管理网络应相互隔离,无法互相访问;
- d) 具备日志审计功能;
- e) 如具备多协议访问功能,设置统一的访问控制策略。

6.4 系统安全

6.4.1 设备可靠运行

6.4.1.1 第一级安全功能要求

应具备管理模块冗余、电源模块冗余、控制模块冗余等功能,并提供容错和故障恢复能力。

6.4.1.2 第二级安全功能要求

应符合以下要求:

- a) 集中式存储设备具备管理模块冗余、电源模块冗余、控制模块冗余等功能,并提供容错和故障恢复能力;
- b) 具备对内存的检测与纠错的功能;
- c) 具备对硬磁盘和固态硬盘检测的功能。

6.4.1.3 第三级安全功能要求

应符合以下要求:

- a) 集中式存储设备具备管理模块冗余、电源模块冗余、控制模块冗余等功能,并提供容错和故障恢复能力;
- b) 具备对内存的检测与纠错的功能;
- c) 具备对硬磁盘和固态硬盘检测的功能;
- d) 具备对 CPU 异常检测的功能。

6.4.2 设备工作状态监控

应具备自动检测设备的工作状态功能,包括不限于检测硬件故障、网络中断、网络连接错误、配额容量预警、业务异常预警等内容,并对监测到的设备异常状态进行告警。

6.4.3 软件及软件运行安全

系统软件及软件运行环境不应存在已知综合分级为高危、中危风险级别的漏洞。

6.4.4 系统完整性保护

6.4.4.1 第二级安全功能要求

应提供系统完整性保护功能,符合以下要求:

- a) 软件安装包进行完整性保护;
- b) 具备在固件升级和安装过程中对固件进行完整性校验的功能。

6.4.4.2 第三级安全功能要求

应提供系统完整性保护功能,符合以下要求:

- a) 软件安装包进行完整性保护;
- b) 具备在固件升级和安装过程中对固件进行完整性校验的功能;
- c) 对软件包进行数字签名。

6.4.5 安全加固

第二级、第三级应具备安全加固功能,符合以下要求:

- a) 对操作系统、数据库和文件系统应进行安全加固;
- b) 关闭不需要的系统服务、默认共享和端口;
- c) 具备关闭不安全访问协议的功能,并缺省关闭;
- d) 不能直接使用 root 账号进行远程登录。

6.4.6 Web 安全

第二级、第三级应提供 Web 安全功能,符合以下要求:

- a) 对于每一个需要授权访问的请求都核实用户的会话标识是否合法、用户是否被授权执行此操作;
- b) 具备对所有来自不可信数据源的数据进行内容校验的功能,拒绝任何没有通过校验的数据;
- c) 若输出到客户端的数据来自不可信的数据源,则对该数据进行相应的编码或转义;
- d) 通过 Web 上传文件时,在服务器端采用白名单方式对上传到 Web 内容目录下的文件类型进行限制;
- e) 在 Web 应用中,用户名和口令鉴别通过后,更换会话标识,使用 cookie 维持会话。

6.4.7 资源隔离

第二级、第三级要求文件存储设备和对象存储设备应具备租户级别的资源隔离功能,保障多租户彼此的资源使用互不干扰。

6.4.8 安全启动

第三级要求设备启动时应对软件和固件进行完整性验证。

6.4.9 硬件可靠性

第三级要求集中式存储设备应具备存储控制器、硬磁盘和固态盘等关键部件热冗余功能,故障时可切换。

6.5 数据安全

6.5.1 数据完整性

6.5.1.1 存储数据的完整性

6.5.1.1.1 第一级安全功能要求

应具备检测存储过程中的数据完整性错误的功能,并提供必要的恢复措施。

6.5.1.1.2 第二级安全功能要求

应对存储过程中的数据进行完整性保护,符合以下要求:

- a) 具备检测存储过程中的数据完整性错误的功能,在有冗余数据情况下提供自动恢复功能;
- b) 具备自动检测存储的数据完整性错误的功能,在有冗余数据情况下提供自动恢复功能;
- c) 文件存储设备具备文件系统粒度的安全快照功能;
- d) 具备 WORM 功能。

6.5.1.1.3 第三级安全功能要求

应对存储过程中的数据进行完整性保护,符合以下要求:

- a) 具备检测存储过程中的数据完整性错误的功能,在有冗余数据情况下提供自动恢复功能;
- b) 具备自动检测存储的数据完整性错误的功能,在有冗余数据情况下提供自动恢复功能;
- c) 具备逻辑单元/文件系统误删除找回功能;
- d) 文件存储设备具备文件系统粒度的安全快照功能;
- e) 具备 WORM 功能。

6.5.1.2 传输数据的完整性

6.5.1.2.1 第二级安全功能要求

应对在网络存储内部传输的数据提供完整性保护,具备检测传输中的数据完整性错误的功能。

6.5.1.2.2 第三级安全功能要求

应对在网络存储内部不同组件、部件之间传输的数据提供完整性保护,符合以下要求:

