ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 29240—2024
代替 GB/T 29240—2012

网络安全技术
终端计算机通用安全技术规范

Cybersecurity technology—General security technical specification for terminal computer

2024-10-26 发布　　2025-05-01 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

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 29240—2012《信息安全技术　终端计算机通用安全技术要求与测试评价方法》，与GB/T 29240—2012相比，除编辑性修改外主要技术变化如下：

——增加了“通则”（见第5章）；

——删除了“硬件系统”（见2012年版的4.1.1.1、4.2.1.1、4.3.1.1、4.4.1.1、4.5.1.1）；

——删除了“操作系统”（见2012年版的4.1.1.2、4.2.1.2、4.3.1.2、4.4.1.2、4.5.1.2）；

——删除了“SSOTC自身安全保护”（见2012年版的4.1.2、4.2.2、4.3.2、4.4.2、4.5.2）；

——删除了“密码支持”（见2012年版的4.2.1.3.1、4.3.1.3.1、4.4.1.3.1、4.5.1.3.1）；

——删除了“数据保密性保护”（见2012年版的4.2.1.3.4、4.3.1.3.5、4.4.1.3.7、4.5.1.3.7）；

——删除了“SSOTC管理”（见2012年版的4.1.4、4.2.4、4.3.4、4.4.4、4.5.4）；

——增加了“硬件接口安全”（见6.1.1）；

——增加了“BIOS固件安全”（见6.1.2）；

——增加了“个人信息安全”（见6.1.3）；

——修改了“身份标识与鉴别”（见6.1.4，2012年版的4.2.1.3.3、4.3.1.3.4、4.4.1.3.6、4.5.1.3.6）；

——增加了“访问控制”（见6.1.5）；

——修改了“运行时防护”（见6.1.6，2012年版的4.1.1.3.1、4.2.1.3.2、4.3.1.3.2、4.4.1.3.3、4.5.1.3.3）；

——修改了“安全审计”（见6.1.7，2012年版的4.2.1.3.5、4.3.1.3.6、4.4.1.3.9、4.5.1.3.9）；

——修改了“安全性分析”（见6.1.8，2012年版的4.3.1.3.3、4.4.1.3.4、4.5.1.3.4）；

——修改了“备份和恢复”（见6.1.9，2012年版的4.1.1.3.2、4.2.1.3.6、4.3.1.3.7、4.4.1.3.10、4.5.1.3.10）；

——增加了“可信度量”（见6.1.10）；

——增加了“无线安全”（见6.1.11）；

——增加了“配置基线检查”（见6.1.12）；

——修改了“安全保障要求”（见6.2，2012年版的4.1.3、4.2.3、4.3.3、4.4.3、4.5.3）；

——修改了“测试评价方法”（见第7章，2012年版的第5章）；

——增加了规范性附录“终端计算机安全技术要求分级表”（见附录A）。

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：公安部第三研究所、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术（北京）股份有限公司、启明星辰信息技术集团股份有限公司、西安交大捷普网络科技有限公司、深圳融安网络科技有限公司、蓝象标准（北京）科技有限公司、长扬科技（北京）股份有限公司、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司、亚信科技（成都）有限公司、中国惠普有限公司、浪潮电子信息产业股份有限公司、三六零科技集团有限公司、中孚信息股份有限公司、中科信息安全共性技术国家工程研究中心有限公司、中国电子科技集团公司第十五研究所、腾讯云计算（北京）有限责任公司、北京数安行科技有

限公司、中电科网络安全科技股份有限公司、蓝盾信息安全技术股份有限公司、飞腾信息技术有限公司、北京珞安科技有限责任公司、国网区块链科技(北京)有限公司、华为技术有限公司、大唐高鸿信安(浙江)信息科技有限公司、北京升鑫网络科技有限公司、博智安全科技股份有限公司、广东省信息安全测评中心、东软集团股份有限公司、北京百度网讯科技有限公司、泰康保险集团股份有限公司、北京北信源软件股份有限公司。

本文件主要起草人:李毅、邱梓华、宋好好、胡维娜、王志佳、李谦、李汝鑫、华昌、赵华、梁连燚、韩秀德、何建锋、刘晨、董晶晶、汪敦全、黄超、张运涛、苏振宇、胡建勋、奚乾悦、刘强、王龑、肖会波、张志磊、廖双晓、杨绍波、杨沅伊、刘俊、张亚京、文槿奕、王志宾、宋晓鹏、刘玉红、万淼、肖智中、潘飚、冯彦朝、石竹玉、乔华阳、李实、叶劲宏、刘祥力、郑驰、傅涛、卞建超、谭琳、崔进、郭建领、黄斌杰、杨华。

本文件及其所代替文件的历次版本发布情况为:

——2012 年首次发布为 GB/T 29240—2012;

——本次为第一次修订。

网络安全技术
终端计算机通用安全技术规范

1 范围

本文件规定了终端计算机的通用安全技术要求，并描述了测试评价方法。

本文件适用于指导终端计算机通用安全功能的设计、开发、测试和评价。

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 5271.1—2000 信息技术 词汇 第1部分：基本术语

GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 20272—2019 信息安全技术 操作系统安全技术要求

GB/T 25069 信息安全技术 术语

GB/T 30278—2013 信息安全技术 政务计算机终端核心配置规范

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

GM/T 0012—2020 可信计算 可信密码模块接口规范

3 术语和定义

GB/T 18336.1—2024、GB/T 18336.3—2024、GB/T 5271.1—2000 和 GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

终端计算机 terminal computer

供个人使用的、能独立进行数据处理及提供网络服务访问的计算机。

注1：本文件中的终端计算机不包括移动智能终端(手机、平板电脑)、车载智能终端、智能电视、可穿戴设备等终端设备。

注2：终端计算机通常由硬件系统、操作系统和应用系统(包括为用户访问网络提供支持的工具软件、安全软件和其他应用软件)等部分组成。

3.2

终端计算机安全子系统 security subsystem of terminal computer

终端计算机内安全保护组件的总称，包括硬件、固件、软件和负责执行安全策略的组合体。

注：终端计算机安全子系统建立了一个基本的终端计算机安全保护环境，并提供终端计算机所要求的附加用户服务。终端计算机安全子系统需从硬件系统、操作系统、应用系统和系统运行等方面对终端计算机进行安全保护。

3.3

配置基线　configuration baseline

能够满足终端计算机安全基本要求的一组配置项基值构成的集合。

[来源:GB/T 30278—2013,3.5,有修改]

3.4

完整性度量　integrity measurement

采用密码杂凑算法对被度量对象计算其杂凑值的过程。

[来源:GB/T 29829—2022, 3.11]