- a) 具备检测传输中的数据完整性错误的功能;
- b) 检测到数据完整性错误时,执行必要的的数据恢复操作。

6.5.1.3 处理数据的完整性

第二级、第三级应具备对处理中的数据进行完整性保护的功能。

6.5.2 数据保密性

6.5.2.1 数据保密性

6.5.2.1.1 第一级安全功能要求

系统管理数据不应对外暴露,应采用非明文方式存储,符合以下要求:

- a) 系统口令等敏感信息非明文存储在本地,需加密保护;
- b) 不在 URL、日志、错误消息、调试信息中暴露系统的口令、密钥、会话标识符等敏感信息。

6.5.2.1.2 第二级安全功能要求

应对数据的保密性进行保护,符合以下要求。

- a) 具备数据存储的透明加解密的功能。
- b) 在非信任网络之间传输数据时,采用安全传输通道或者加密后传输。
- c) 系统管理数据不对外暴露,采用非明文方式存储,并符合以下要求:
 - 1) 系统口令等敏感信息非明文存储在本地,需加密保护;
 - 2) 不在 URL、日志、错误消息、调试信息中暴露系统口令、密钥、会话标识符等敏感信息。
- d) 对敏感数据的访问应具备鉴别、授权或加密机制。
- e) 具备对存储的数据进行加密的功能。

6.5.2.1.3 第三级安全功能要求

应对数据的保密性进行保护,符合以下要求。

- a) 具备数据落盘的透明加解密的功能。
- b) 具备数据传输过程中的加密功能。
- c) 系统管理数据不应对外暴露,采用非明文方式存储,符合以下要求:
 - 1) 系统口令等敏感信息不明文存储在本地,需加密保护;
 - 2) 不在 URL、日志、错误消息、调试信息中暴露系统口令、密钥、会话标识符等敏感信息。
- d) 对敏感数据的访问要有鉴别、授权或加密机制。
- e) 具备对存储的数据进行加密的功能。

6.5.2.2 剩余信息保护

第三级应具备剩余信息保护功能,符合以下要求:

- a) 具备对鉴别信息和敏感信息所在的存储空间进行完全清除的功能;
- b) 具备硬磁盘和固态盘数据安全擦除的功能,数据擦除后,不可恢复。

6.5.3 数据可用性

6.5.3.1 备份与恢复

6.5.3.1.1 第一级安全功能要求:

应具备对数据进行备份和恢复的功能,符合以下要求:

- a) 具备对数据进行手动备份与备份恢复的功能;
- b) 具备对数据进行全备份与备份恢复的功能;
- c) 具备对数据进行异步备份与备份恢复的功能;
- d) 具备对数据进行本地备份与备份恢复的功能;
- e) 具备快照方式的数据备份与恢复功能。

6.5.3.1.2 第二级、第三级安全功能要求

应具备对数据进行备份和恢复的功能,符合以下要求:

- a) 具备对数据进行手动备份与备份恢复的功能;
- b) 具备对数据进行全备份与备份恢复的功能;
- c) 具备对数据进行异步备份与备份恢复的功能;
- d) 具备对数据进行本地备份与备份恢复的功能;
- e) 具备快照方式的数据备份与恢复功能;
- f) 具备对数据进行自动备份与备份恢复的功能;
- g) 具备对数据进行增量备份与备份恢复的功能;
- h) 具备对数据进行同步备份与备份恢复的功能;
- i) 具备对数据进行异地备份与备份恢复的功能;
- j) 具备远程复制提供数据的备份与恢复功能。

6.5.3.2 防病毒

文件存储设备和对象存储设备应具备病毒扫描和查杀功能。

6.5.3.3 数据冗余

应具备 RAID、多副本、纠删码其中一种或多种数据冗余功能。

6.5.3.4 链路断开

第三级应具备勒索软件攻击自动检测及数据副本环境和生产环境链路的快速关断功能。

6.5.3.5 高可用

第三级要求网络存储发生故障时,业务应自动切换到备用的网络存储。

6.6 管理安全

6.6.1 身份管理

6.6.1.1 身份标识管理

6.6.1.1.1 第一级安全功能要求

应提供设备用户的标识功能,为每个用户提供唯一的身份标识。

6.6.1.1.2 第二级安全功能要求

应提供设备用户的标识功能,符合以下要求:

- a) 为每个用户提供唯一的身份标识;
- b) 未授权用户无法对用户身份标识进行访问和管理。

6.6.1.1.3 第三级安全功能要求

应提供设备用户的标识功能,符合以下要求:

- a) 为每个用户提供唯一的身份标识;
- b) 未授权用户无法对用户身份标识进行访问和管理;
- c) 将用户身份标识和该用户的所有可审计事件相关联。

6.6.1.2 账号安全管理

6.6.1.2.1 第一级安全功能要求

应符合以下要求:

- a) 系统中的账号具有唯一性;
- b) 不预留任何的未公开账号,所有账号都能被系统管理,并在资料中提供所有账号及管理操作说明。

6.6.1.2.2 第二级、第三级安全功能要求

应符合以下要求:

- a) 系统中的账号具有唯一性;
- b) 不预留任何的未公开账号,所有账号都可被系统管理,并在资料中提供所有账号及管理操作说明;
- c) 若产品自带数据库且存在多个默认账号,禁用或删除不使用的账号;若无法删除或禁用,在产品资料中提示用户修改默认账号的口令并定期更新。

6.6.1.3 账号权限管理

应符合以下要求:

- a) 采用基于角色的账号权限管理模型;
- b) 对于账号的授权应基于最小特权原则;
- c) 系统中的账号不能修改自身权限。

6.6.2 身份鉴别

6.6.2.1 鉴别机制管理

6.6.2.1.1 第一级安全功能要求

应符合以下要求：

- a) 在用户对网络存储进行操作之前,先对提出该操作请求的用户进行鉴别；
- b) 对用户的最终鉴别处理、鉴权处理过程按先鉴权后执行的原则在服务端进行。

6.6.2.1.2 第二级安全功能要求

应符合以下要求：

- a) 在用户对网络存储进行操作之前,先对提出该操作请求的用户进行鉴别；
- b) 对用户的最终鉴别处理、鉴权处理过程按先鉴权后执行的原则在服务端进行；
- c) 当用户连续鉴别失败达到设定次数后,采取措施阻止用户的进一步请求；
- d) 用户操作超时被断开后,重新连接时重新进行鉴别；
- e) 具备用户鉴别信息非明文存储的功能,且鉴别数据不被未授权查阅和修改。

6.6.2.1.3 第三级安全功能要求

应符合以下要求：

- a) 在用户对网络存储进行操作之前,先对提出该操作请求的用户进行鉴别；
- b) 对用户的最终鉴别处理、鉴权处理过程按先鉴权后执行的原则在服务端进行；
- c) 当用户连续鉴别失败达到设定次数后,采取措施阻止用户的进一步请求；
- d) 用户操作超时被断开后,重新连接时重新进行鉴别；
- e) 用户鉴别信息应非明文存储,且鉴别数据不被未授权查阅和修改；
- f) 提供多种鉴别机制及相应鉴别规则；
- g) 实现基于密码技术的身份鉴别机制。

6.6.2.2 口令安全管理

6.6.2.2.1 第一级安全功能要求

应符合以下要求。

- a) 首次管理设备时不使用缺省口令,强制修改缺省口令或设置口令。
- b) 具备设置口令生存周期的功能。
- c) 用户输入口令时,不明文显示口令。
- d) 对于管理层,系统提供检测口令复杂度的功能,若设置的口令不符合复杂度要求,不准许设置成功并给出合理的提示,对于系统自动生成的口令,使用安全随机数生成。
- e) 口令复杂度符合以下要求：
 - 1) 口令长度至少 8 个字符；
 - 2) 口令包含至少 2 种字符的组合；
 - 3) 口令不可与账号或账号的倒写相同。
- f) 产品出厂使用的第三方和开源软件不使用缺省口令。
- g) 不存在用户无法修改的口令。对于出厂时缺省设置的账号/口令或用于传输的加密密钥,提供修改机制,提醒用户修改及定期更新,并提示风险。
- h) 提供的口令输入框不可复制出口令。
- i) 操作界面中的口令不明文显示。
- j) 密码口令文件设置访问权限,无访问权限用户不可读取或复制口令等数据内容。
- k) 用户修改口令时,强制验证当前口令。

6.6.2.2.2 第二级安全功能要求

应符合以下要求。

- a) 对于管理层面,系统提供检测口令复杂度的功能,若设置的口令不符合复杂度要求,不设置成功,并给出设置不成功的提示,对于系统自动生成的口令,使用安全随机数生成。
- b) 口令复杂度符合以下要求:
 - 1) 口令长度至少 8 个字符;
 - 2) 口令包含至少 2 种字符的组合;
 - 3) 口令不可与账号相同。
- c) 产品出厂使用的第三方和开源软件不使用缺省口令。
- d) 系统默认账号禁止使用缺省口令,对于系统外部可访问的所有管理账号,在系统初始安装过程中或首次登录时,强制设置或修改符合口令复杂度的口令,并且在完成口令设置或修改前,禁止登录到系统进行其他操作。
- e) 由管理员新建/重置用户账号的口令,用户首次登录时强制修改口令。
- f) 不存在用户无法修改的口令。对于出厂时缺省设置的账号/口令或用于传输的加密密钥,产品提供修改机制,提醒用户修改及定期更新,并提示风险。
- g) 产品提供的口令输入框不可复制出口令。
- h) 操作界面中的口令不明文显示。
- i) 密码口令文件设置访问权限,无访问权限用户不可读取或复制加密的内容。
- j) 用户修改口令时,强制验证当前口令。