3.5

可信度量　trust for measurement

针对 BIOS、操作系统加载器、操作系统内核、可执行程序等的可信完整性度量,包括度量基准值的可信存储。

4　缩略语

下列缩略语适用于本文件:

BIOS:基本输入输出系统(Basic Input Output System)

CPU:中央处理器(Central Processing Unit)

IP:网际协议(Internet Protocol)

MAC:媒体存取控制地址(Media Access Control)

WLAN:无线局域网(Wireless Local Area Network)

5　通则

终端计算机的通用技术要求包括安全功能要求和安全保障要求。安全功能包括硬件接口安全、BIOS 固件安全、个人信息安全、身份标识与鉴别、访问控制、运行时防护、安全审计、安全性分析、备份和恢复、可信度量、无线安全、配置基线检查等 12 项。安全保障要求按照 GB 42250—2022,包括供应链安全、设计与开发、生产和交付、运维服务保障和用户信息保护。

本文件将终端计算机划分为基本级和增强级。基本级终端计算机的安全功能要求包含硬件接口安全、BIOS 固件安全、个人信息安全、身份标识与鉴别、访问控制、运行时防护、安全审计、无线安全,安全保障要求按照 GB 42250—2022 中的基本级要求;增强级终端计算机的安全功能要求除了对基本级的安全功能部分进行必要的增强之外,还增加了安全性分析、数据备份和恢复、可信度量、配置基线检查要求,安全保障要求按照 GB 42250—2022 中的增强级要求。

与基本级内容相比,增强级中要求有所增加或变更的内容在正文中通过**“宋体加粗”**表示。产品基本级、增强级的划分应符合附录 A。

6　安全技术要求

6.1　安全功能要求

6.1.1　硬件接口安全

终端计算机的硬件接口安全要求如下:

a)　应对外部硬件接口进行明示,不应存在未明示的外部硬件调试接口;

b)　如果终端计算机配备有摄像头模块,宜具备物理开关来关闭或遮蔽摄像头;

c） **如果终端计算机配备有摄像头模块，应具备物理开关来关闭或遮蔽摄像头；**

d） **如果终端计算机配备有录音模块，宜具备物理开关来禁用录音模块。**

注：明示的形式包括在产品说明书、官方网站或设备机身等处进行说明。

6.1.2 BIOS 固件安全

终端计算机的 BIOS 固件安全要求如下：

a） 应具备对 BIOS 固件升级包进行完整性校验的功能，校验通过后才能进行升级；

b） **应具备对 BIOS 固件升级包进行基于数字证书的完整性校验的功能，校验通过后才能进行升级；**

c） BIOS 固件升级失败时，应完整、自动恢复到升级前的固件版本；

d） **BIOS 固件及其升级包的不同版本应具备唯一性标识；**

e） **应有明确的信息告知用户 BIOS 固件更新过程的开始、结束以及更新的内容。**

6.1.3 个人信息安全

若终端计算机存在采集个人生物识别信息（包括：指纹、声纹、人脸、虹膜等识别数据）的情况，应满足 GB/T 35273—2020 第 5 章中的要求。

6.1.4 身份标识与鉴别

终端计算机的身份标识与鉴别功能要求如下。

a） **BIOS 身份鉴别：**

在登录 BIOS 设置界面时应采用口令或其他方式进行 BIOS 身份鉴别。

b） 操作系统用户身份标识与鉴别。

1） 应采用账户口令或其他方式对操作系统用户进行身份鉴别。

2） 若采用账户口令方式，则不准许空口令账户登录系统，并应明示口令长度要求、复杂度要求；用户设置口令或修改口令时，应满足长度要求、复杂度要求。

3） **若采用账户口令方式，口令应至少包含：数字、小写字母、大写字母、特殊字符 4 类中的 3 类，口令长度至少 8 位。用户设置口令或修改口令时，应明示口令长度要求、复杂度要求。**

4） **应采用账户口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对操作系统用户进行身份鉴别。如果采用了密码模块，密码模块应至少满足 GB/T 37092—2018 中“安全一级”的要求。**