6.6.2.2.3 第三级安全功能要求

应符合以下要求。

- a) 对于管理层面,系统提供检测口令复杂度的功能,若设置的口令不符合复杂度要求,不设置成功,并给出设置不成功的提示,对于系统自动生成的口令,使用安全随机数生成。
- b) 口令复杂度符合以下要求:
 - 1) 口令长度至少 8 个字符;
 - 2) 口令包含至少 2 种字符的组合;
 - 3) 口令不可与账号相同。
- c) 产品出厂使用的第三方和开源软件不使用缺省口令。
- d) 系统默认账号禁止使用缺省口令,对于系统外部可访问的所有管理账号,在系统初始安装过程中或首次登录时,强制设置或修改符合口令复杂度的口令,并且在完成口令设置或修改前,禁止登录到系统进行其他操作。
- e) 由管理员新建/重置用户账号的口令,用户首次登录时强制修改口令。
- f) 系统提供弱口令字典功能,避免用户使用弱口令字典中的任何口令。
- g) 不存在用户无法修改的口令。对于出厂时缺省设置的账号/口令或用于传输的加密密钥,提供修改机制,提醒用户修改及定期更新,并提示风险。
- h) 提供的口令输入框不可复制出口令。
- i) 操作界面中的口令不明文显示。
- j) 密码口令文件设置访问权限,无访问权限用户不可读取或复制加密的内容。
- k) 用户修改口令时,强制验证当前口令。

6.6.2.3 登录身份鉴别

6.6.2.3.1 第一级、第二级安全功能要求

应提供登录身份鉴别功能,符合以下要求:

- a) 管理接口应提供接入鉴别机制,所有通过人工操作方式对系统进行管理配置的交互接口以及

跨信任网络的机机交互接口具备安全的接入鉴别机制并缺省启用,标准协议没有鉴别机制的除外;

- b) 外部可见的可对系统进行调试或管理的物理接口禁用或有接入鉴别机制;
- c) 对于通过人工操作方式对系统进行管理配置的交互接口或跨信任网络的机机交互接口的登录身份鉴别应实现口令防暴力破解机制,当重复输入错误口令次数超过设定值时采取合适保护措施。

6.6.2.3.2 第三级安全功能要求

应提供登录身份鉴别功能,符合以下要求:

- a) 管理接口应提供接入鉴别机制,所有通过人工操作方式对系统进行管理配置的交互接口以及跨信任网络的机机交互接口具备安全的接入鉴别机制并缺省启用,标准协议没有鉴别机制的除外;
- b) 外部可见的可对系统进行调试或管理的物理接口禁用或有接入鉴别机制;
- c) 对于通过人工操作方式对系统进行管理配置的交互接口或跨信任网络的机机交互接口的登录身份鉴别应实现口令防暴力破解机制,当重复输入错误口令次数超过设定值时采取合适保护措施;
- d) 具备口令错误次数、用户锁定时长配置功能。

6.6.3 会话管理

6.6.3.1 第一级安全功能要求

应具备会话超时设置功能,并在超时过后清除该会话信息。

6.6.3.2 第二级安全功能要求

应提供会话管理功能,符合以下要求。

- a) 应具备会话超时设置功能,并在超时时清除该会话信息。
- b) 所有登录后才可访问的界面都提供主动退出选项。当用户退出时,服务端应清除该用户的会话信息。

6.6.3.3 第三级安全功能要求

应提供会话管理功能,符合以下要求。

- a) 具备会话超时设置功能,并在超时时清除该会话信息。
- b) 所有登录后才可访问的界面都提供主动退出选项。当用户退出时,服务端清除该用户的会话信息。
- c) 会话标识应使用安全随机数算法生成。
- d) 具备会话超时的时间可配置的功能。

6.6.4 密码算法

第三级要求产品中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

6.6.5 安全审计

6.6.5.1 审计数据产生

6.6.5.1.1 第一级安全功能要求

应符合以下要求:

- a) 具备对表 1 中的可审计事件进行安全审计的功能,并生成审计数据;
- b) 对于每一个事件,其审计记录包括用户、被访问资源的名称、访问发起端地址或标识、事件的日

期和时间、事件类型、事件是否成功,及其他与审计相关的信息。

表 1 可审计事件列表

序号	可审计事件
1	审计功能的开启和关闭
2	针对数据的备份、恢复、删除、迁移等操作
3	以下的用户活动和关键操作行为： ——登录和注销； ——增加、删除用户和用户属性(账号、口令等)的变更； ——用户的锁定与解锁、禁用与恢复； ——角色权限变更； ——系统安全配置(如安全日志内容等配置)的变更； ——重要资源的变更,如某个重要文件的删除、修改等； ——对系统配置参数的修改； ——对系统进行启动、关闭、重启、暂停、恢复、倒换等操作； ——存储业务的加载、卸载； ——对软件的升级操作,包括远程升级和本地升级； ——对重要业务数据(特别是逻辑卷、文件系统、对象等)的创建、删除、修改等
4	其他与系统安全有关的事件或特指的可审计事件

6.6.5.1.2 第二级、第三级安全功能要求

应符合以下要求：

- a) 具备对表 1 中的可审计事件进行安全审计的功能,并生成审计数据；
- b) 对于每一个事件,其审计记录包括用户、被访问资源的名称、访问发起端地址或标识、事件的日期和时间、事件类型、事件是否成功信息；
- c) 审计数据产生时的时间由网络存储所在系统范围内唯一确定的时钟产生；
- d) 对于身份鉴别事件,审计记录包含请求的来源。

6.6.5.2 审计数据管理

6.6.5.2.1 第一级、第二级安全功能要求

应符合以下要求：

- a) 只有具有相应权限的用户才能读取对应的审计数据；
- b) 以可被处理的形式提供审计数据。

6.6.5.2.2 第三级安全功能要求

应符合以下要求：

- a) 只有具有相应权限的用户才能读取对应的审计数据；
- b) 以可被处理的形式提供审计数据；
- c) 具备条件化检索审计数据的功能,例如搜索、分类、排序等。

6.6.5.3 审计数据存储

6.6.5.3.1 第一级安全功能要求

审计记录的留存时间应不低于 6 个月。

6.6.5.3.2 第二级、第三级安全功能要求

应符合以下要求：

- a) 审计记录的留存时间不低于 6 个月；
- b) 检测或防止对审计记录的未授权修改；
- c) 审计数据被未授权修改时,对该操作进行审计；
- d) 审计存储已满、存储失败时,审计记录不丢失。

6.6.6 数字证书管理

6.6.6.1 第一级安全功能要求

应符合以下要求：

- a) 能处理 PEM、CER、JKS、PKCS#12、DER 等通用格式的一种或多种,且使用安全的证书签名算法；
- b) 设置合理的证书有效期；
- c) 具备证书的有效性验证功能。

6.6.6.2 第二级安全功能要求

应符合以下要求：

- a) 能处理 PEM、CER、JKS、PKCS#12、DER 等通用格式的一种或多种,且使用安全的证书签名算法；
- b) 设置合理的证书有效期；
- c) 具备证书的有效性验证功能；
- d) 证书的私钥加密保存,私钥保护口令符合复杂度要求并加密保存,同时控制私钥文件和证书文件的访问权限；
- e) 具备设备上各种类型的证书周期性检查功能,检查该证书是否过期或即将过期；
- f) 使用安全随机数生成密钥对。

6.6.6.3 第三级安全功能要求

应符合以下要求：

- a) 能处理 PEM、CER、JKS、PKCS#12、DER 等通用格式的一种或多种,且使用安全的证书签名算法；
- b) 设置合理的证书有效期；
- c) 具备证书的有效性验证功能；
- d) 证书的私钥加密保存,私钥保护口令符合复杂度要求并加密保存,同时控制私钥文件和证书文件的访问权限；
- e) 具备设备上各种类型的证书周期性检查功能,检查该证书是否过期或即将过期；
- f) 使用安全随机数生成密钥对；
- g) 适配第三方可信机构颁发的数字证书；
- h) 具备对证书的吊销状态进行验证的功能。

6.6.7 密钥管理

6.6.7.1 第一级安全功能要求

应符合以下要求：

- a) 对密钥进行分层管理；
- b) 手动输入的值,不可直接作为密钥使用；

- c) 用于敏感数据加密的密钥,不可写在源代码中。

6.6.7.2 第二级安全功能要求

应符合以下要求:

- a) 对密钥进行分层管理;
- b) 手动输入的值,不可直接作为密钥使用;
- c) 用于敏感数据加密的密钥,不可写在源代码中;
- d) 密钥及相关信息在本地存储时需提供完整性保护和机密性保护。

6.6.7.3 第三级安全功能要求

应符合以下要求:

- a) 对密钥进行分层管理;
- b) 手动输入的值,不可直接作为密钥使用;
- c) 用于敏感数据加密的密钥,不可写在源代码中;
- d) 密钥及相关信息在本地存储时需提供完整性保护和机密性保护;
- e) 密钥管理系统具备对存储进行必要的密钥管理的功能。

7 安全保障要求

7.1 总则

本章规定了网络存储的安全保障要求,所选择的安全保障要求级别应不低于安全功能要求的级别。本章中没有明确具体级别的要求章条,则表示第一级、第二级、第三级均应符合该章条的要求;有明确具体级别的要求章条,则对应具体级别应符合该章条的要求。不同级别安全保障要求的对应章条见表 B.2。

7.2 通用要求

应符合 GB 42250—2022 中第 6 章规定的供应链安全、设计与开发、生产和交付、运维服务保障、用户信息保护方面的要求。

7.3 开发

7.3.1 安全架构

开发者应向评估者提供产品安全功能的安全架构描述:

- a) 与产品设计文档中对安全功能要求执行的抽象描述详细程度一致;
- b) 描述与安全功能要求一致的产品安全功能的安全域;
- c) 描述产品安全功能初始化过程为何是安全的;
- d) 证实产品安全功能能防止被破坏;
- e) 证实产品安全功能能防止安全功能要求执行的功能被旁路。

7.3.2 功能规范文档

7.3.2.1 第一级安全保障要求

开发者应向评估者提供一个功能规范文档:

- a) 完整描述产品的安全功能;
- b) 描述所有安全功能接口的目的与使用方法;
- c) 标识和描述每个安全功能接口相关的所有参数;
- d) 描述安全功能接口相关的安全功能要求执行行为;
- e) 描述由安全功能要求执行行为相关处理而引起的直接错误消息;