5） 应能配置操作系统用户身份鉴别失败次数。用户鉴别失败达到限制次数后，应采取锁定用户账户或其他安全措施限制用户登录系统。

6） 应禁止操作系统用户开机自动登录操作系统。

7） **对于远程登录失败，应对远程登录的用户标识（如访问的 IP 地址）进行锁定，并且只能由系统管理员恢复该用户的访问权限。**

c） 操作系统用户身份标识与鉴别信息的修改与存储。

1） 应能禁用操作系统的默认账户或将默认账户更改成其他名称。

2） 应采取措施对操作系统用户身份鉴别信息进行存储保护。

3） **应限制口令的最长使用期限。用户在更改口令时应能禁止重复使用原口令。**

d） 操作系统用户超时退出：

操作系统用户身份鉴别成功登录系统后，当其空闲操作的时间超过设定值后，在该用户需要执行操作前，应重新进行身份鉴别。

e） **应用软件标识：**

终端计算机中的应用软件，应有唯一性标识。

6.1.5 访问控制

6.1.5.1 本地访问控制

终端计算机的本地访问控制功能要求如下：

a) 应对操作系统的系统文件、系统目录进行保护，防止未授权修改、删除；

b) 宜按照 GB/T 20272—2019 中 6.31.3a)、b)、c)、d)的要求，对终端计算机中的文件、目录、进程等客体进行强制访问控制。

6.1.5.2 网络访问控制

终端计算机的网络访问控制功能要求如下：

a) 默认状态下应仅开启必要的服务和对应的端口，应明示所有默认开启的服务、对应的端口及用途；

b) 应能关闭默认开启的服务和对应的端口；

c) 非默认开放的端口和服务，应在用户知晓同意后才可启用；

d) 可设置为默认状态下拒绝所有外部主机/网络对本主机的网络访问；

e) 应能基于应用程序的白名单，对本主机访问外部网络进行访问控制；

f) 应能基于 IP 地址、端口号进行网络访问控制；

g) 应能基于源 IP 地址、目的 IP 地址、目的端口号、协议进行网络访问控制。

6.1.6 运行时防护

6.1.6.1 漏洞修复

终端计算机的漏洞修复功能要求如下：

a) 应能对操作系统、应用程序安装补丁程序，修复系统漏洞；

b) 应能获取操作系统最新的安全补丁安装包，并对安全补丁安装包的来源、完整性进行验证，验证成功后才允许安装升级；

c) 应能支持应用程序安全补丁的安装升级，并对操作系统自带应用程序的升级程序的来源、完整性进行验证。

6.1.6.2 恶意代码防护

终端计算机的恶意代码防护功能要求如下：

a) 应能对恶意代码查杀；

b) 应能在不连接互联网的环境下实现恶意代码防护；

c) 应能定期在线更新特征库；

d) 应能定期在不连接互联网的环境下更新特征库；

e) 应能对文件系统和接入的移动存储介质进行恶意代码查杀，并根据查杀结果采取相应措施，如清除或隔离。

6.1.6.3 外设防护

终端计算机的外设防护功能要求如下：

a) 应能对外部移动设备接入终端计算机的权限进行管理，并基于设备授权情况进行注册、读写等操作的控制，设备类型包括但不限于 U 盘、移动硬盘等；

b) 在未授权外部移动设备接入时应能告警，并生成审计日志。

6.1.6.4 资源监测

终端计算机的资源监测功能要求如下：

a) 应能对系统的 CPU、内存、硬盘、网卡等资源的使用情况进行监测；

b) 应能对运行中进程的使用资源情况进行监测；

c) **应具有资源告警阈值，并能对资源不足的情况进行告警。**

6.1.7 安全审计

终端计算机的安全审计功能要求如下。

a) 应能审计用户的操作行为，至少包含以下事件：

1) 用户的登录和注销、关机；

2) 系统安全事件，如：网络访问控制事件、恶意代码防护事件等；

3) 系统管理员的所有操作；

4) **用户口令修改；**

5) **未授权外部移动设备接入；**

6) **访问控制相关事件；**

7) **用户权限的更改；**

8) **软件安装记录。**

b) 审计记录应至少包括以下内容：

1) 事件发生日期和时间；

2) 用户名；

3) 事件描述(包括类型、操作内容)；

4) 事件成功或失败；

5) **IP 地址、MAC 地址或主机名(采用远程管理方式时)。**

c) **应能设置审计存储空间的阈值，当审计存储空间达到阈值时，应产生告警信息。**

d) **应能通过配置日志服务器等方式进行日志外发，并能定期自动转存审计数据。**

e) **应提供对审计记录的统计、查询功能，包括按时间范围、用户名、客体名称、事件等条件进行检索查询，并应具有生成审计结果报告的能力。**

f) **应确保审计记录的完整性，禁止非授权修改、删除。**

6.1.8 安全性分析

6.1.8.1 操作系统安全分析

终端计算机在开机运行状态下应具备以下操作系统安全分析功能：

a) **分析文件许可、文件宿主、网络服务设置、账户设置、程序真实性等，以及与用户相关的安全风险等，发现存在的脆弱性；**

b) **对终端计算机中的各类系统文件、审计日志文件等进行完整性检测。**

6.1.8.2 硬件系统安全分析

终端计算机在开机运行状态下应能对终端计算机硬件系统进行分析，包括硬件变更等。

6.1.8.3 应用程序安全分析

在应用程序初始安装时，终端计算机应采用签名验证等方式确保应用程序的来源可靠。

6.1.9 备份和恢复

6.1.9.1 数据备份

应能对终端计算机及其存储的文件进行备份。备份方式应包括：完全备份、增量备份、差量备份。

6.1.9.2 数据恢复

应在数据恢复过程中保障数据的安全，恢复方式应包括：完全恢复、个别文件恢复、重定向恢复。

6.1.10 可信度量

终端计算机的可信度量功能要求如下。

a) 终端计算机开机启动时应对 BIOS 进行完整性度量。如果完整性度量失败，应能恢复到可信的 BIOS。
b) 在操作系统加载器加载时，应对操作系统加载器进行完整性度量。
c) 在操作系统启动时，应对操作系统内核进行完整性度量。
d) 在可执行程序启动时，应对其进行完整性度量。
e) 应对完整性度量基准值进行可信存储，防止其被篡改。
f) 应使用至少满足 GB/T 37092—2018 中“安全一级”的可信计算技术硬件模块作为信任根。如果终端计算机使用可信密码模块作为信任根，则可信密码模块应符合 GM/T 0012—2020 的要求。

6.1.11 无线安全

如果终端计算机具有无线功能，则无线安全功能要求如下：

a) 终端计算机应支持开启和关闭无线通信功能；
b) 终端计算机在未经用户允许的情况下，禁止在后台自动开启无线通信功能；
c) 终端计算机应在无线通信状态发生变化时通知用户；
d) 终端计算机宜支持使用自定义或硬件随机 MAC 地址连接无线通信。

6.1.12 配置基线检查

终端计算机在开机运行状态下，宜按照 GB/T 30278—2013 第 6 章的要求或者定制的配置基线要求，对终端计算机的配置进行基线检查。

6.2 安全保障要求

6.2.1 供应链安全

产品应符合 GB 42250—2022 中 6.1 规定的供应链安全要求。

6.2.2 设计与开发

6.2.2.1 通用要求

产品提供者应符合 GB 42250—2022 中 6.2 规定的设计与开发要求。

6.2.2.2 安全设计

开发者应提供产品安全功能和自身安全功能的设计文档，应满足以下要求：

a) 描述产品安全架构设计，并与产品的安全功能和自身安全功能一致；
b) 描述产品采取的自我保护、不可旁路的安全机制；

c) 完整地描述产品的安全功能和自身安全功能；
d) 描述所有安全功能和自身安全功能接口的目的、使用方法及相关参数；
e) 标识和描述产品安全功能和自身安全功能的所有子系统，并描述子系统间的相互作用；
f) 提供子系统和安全功能接口间的对应关系；
g) 通过实现模块描述安全功能，标识和描述实现模块的目的、相关接口及返回值等，并描述实现模块间的相互作用及调用的接口；
h) 提供实现模块和子系统间的对应关系。

6.2.2.3 实现表示

开发者应为全部安全功能提供实现表示，应满足以下要求：
a) 实现表示应按详细级别定义产品安全功能，且详细程度达到无须进一步设计就能生成产品安全功能的程度；
b) 实现表示应以开发人员使用的形式提供；
c) 设计描述与实现表示示例之间的映射应能证明它们的一致性。

6.2.2.4 配置管理

开发者的配置管理能力应满足以下要求：
a) 使用配置管理系统对组成产品的所有配置项进行维护；
b) 建立维护配置项列表，包括产品评估证据和产品组成部分；
c) 配置管理系统提供一种自动方式来支持产品的生产，通过该方式确保只能对产品的实现表示进行已授权的改变；
d) 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；
e) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

6.2.2.5 指导性文档

开发者应提供操作用户指南和准备程序，应满足以下要求：
a) 描述用户可访问的功能和特权，包含适当的警示信息；
b) 描述用户以安全方式使用产品提供的可用接口；
c) 描述产品安全功能及接口的用户操作方法，包括配置参数的安全值等；
d) 标识和描述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；
e) 描述实现产品安全目的所需执行的安全策略；
f) 描述安全安装产品及其运行环境必需的所有步骤。

6.2.2.6 安全测试

开发者对产品进行安全测试，应满足以下要求：
a) 测试文档描述所有测试项与安全设计文档中所描述产品的安全功能和自身安全功能间的对应性；
b) 测试文档所标识的测试项与安全设计中产品安全功能接口间的对应性，并证实所有安全功能接口都进行了测试；
c) 测试文档描述所有测试项的测试计划和执行方案，方案包括如测试条件、测试步骤、预期结果和实际结果等内容；
d) 基于已标识潜在脆弱性，产品能够抵抗具备基本攻击潜力的攻击者的攻击；
e) 基于已标识潜在脆弱性，产品能够抵抗具备中等攻击潜力的攻击者的攻击。

6.2.3 生产和交付

产品提供者应符合 GB 42250—2022 中 6.3 规定的生产和交付要求。

6.2.4 运维服务保障

产品提供者应符合 GB 42250—2022 中 6.4 规定的运维服务保障要求。

6.2.5 用户信息保护

产品提供者应符合 GB 42250—2022 中 6.5 规定的用户信息保护要求。

7 测试评价方法

7.1 总体说明

测评方法与安全技术要求一一对应，它给出具体测评方法来验证终端计算机产品是否达到安全技术要求中所提出的要求，主要由测评内容、预期结果和结果判定构成。

7.2 测试环境

测试环境参见图 1。其中无线路由器、蓝牙设备用于测试终端计算机的无线安全，端口扫描设备、主机 1 用于对网络访问控制功能进行测试。

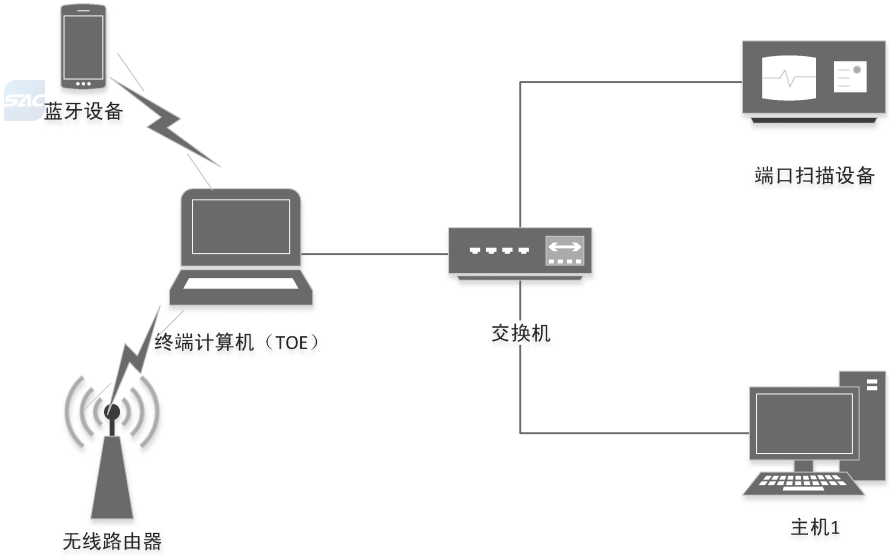

图 1 测试环境图

7.3 安全功能要求测试和评价

7.3.1 硬件接口安全

硬件接口安全的测试评价方法如下。

a) 测评内容：

1) 检验终端计算机是否包含有外部硬件接口；

2) 检验外部硬件接口是否均有明示标记；

3) 检验是否存在未明示的外部硬件调试接口；

4） 检验终端计算机是否配备有摄像头模块，如果配备检验终端计算机是否有物理开关来关闭或遮蔽摄像头；

5） 检验终端计算机是否配备有录音模块，如果配备检验终端计算机是否有物理开关来禁用录音模块。

b） 预期结果：

1） 若终端计算机包含有外部硬件接口，则终端计算机所有外部硬件接口均有明示标记，明示的形式包括在产品说明书、官方网站或设备机身等处进行说明；不存在未明示的外部硬件调试接口；

2） 若终端计算机配备有摄像头模块，则终端计算机应有物理开关来关闭或遮蔽摄像头；

3） 若终端计算机配备有录音模块，则终端计算机应有物理开关来禁用录音模块。

c） 结果判定：

1） 是否有物理开关来禁用录音模块，不作为结果判定要求；

2） 若终端计算机配备有摄像头模块，且实际测试结果与 b）中第 1）条、第 2）条预期结果一致则判定为符合，其他情况判定为不符合；

3） 若终端计算机未配备摄像头模块，且实际测试结果与 b）中第 1）条预期结果一致则判定为符合，其他情况判定为不符合。

7.3.2 BIOS 固件安全

BIOS 固件安全测试评价方法如下。

a） 测评内容：

1） 查看开发者文档是否具有对 BIOS 固件升级包进行完整性校验的方法说明；分别使用完整 BIOS 固件升级包和不完整 BIOS 固件升级包进行验证，查看是否具有完整性校验过程和结果，查看升级是否成功；

2） 查看开发者文档是否具有对 BIOS 固件升级包基于签名证书进行完整性校验的方法说明；分别使用具有数字证书签名的完整 BIOS 固件升级包和不完整 BIOS 固件升级包进行验证，查看是否具有完整性校验过程和结果，查看升级是否成功；

3） 尝试进行 BIOS 固件升级失败的操作，检验终端计算机能否完整、自动恢复到升级前的固件版本，并能够正常启动终端计算机；

4） 尝试定义多个预装 BIOS 固件、升级包的不同版本；尝试添加一个已有标识升级包的版本，检验系统是否提示该标识已存在，是否拒绝具有相同版本升级包的升级；

5） 尝试进行固件更新，检验是否具有明确的信息告知用户更新过程的开始、结束以及更新的内容。

b） 预期结果：

1） 开发者文档具有对 BIOS 固件升级包进行完整性校验的功能，校验通过后才能进行升级；

2） BIOS 固件升级失败时，完整、自动恢复到升级前的固件版本，并能正常启动终端计算机；

3） 预装 BIOS 固件、升级包的不同版本具备唯一性标识，拒绝具有相同版本升级包的升级；

4） 有明确的信息告知用户 BIOS 固件更新过程的开始、结束以及更新的内容。

c） 结果判定：

若终端计算机包含有 BIOS 固件，且实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.3 个人信息安全