- f) 证实安全功能要求与安全功能接口的追溯关系。

7.3.2.2 第二级安全保障要求

开发者应向评估者提供一个功能规范文档：

- a) 完整描述产品的安全功能；
- b) 描述所有安全功能接口的目的与使用方法；
- c) 标识和描述每个安全功能接口相关的所有参数；
- d) 总结与每个安全功能接口相关的安全功能要求支撑和无关的行为；
- e) 描述由安全功能接口调用相关的安全实施行为和异常而引起的直接错误消息；
- f) 证实安全功能要求与安全功能接口的追溯关系。

7.3.2.3 第三级安全保障要求

开发者应向评估者提供一个功能规范文档：

- a) 完整描述产品的安全功能；
- b) 描述所有安全功能接口的目的与使用方法；
- c) 标识和描述每个安全功能接口相关的所有参数；
- d) 描述安全功能接口相关的所有行为；
- e) 描述可能由每个安全功能接口的调用而引起的所有直接错误消息；
- f) 证实安全功能要求与安全功能接口的追溯关系。

7.3.3 实现表示

第三级要求开发者应向评估者提供全部安全功能的实现表示,实现表示应符合以下要求：

- a) 详细地给出产品安全功能,详细程度达到无须进一步设计就能生成安全功能的程度；
- b) 以开发人员使用的形式提供；
- c) 提供产品设计描述与实现表示实例之间的映射,并证明其一致性。

7.3.4 产品设计

7.3.4.1 第一级安全保障要求

开发者应向评估者提供产品设计文档：

- a) 根据子系统描述产品结构；
- b) 标识产品安全功能的所有子系统；
- c) 对每一个安全功能要求支撑或安全功能要求无关的安全功能子系统的行为进行足够详细的描述；
- d) 概述安全功能要求执行子系统的安全功能要求执行行为；
- e) 描述安全功能要求执行子系统间的交互关系、安全功能要求执行子系统与其他安全功能子系统的交互关系；
- f) 提供映射关系,证实设计中描述的所有行为能映射到调用它的安全功能接口。

7.3.4.2 第二级安全保障要求

开发者应向评估者提供产品设计文档：

- a) 根据子系统描述产品结构；
- b) 标识产品安全功能的所有子系统；
- c) 对每一个安全功能要求无关子系统的行为进行概述；
- d) 描述安全功能要求执行子系统的安全功能要求执行行为；
- e) 概述安全功能要求执行子系统的安全功能要求支撑和无关行为；
- f) 描述安全功能要求支撑子系统的行为；

- g) 描述安全功能所有子系统间的交互关系；
- h) 提供映射关系，证实设计中描述的所有行为能映射到调用它的安全功能接口。

7.3.4.3 第三级安全保障要求

开发者应向评估者提供产品设计文档：

- a) 根据子系统描述产品结构；
- b) 根据模块描述安全功能；
- c) 标识产品安全功能的所有子系统；
- d) 描述每一个产品安全功能子系统；
- e) 描述安全功能所有子系统间的交互关系；
- f) 提供映射关系，证实设计中描述的所有行为能映射到调用它的安全功能接口；
- g) 提供安全功能子系统到模块间的映射关系；
- h) 描述每一个安全功能要求执行模块，包括其目的及与其他模块间的交互关系；
- i) 描述每一个安全功能要求执行模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的交互关系及调用的接口；
- j) 描述所有安全功能要求的支撑或无关模块，包括其目的及与其他模块间的交互关系。

7.4 指导性文档

7.4.1 操作用户指南

开发者应向评估者提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应符合以下要求：

- a) 描述在安全处理环境中被控制的用户可访问的功能和权限，包含适当的警示信息；
- b) 描述如何以安全的方式使用产品提供的可用接口；
- c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
- d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
- e) 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
- f) 充分实现安全目的所必须执行的安全策略。

7.4.2 准备程序

开发者应向评估者提供产品及其准备程序，准备程序描述应符合以下要求：

- a) 描述与开发者交付程序相一致的安全接收所交付产品所有必需的步骤；
- b) 描述安全安装产品及安全准备其运行环境必需的所有步骤。

7.5 生存周期管理

7.5.1 配置管理能力

7.5.1.1 第一级安全保障要求

开发者应使用配置管理系统，并向评估者提供配置管理文档：

- a) 为产品的不同版本提供唯一的标识；
- b) 配置管理文档描述用于唯一标识配置项的方法；
- c) 配置管理系统单唯一标识所有配置项。

7.5.1.2 第二级安全保障要求

开发者应使用配置管理系统，并向评估者提供配置管理文档：

- a) 为产品的不同版本提供唯一的标识；
- b) 配置管理文档描述用于唯一标识配置项的方法；
- c) 配置管理系统应唯一标识所有配置项；
- d) 使用配置管理系统对组成产品的所有配置项进行维护；
- e) 配置管理系统应提供措施,使得只能对配置项进行授权变更；
- f) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发产品；
- g) 实施的配置管理与配置管理计划相一致。

7.5.1.3 第三级安全保障要求

开发者应使用配置管理系统,并向评估者提供配置管理文档：

- a) 为产品的不同版本提供唯一的标识；
- b) 提供配置管理文档,配置管理文档描述用于唯一标识配置项的方法；
- c) 配置管理系统唯一标识所有配置项；
- d) 使用配置管理系统对组成产品的所有配置项进行维护；
- e) 配置管理系统提供自动化的措施,使得只能对配置项进行授权变更；
- f) 配置管理系统采用自动方式保障产品的生产；
- g) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发产品；
- h) 实施的配置管理与配置管理计划相一致；
- i) 配置管理计划描述用来接受修改或新建配置项作为产品组成部分的程序。