个人信息安全测试评价方法如下。

a） 测评内容：

1） 检验终端计算机是否存在采集个人生物识别信息（包括：指纹、声纹、人脸、虹膜等识别数据）的情况；

2） 如果存在以上情况，检验终端计算机是否满足 GB/T 35273—2020 第 5 章中的要求。

b） 预期结果：

若终端计算机存在采集个人生物识别信息（包括：指纹、声纹、人脸、虹膜等识别数据）的情况，则终端计算机满足了 GB/T 35273—2020 第 5 章中的要求。

c） 结果判定：

若终端计算机不采集个人生物识别信息，则本项为不适用。若终端计算机采集个人生物识别信息，且实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.4 身份标识与鉴别

身份标识与鉴别测试评价方法如下。

a） 测评内容。

1） 尝试登录 BIOS，检验是否需要口令或其他方式进行身份鉴别。

2） 若采用账户口令方式，尝试设置账户为空口令，并尝试登录系统。

3） 对采用基于口令作为鉴别信息的系统，在设置或修改账户口令时，检验系统是否明示口令长度要求、复杂度要求，是否对设置的口令进行复杂度、长度检查，是否满足口令复杂度要求。

4） 对采用基于口令作为鉴别信息的系统，在设置或修改账户口令时，检验系统是否对设置的口令进行复杂度、长度检查，是否明示口令长度要求、复杂度要求，是否要求至少包含：数字、小写字母、大写字母、特殊字符 4 类中的 3 类，口令长度至少 8 位。

5） 尝试登录操作系统，检验是否需要进行身份鉴别，明确是否采用账户口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别；分别采用正确的账户名和鉴别信息、正确的账户名和错误的鉴别信息、错误的账户名进行登录尝试。

6） 如果采用了密码模块进行身份鉴别，则开发者应提供密码模块至少满足 GB/T 37092—2018 中“安全一级”的证据材料。

7） 检验系统是否具备鉴别失败处理功能，是否可以定义限制终端计算机身份鉴别失败次数，设置身份鉴别失败次数，尝试多次失败登录，检验达到设置的失败次数后，系统是否采取锁定用户等措施限制用户登录系统。

8） 检验操作系统用户开机时是否自动登录操作系统。

9） 尝试使用远程方式进行多次失败登录，检验系统是否对远程登录的用户标识（如访问的 IP 地址）进行锁定，锁定后尝试使用远程方式以正确的鉴别信息进行登录，检验是否能正常登录系统；以系统管理员身份恢复该用户标识的远程登录权限后，再次使用正确的鉴别信息尝试远程登录。

10） 尝试设置操作系统用户开机自动登录操作系统，检验能否设置成功。

11） 根据终端计算机相关文档的说明，以系统管理员身份登录终端计算机，检验能否禁用默认账户或将默认账户更改成其他名称。

12） 查看开发者文档检验是否具有保证鉴别信息在存储过程中安全所使用的措施的详细说明；查看登录界面修改口令时是否进行遮蔽处理；查看系统后台存储口令文件内容是否进行安全保护，密码是否明文存储。

13） 检验系统是否提供鉴别信息最长使用期限和定期更换功能，当鉴别信息使用时间达到使用期限阈值前，是否提示用户进行修改，修改时尝试设置原口令，检验系统能否禁用原口令。

14） 检验系统是否具有账户登录超时重新鉴别功能，设定账户登录超时重新鉴别的时间间

隔，检验登录账户在设定的时间间隔内没有任何操作的情况后，该用户需要执行操作前，是否需要重新进行系统身份鉴别。

15） 查看终端计算机中的应用软件标识，检验是否唯一。

b） 预期结果。

1） 在登录 BIOS 设置界面时采用口令等方式进行 BIOS 身份鉴别。

2） 系统不准许空口令账户登录系统，账户不准许设置空口令。

3） 对采用基于口令作为鉴别信息的终端计算机，系统明示口令长度要求、复杂度要求，口令满足复杂度、长度的要求。

4） 对采用基于口令作为鉴别信息的终端计算机，在设置或修改账户口令时明示口令长度要求、复杂度要求，并且口令满足复杂度、长度的要求；口令至少包含：数字、小写字母、大写字母、特殊字符 4 类中的 3 类，口令长度至少 8 位。

5） 采用账户口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对操作系统用户进行身份鉴别，且仅在输入正确的账户名和鉴别信息时能够登录系统。

6） 如果采用了密码模块进行身份鉴别，则密码模块至少满足 GB/T 37092—2018 中“安全一级”的要求。

7） 系统具备鉴别失败处理功能，限制终端计算机身份鉴别失败次数，超过限制次数后采取锁定用户或其他安全措施限制用户登录系统。

8） 操作系统用户开机不能自动登录操作系统。

9） 对于远程多次登录失败的用户，系统应对 IP 进行锁定，锁定后无法登录，使用管理员恢复远程登录权限后，可以成功登录。

10） 无法设置操作系统用户开机自动登录操作系统。

11） 终端计算机能够禁用默认账户或将默认账户更改成其他名称。

12） 鉴别信息采取了相应的安全措施进行存储，口令非明文存储。

13） 限制了口令的最长使用期限。用户在更改口令时能禁止使用原口令。

14） 系统具有登录超时重新鉴别功能，系统鉴别成功后，系统账户在设定的时间间隔内没有任何操作的情况下，系统被锁定或终止会话，在该用户需要执行操作前，需要重新进行系统身份鉴别。

15） 终端计算机中的应用软件，有唯一性标识。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.5 访问控制

7.3.5.1 本地访问控制

本地访问控制测试评价方法如下。

a） 测评内容。

1） 尝试以普通用户身份对操作系统的系统文件、系统目录进行修改、删除，检验能否操作成功。

2） 尝试对操作系统的系统文件、系统目录进行未授权的修改、删除，检验能否操作成功。

3） 查看开发者文档，检验终端计算机的操作系统，是否满足 GB/T 20272—2019 6.3.1.3 中 a）、b）、c）、d）的要求；如果满足，尝试对终端计算机中的文件、目录、进程等客体进行强制访问控制，检验强制访问控制策略能否生效。

b） 预期结果。

1） 终端计算机对操作系统的系统文件、系统目录进行保护，能够防止未授权修改、删除。

2） 能够按照 GB/T 20272—2019 6.3.1.3 中 a）、b）、c）、d）的要求，对终端计算机中的文件、目

录、进程等客体进行强制访问控制。

c） 结果判定。

强制访问控制功能要求不作结果判定。实际测试结果与 b）中第 1）条预期结果一致则判定为符合，与 b）中第 1）条预期结果不一致判定为不符合。

7.3.5.2 网络访问控制

网络访问控制测试评价方法如下。

a） 测评内容。

1） 登录终端计算机，输入命令或打开设置页面查看开放的端口和服务。

2） 根据终端计算机相关文档的说明，查找业务所需的端口和服务。

3） 登录终端计算机，检验能否关闭默认开启的服务和对应的端口。

4） 尝试开启非默认开放的服务和对应端口，检验系统是否在用户知晓同意后才开启非默认开放的服务和对应端口。

5） 设置终端计算机为默认状态下，拒绝外部主机访问本主机的开放端口。在默认状态下，从外部主机尝试访问本主机的开放端口，检验能否访问成功。

6） 设置基于应用程序的白名单，通过白名单内的应用程序访问外部网络，检验能否访问成功。通过不在白名单内的应用程序访问外部网络，检验能否访问成功。

7） 打开终端计算机的网络访问控制功能模块，设置基于 IP 地址或 IP 地址段、端口的访问外部网络的控制策略。

8） 打开终端计算机的网络访问控制功能模块，设置基于源 IP 地址、目的 IP 地址、目的端口号、协议的访问控制策略。

9） 尝试进行网络访问，查看访问结果符合预先设定的访问控制策略。

b） 预期结果。

1） 终端计算机文档明确了默认开启的服务、对应的端口以及用途。

2） 经查看，系统仅开启了必要的端口和服务。

3） 能关闭默认开启的服务和对应的端口。

4） 在用户知晓同意后才可以开启非默认开放的端口和服务。

5） 在默认状态下，拒绝外部主机访问本主机的开放端口。

6） 只有白名单内的应用程序，才能访问外部网络。

7） 网络访问控制功能模块能够基于 IP 地址、端口进行网络访问控制。

8） 网络访问控制功能模块能够基于源 IP 地址、目的 IP 地址、目的端口号、协议进行网络访问控制。

9） 访问结果符合预先设定的访问控制策略。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.6 运行时防护

7.3.6.1 漏洞修复

漏洞修复测试评价方法如下。

a） 测评内容。

1） 根据终端计算机相关文档的说明，检验能否支持对终端计算机的操作系统、应用程序进行补丁更新。

2） 根据终端计算机文档对终端计算机的操作系统、应用程序更新补丁。

3） 根据终端计算机相关文档的说明，检验能否获取操作系统最新补丁安装包，并对补丁安装

包的来源、完整性进行验证。

4） 对来源合法、完整的操作系统补丁安装包进行验证，验证成功后安装该补丁安装包，检验能否安装成功。

5） 对来源不合法或完整受到破坏的操作系统补丁安装包进行验证，检验能否验证成功。

6） 尝试安装来源不合法或完整受到破坏的操作系统补丁安装包，检验能否安装成功。

7） 根据终端计算机相关文档的说明，检验能否支持应用程序安全补丁的安装升级，并对操作系统自带应用程序的升级程序的来源、完整性进行验证。

8） 对来源合法、完整的应用程序安全补丁进行验证，验证成功后安装该补丁程序，检验能否安装成功。

9） 对来源不合法或完整受到破坏的应用程序安全补丁进行验证，检验能否验证成功。

10） 尝试安装来源不合法或完整受到破坏的应用程序安全补丁，检验能否安装成功。

b） 预期结果。

1） 终端计算机能够对终端计算机的操作系统进行补丁更新。

2） 终端计算机能获取操作系统最新的安全补丁安装包，并对安全补丁安装包的来源、完整性进行验证，验证成功后才允许安装升级。

3） 终端计算机支持应用程序安全补丁的安装升级，并对操作系统自带应用程序的升级程序的来源、完整性进行验证，验证不通过将拒绝安装、升级。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.6.2 恶意代码防护

恶意代码防护的测试评价方法如下。

a） 测评内容。

1） 根据终端计算机相关文档的说明，检验能否对恶意代码进行查杀。

2） 根据终端计算机相关文档的说明，检验能否在不连接互联网的环境下实现恶意代码防护。

3） 根据终端计算机相关文档的说明，检验能否支持特征库的定期更新。

4） 根据终端计算机相关文档的说明，检验能否支持在不连接互联网的环境下对特征库进行定期更新。

5） 开启恶意代码保护功能，尝试对计算机文件和接入的移动存储介质进行特征码扫描。

6） 查看扫描结果，尝试隔离或清除恶意代码。

b） 预期结果。

1） 能对恶意代码查杀。

2） 能在不连接互联网的环境下实现恶意代码防护。

3） 特征库能够定期在线更新。

4） 特征库能够在不连接互联网的环境下进行定期更新。

5） 能对文件系统和接入的移动存储介质采用特征码扫描，并根据扫描结果采取相应措施，清除或隔离恶意代码。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.6.3 外设防护

外设防护的测试评价方法如下。

a） 测评内容：

1） 根据终端计算机相关文档的说明，检验能否支持对移动设备接入终端计算机的权限进行

管理，并基于设备授权情况进行注册、读写等操作的控制；

2） 接入已授权的 U 盘、移动硬盘，检验能否支持对 U 盘、移动硬盘等多种移动设备管控；

3） 接入未授权的 U 盘、移动硬盘，检验能否生成告警信息并产生日志。

b） 预期结果：

1） 终端计算机能对移动设备接入终端计算机的权限进行管理，并基于设备授权情况进行注册、读写等操作的控制；

2） 终端计算机能对 U 盘、移动硬盘等多种移动设备管控；

3） 未授权设备接入时能生成告警信息并产生审计日志。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.6.4 资源监测

资源监测的测试评价方法如下。

a） 测评内容：

1） 在终端计算机上打开资源监测功能模块，检验终端计算机系统是否提供对 CPU、内存、硬盘、网卡等资源的使用情况的监测方式；

2） 在终端计算机上打开资源监测功能模块，检验终端计算机系统能否对运行中进程的使用资源情况进行监测；

3） 设置资源告警阈值，或者使用系统默认的告警阈值，尝试产生资源不足的情况，检验终端计算机系统是否能对资源不足的情况进行告警。

b） 预期结果：

1） 终端计算机能够对 CPU、内存、硬盘、网卡等资源的使用情况进行监测；

2） 终端计算机能够对运行中进程使用资源的情况进行监测；

3） 终端计算机具有资源告警阈值，能够对资源不足的情况进行告警。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.7 安全审计