7.5.2 配置管理范围

7.5.2.1 第一级安全保障要求

开发者应向评估者提供产品配置清单：

- a) 配置清单包含产品本身、安全保障要求所需的评估证据和产品的组成部分；
- b) 配置清单唯一标识配置项；
- c) 对于每一个安全功能相关的配置项,配置清单注明该配置项的开发者。

7.5.2.2 第二级安全保障要求

开发者应向评估者提供产品配置清单：

- a) 配置清单包含产品本身、安全保障要求所需的评估证据、产品的组成部分和实现表示；
- b) 配置清单唯一标识配置项；
- c) 对于每一个安全功能相关的配置项,配置清单注明该配置项的开发者。

7.5.2.3 第三级安全保障要求

开发者应向评估者提供产品配置清单：

- a) 配置清单包含产品本身、安全保障要求所需的评估证据、产品的组成部分、实现表示、安全缺陷报告及其解决状态；
- b) 配置清单唯一标识配置项；
- c) 对于每一个安全功能相关的配置项,配置清单注明该配置项的开发者。

7.5.3 交付程序

开发者应使用一定的交付程序交付产品,并将交付过程文档化。交付文档应描述,向用户方分发产品的版本时,用以维护安全所必需的所有程序。

7.5.4 开发者环境安全

第二级、第三级要求开发者应向评估者提供开发安全文档。开发安全文档应描述在产品的开发环

境中,为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.5.5 开发生存周期

第二级、第三级要求开发者应建立一个生存周期模型对产品的开发和维护进行必要控制,并向评估者提供生存周期文档,描述用于开发和维护产品的模型。

7.5.6 工具和技术

第三级要求开发者应向评估者提供开发工具文档:

- a) 标识且明确规定用于实现产品的每个开发工具;
- b) 提供每个开发工具选定的实现依赖选项;
- c) 每个开发工具的文档明确规定在实现中使用的所有声明、约定、指示,以及所有实现时所依赖选项的含义。

7.6 测试

7.6.1 测试覆盖

7.6.1.1 第一级安全保障要求

开发者应向评估者提供测试覆盖的证据,测试覆盖的证据应表明测试文档中的测试与功能规范文档中安全功能接口之间的对应性。

7.6.1.2 第二级、第三级安全保障要求

开发者应向评估者提供测试覆盖的证据:

- a) 测试覆盖的证据应表明测试文档中的测试与功能规范文档中安全功能接口之间的对应性;
- b) 测试覆盖的证据应表明上述对应性是完备的,并证实已经对功能规范文档中的所有安全功能接口都进行了测试。

7.6.2 测试深度

第二级、第三级要求开发者应向评估者提供测试深度的分析:

- a) 证实测试文档中的测试与产品设计中的安全功能子系统之间的对应性;
- b) 证实产品设计中的所有安全功能子系统都已经进行过测试。

7.6.3 功能测试

开发者应测试产品安全功能,将结果文档化并向评估者提供测试文档:

- a) 测试文档包括测试计划、测试判定方法和测试结果;
- b) 测试计划标识要执行的测试,并描述执行每个测试的方案,这些方案包括对于其他测试结果的任何顺序依赖性;
- c) 测试判定方法应表明测试成功后的预期输出;
- d) 测试结果和测试判定方法的对比。

7.6.4 独立测试

开发者应向评估者提供一组与其自测安全功能时使用的同等资源,以用于安全功能的抽样测试。

7.7 脆弱性评定

7.7.1 第一级、第二级安全保障要求

开发者应向评估者提供用于测试的产品和产品交付件中包含的第三方部件列表,并识别产品、第三

方部件的潜在脆弱性。基于已标识的潜在脆弱性,产品能抵抗具有基本攻击潜力的攻击者的攻击。

注:抵抗具有基本攻击潜力的攻击者的攻击,需要综合考虑以下五个具体因素:攻击时间、攻击者能力、对产品的了解程度、访问产品的时间或攻击样品数量、使用的攻击设备,详见 GB/T 30270—2024 的 A.8。

7.7.2 第三级安全保障要求

开发者应向评估者提供用于测试的产品和产品交付件中包含的第三方部件列表,并识别产品、第三方部件的潜在脆弱性。基于已标识的潜在脆弱性,产品能抵抗具有**增强型**基本攻击潜力的攻击者的攻击。

注:抵抗具有增强型基本攻击潜力的攻击者的攻击,需要综合考虑以下五个具体因素:攻击时间、攻击者能力、对产品的了解程度、访问产品的时间或攻击样品数量、使用的攻击设备,见 GB/T 30270—2024 的 A.8。