安全审计的测试评价方法如下。

a） 测评内容。

1） 以系统管理员身份、普通用户身份在终端计算机中进行至少以下操作：用户本地和远程登录、用户注销、系统开机、关机、用户口令修改、未授权外部移动设备接入、成功和失败的访问控制操作、用户权限更改、软件安装、系统管理操作（如：用户的创建和删除等）、系统安全事件操作（如：发现恶意代码等）。

2） 以授权用户或系统管理员的身份查阅审计记录，检验是否对执行的操作和如下事件产生了审计记录：

——用户的登录和注销、关机；

——系统安全事件，如：网络访问控制事件、恶意代码防护事件等；

——系统管理员的所有操作；

——用户口令修改；

——未授权外部移动设备接入日志；

——访问控制相关事件；

——用户权限的更改；

——软件安装记录。

3） 查看审计记录中是否包括以下记录：

——事件发生日期和时间；

——用户名；

——事件描述(包括类型、操作内容)；

——事件成功或失败；

——IP 地址、MAC 地址或主机名(采用远程管理方式时)。

4） 设置审计存储空间的阈值，验证当审计存储空间达到阈值时，检验是否产生告警信息。

5） 验证能否通过配置日志服务器等方式进行日志外发，并定期自动转存审计数据。

6） 验证是否能够按照一定条件，包括时间范围、用户名、客体名称、事件等对审计记录进行检索查询和统计，并能生成审计结果报告。

7） 验证是否能通过技术手段保护审计记录，避免受到未授权的删除。

b） 预期结果。

1） 能审计用户的操作行为，至少包含以下事件：

① 用户的登录和注销、关机；

② 系统安全事件；

③ 系统管理员的所有操作。

④ 用户口令修改；

⑤ 未授权外部移动设备接入日志；

⑥ 访问控制相关事件；

⑦ 用户权限的更改；

⑧ 软件安装记录。

2） 每个审计记录中均包含以下信息：

① 事件发生日期和时间；

② 用户名；

③ 事件描述(包括类型、操作内容)；

④ 事件成功或失败；

⑤ IP 地址、MAC 地址或主机名(采用远程管理方式时)。

3） 能设置审计存储空间的阈值，当审计存储空间达到阈值时，能够产生告警信息。

4） 能够通过配置日志服务器等方式进行日志外发，并能定期自动转存审计数据。

5） 能够对审计记录进行统计、查询，包括按时间范围、用户名、客体名称、事件等条件进行检索查询，并能够生成审计结果报告。

6） 能够确保审计记录的完整性，禁止非授权修改、删除。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.8 安全性分析

7.3.8.1 操作系统安全分析

操作系统安全分析的测试评价方法如下。

a） 测评内容：

1） 检验终端计算机是否具备操作系统安全分析功能，能否在开机运行状态下分析文件许可、文件宿主、网络服务设置、账户设置、程序真实性等，以及与用户相关的安全风险等，发现操作系统存在的脆弱性；

2） 验证终端计算机能否在开机运行状态下对终端计算机中的各类文件(如系统文件、审计日志等)进行完整性检测。

b） 预期结果：

1） 终端计算机具备操作系统安全分析功能，能够在开机运行状态下分析文件许可、文件宿主、网络服务设置、账户设置、程序真实性等，以及与用户相关的安全风险等，进而发现操作系统存在的脆弱性；

2） 能够在开机运行状态下对终端计算机中的各类系统文件、审计日志文件等进行完整性检测，即检测出文件的完整性是否被破坏。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.8.2 硬件系统安全分析

硬件系统安全分析的测试评价方法如下。

a） 测评内容：

检验终端计算机在运行状态，是否具备硬件系统安全分析功能，能否分析硬件变更等。

b） 预期结果：

终端计算机在运行状态具备硬件系统安全分析功能，能够分析硬件变更等。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.8.3 应用程序安全分析

应用程序安全分析的测试评价方法如下。

a） 测评内容：

1） 在应用程序初始安装时，检验终端计算机能否采用签名验证等方式确保应用程序的来源可靠；

2） 尝试安装来源不可靠的应用程序，检验能否安装成功。

b） 预期结果：

终端计算机在应用程序初始安装时，能够采用签名验证等方式确保应用程序的来源可靠。对于来源不可靠的应用程序，终端计算机能够拒绝安装。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.9 备份和恢复

7.3.9.1 数据备份

数据备份的测试评价方法如下。

a） 测评内容：

1） 按终端计算机提供的指导性文档对终端计算机的文件配置备份策略；

2） 分别设置完全备份、增量备份、差量备份等备份方式；

3） 对每种备份方式分别进行验证，是否能按预期的备份方式进行备份。

b） 预期结果：

终端计算机能对终端计算机的文件进行备份，支持完全备份、增量备份、差量备份等备份方式。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.9.2 数据恢复

数据恢复的测试评价方法如下。

a) 测评内容：
   1) 按终端计算机提供的指导性文档对终端计算机的文件配置数据恢复策略；
   2) 分别设置完全恢复、个别文件恢复、重定向恢复等恢复方式；
   3) 验证恢复后的数据是否与备份对象一致且可用。
b) 预期结果：
   终端计算机能进行数据恢复，方式包括：完全恢复、个别文件恢复、重定向恢复。
c) 结果判定：
   实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.10 可信度量

可信度量的测试评价方法如下。

a) 测评内容：
   1) 根据终端计算机相关文档的说明，检验在终端计算机启动时是否对 BIOS 进行完整性度量；
   2) 根据终端计算机相关文档的说明，检验在操作系统加载器加载时，是否对操作系统加载器进行完整性度量；
   3) 根据终端计算机相关文档的说明，检验在操作系统启动时是否对操作系统内核进行完整性度量；
   4) 根据终端计算机相关文档的说明，检验在可执行程序启动时是否进行完整性度量；
   5) 根据终端计算机相关文档的说明，检验终端计算机是否对完整性度量基准值进行可信存储，防止其被篡改；
   6) 根据终端计算机相关文档的说明，检验终端计算机是否使用可信计算技术硬件模块作为信任根，并且检验开发者是否提供了相关证据，证明密码模块至少满足 GB/T 37092—2018 中“安全一级”的要求；
   7) 如果终端计算机使用可信密码模块作为信任根，开发者应提供可信密码模块符合 GM/T 0012—2020 的证据。
b) 预期结果：
   1) 终端计算机开机启动时应对 BIOS 进行完整性度量；
   2) 在操作系统加载器加载时，应对操作系统加载器进行完整性度量；
   3) 在操作系统启动时，应对操作系统内核进行完整性度量；
   4) 可执行程序启动时进行完整性度量；
   5) 对完整性度量基准值进行可信存储，防止其被篡改；
   6) 使用可信计算技术硬件模块作为信任根，并且可信计算技术硬件模块至少满足 GB/T 37092—2018 中“安全一级”的要求；
   7) 如果终端计算机使用可信密码模块作为信任根，则可信密码模块符合 GM/T 0012—2020 的相关要求。
c) 结果判定：
   实际测试结果与上述预期结果一致则判定为符合，其他情况判定为不符合。