附 录 A
(资料性)
安全功能要求能力说明

根据网络存储的安全覆盖范围、防护机制的严格程度和应对风险能力程度,不同级别网络存储安全功能要求的能力说明见表 A.1。

表 A.1 网络存储安全功能要求能力说明

级别	能力说明	推荐场景
第一级	网络存储的基本安全功能,防范偶然的、非蓄意的威胁,保障设备基本可用性	对网络存储安全要求不高的场景,如小微单位、非核心业务数据存储等
第二级	网络存储的通用安全功能,抵御有一定技术能力的攻击者,防范蓄意的非复杂攻击	对网络存储安全要求较高的场景,如大中型单位、核心业务数据存储等
第三级	网络存储的增强安全功能,抵御持续攻击,保护数据的机密性和完整性	对网络存储安全要求超高的场景,如涉密单位、有特殊安全需求的数据存储等

附 录 B

(资料性)

安全功能要求与安全保障要求对应章条

不同级别安全功能要求的对应章条见表 B.1。

表 B.1 安全功能要求列表

安全功能要求			第一级	第二级	第三级
通用要求			6.2	6.2	6.2
访问安全	访问鉴别		6.3.1	6.3.1	6.3.1
	访问控制		6.3.2	6.3.2	6.3.2
系统安全	设备可靠运行		6.4.1.1	6.4.1.2	6.4.1.3
	设备工作状态监控		6.4.2	6.4.2	6.4.2
	软件及软件运行安全		6.4.3	6.4.3	6.4.3
	系统完整性保护		—	6.4.4.1	6.4.4.2
	安全加固		—	6.4.5	6.4.5
	Web 安全		—	6.4.6	6.4.6
	资源隔离		—	6.4.7	6.4.7
	安全启动		—	—	6.4.8
	硬件可靠性		—	—	6.4.9
数据安全	数据完整性	存储数据的完整性	6.5.1.1.1	6.5.1.1.2	6.5.1.1.3
		传输数据的完整性	—	6.5.1.2.1	6.5.1.2.2
		处理数据的完整性	—	6.5.1.3	6.5.1.3
	数据保密性	数据保密性	6.5.2.1.1	6.5.2.1.2	6.5.2.1.3
		剩余信息保护	—	—	6.5.2.2
	数据可用性	备份与恢复	6.5.3.1.1	6.5.3.1.2	6.5.3.1.2
		防病毒	6.5.3.2	6.5.3.2	6.5.3.2
		数据冗余	6.5.3.3	6.5.3.3	6.5.3.3
		链路断开	—	—	6.5.3.4
		高可用	—	—	6.5.3.5
管理安全	身份管理	身份标识管理	6.6.1.1.1	6.6.1.1.2	6.6.1.1.3
		账号安全管理	6.6.1.2.1	6.6.1.2.2	6.6.1.2.2
		账号权限管理	6.6.1.3	6.6.1.3	6.6.1.3
	身份鉴别	鉴别机制管理	6.6.2.1.1	6.6.2.1.2	6.6.2.1.3
		口令安全管理	6.6.2.2.1	6.6.2.2.2	6.6.2.2.3
		登录身份鉴别	6.6.2.3.1	6.6.2.3.1	6.6.2.3.2
	会话管理		6.6.3.1	6.6.3.2	6.6.3.3
	密码算法		—	—	6.6.4
	安全审计	审计数据产生	6.6.5.1.1	6.6.5.1.2	6.6.5.1.2
		审计数据管理	6.6.5.2.1	6.6.5.2.1	6.6.5.2.2
		审计数据存储	6.6.5.3.1	6.6.5.3.2	6.6.5.3.2
	数字证书管理		6.6.6.1	6.6.6.2	6.6.6.3
密钥管理		6.6.7.1	6.6.7.2	6.6.7.3	
注：“—”表示本级无要求。					

不同级别安全保障要求的对应章条见表 B.2。

表 B.2 安全保障要求列表

安全保障要求		第一级	第二级	第三级
通用要求		7.2	7.2	7.2
开发	安全架构	7.3.1	7.3.1	7.3.1
	功能规范文档	7.3.2.1	7.3.2.2	7.3.2.3
	实现表示	—	—	7.3.3
	产品设计	7.3.4.1	7.3.4.2	7.3.4.3
指导性文档	操作用户指南	7.4.1	7.4.1	7.4.1
	准备程序	7.4.2	7.4.2	7.4.2
生存周期管理	配置管理能力	7.5.1.1	7.5.1.2	7.5.1.3
	配置管理范围	7.5.2.1	7.5.2.2	7.5.2.3
	交付程序	7.5.3	7.5.3	7.5.3
	开发者环境安全	—	7.5.4	7.5.4
	开发生存周期	—	7.5.5	7.5.5
	工具和技术	—	—	7.5.6
测试	测试覆盖	7.6.1.1	7.6.1.2	7.6.1.2
	测试深度	—	7.6.2	7.6.2
	功能测试	7.6.3	7.6.3	7.6.3
	独立测试	7.6.4	7.6.4	7.6.4
脆弱性评定		7.7.1	7.7.1	7.7.2
注：“—”表示本级无要求。				

参 考 文 献

- [1] GB/T 30270—2024 网络安全技术 信息技术安全评估方法
 - [2] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
 - [3] GB/T 43206—2023 信息安全技术 信息系统密码应用测评要求
-