7.3.11 无线安全

无线安全测试评价方法如下。

a) 测评内容：
   1) 根据终端计算机相关文档的说明，分别开启和关闭蓝牙、WLAN 等无线通信功能，检测能否操作成功；

2） 尝试在无线通信功能关闭状态下，未经用户允许在后台开启蓝牙、WLAN 等无线通信功能，检测能否操作成功；

3） 改变终端计算机的无线通信状态（如：连接、断开无线通信），检测终端计算机能否在无线通信状态发生变化时通知用户；

4） **根据终端计算机相关文档的说明，使用自定义或硬件随机 MAC 地址连接无线通信，检测能否操作成功。**

b） **预期结果：**

1） **终端计算机支持开启和关闭蓝牙、WLAN 等无线通信功能；**

2） **终端计算机在无线通信状态发生变化时能够通知用户；**

3） **终端计算机支持使用自定义或硬件随机 MAC 地址连接无线通信。**

c） **结果判定：**

使用自定义或硬件随机 MAC 地址连接无线通信的功能不作为判定条件。实际测试结果与 b）中第 1）条、第 2）条预期结果一致则判定为符合，其他情况判定为不符合。

7.3.12 配置基线检查

配置基线检查的测试评价方法如下：

a） **测评内容：**

1） **根据终端计算机相关文档的说明，分别开启和关闭蓝牙、WLAN 等无线通信功能，检测能否操作成功。**

b） **预期结果：**

1） **终端计算机按照 GB/T 30278—2013 中第 6 章，能够对终端计算机的配置进行基线检查；**

2） **终端计算机能够按照定制的配置基线要求对终端计算机的配置进行基线检查。**

c） **结果判定：**

本项功能不做符合性判定。

7.4 安全保障要求测试和评价

7.4.1 供应链安全

供应链安全的测试评价方法如下。

a） 测评内容。

1） 检查产品提供者是否制定了供应商选择、评定、日常管理等程序。

2） 检查产品提供者是否保存对供应商选择、评价和日常管理的记录。

3） 检查相应程序是否对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出管理要求，以确保供应商提供的关键部件能够满足安全要求。

4） 检查产品提供者是否建立程序或控制机制，确保供应链各环节核心要素的追溯能力，以保障核心要素供应稳定。

5） 检查产品提供者是否制定持续开展安全意识和技能培训的程序。

6） 检查是否保存了相关培训记录。

b） 预期结果。

1） 产品提供者制定了供应商选择、评定、日常管理等程序；保存了对供应商选择、评价和日常管理的记录；相应程序对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出了管理要求。

2） 产品提供者建立了程序或控制机制，确保供应链各环节核心要素的追溯能力；针对产品提供者和产品特点，列举所保障的核心要素（如，核心技术知识产权、工具及部件等）。

3） 产品提供者制定了持续开展安全意识和技能培训的程序；保存了相关培训记录。

c) 结果判定。

实际测试结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2 设计与开发

7.4.2.1 通用要求

通用要求的测试评价方法如下。

a) 测评内容。

1) 检查产品提供者是否针对产品制定了安全开发的制度和流程，检查相关内容是否包括产品开发过程的安全策略、安全风险分析和威胁建模；检查是否至少包括代码编写规范、研发环境安全管理制度、研发人员安全管理制度、研发交付制度等安全开发制度及流程，以确保开发环境安全。

2) 检查产品提供者是否制定了产品的安全设计文档，检查其中是否包括产品安全功能和自身安全功能的设计内容；检查设计文档的描述，是否与安全功能和自身安全功能保持一致。

3) 检查产品提供者提供的配置管理文档和描述，是否制定了产品标识的命名规则，并确认具备唯一性标识；检查内容是否为配置项制定了命名规则，并确定唯一标识；检查是否建立并维护配置项列表。

4) 检查产品提供者的产品相关设计文档或产品指导性文档，是否明确描述产品的功能模块、接口，并阐述未设置恶意程序、隐蔽接口或未明示功能模块等；检查是否通过用户协议、产品说明书等途径将所有功能模块、接口等告知用户。

5) 检查产品提供者是否对产品进行了安全性测试并提供相应的测试文档；检查测试文档的内容是否包括漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证等。

b) 预期结果。

1) 产品提供者制定了安全开发的制度和流程，其中内容包括产品开发过程的安全策略、安全风险分析和威胁建模；包括了代码编写规范、研发环境安全管理制度、研发人员安全管理制度、研发交付制度等安全开发制度及流程，以确保开发环境安全。

2) 产品提供者制定了产品安全功能和自身安全功能的设计文档；设计文档的描述，能够与安全功能和自身安全功能保持一致。

3) 产品提供者能够提供配置管理文档，并制定了产品标识的命名规则和确定唯一性标识；建立了产品配置项命名规则并确定唯一标识；能够建立并维护配置项列表，配置项至少包括源代码、工具、文档、组件、配置信息等。

4) 产品提供者的产品相关设计文档或指导性文档，能够明确描述产品的功能模块、接口，并阐述未设置恶意程序、隐蔽接口或未明示功能模块等；能够通过用户协议、产品说明书等途径将所有功能模块、接口等告知用户。

5) 产品提供者对产品进行了安全性测试并提供相应的测试文档；测试文档的内容包括漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证等。

c) 结果判定。

实际测试结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2.2 安全设计

安全设计的测试评价方法如下。

a) 测评内容：

检查安全架构、功能规范或产品设计文档是否准确描述如下内容：

1) 描述产品安全架构设计，并与产品的安全功能和自身安全功能一致；

2） 描述产品采取的自我保护、不可旁路的安全机制；
3） 完整地描述产品的安全功能和自身安全功能；
4） 描述所有安全功能和自身安全功能接口的目的、使用方法及相关参数；
5） 标识和描述产品安全功能和自身安全功能的所有子系统，并描述子系统间的相互作用；
6） 提供子系统和安全功能接口间的对应关系；
7） 通过实现模块描述安全功能，标识和描述实现模块的目的、相关接口及返回值等，并描述实现模块间的相互作用及调用的接口；
8） 提供实现模块和子系统间的对应关系。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2.3 实现表示

实现表示的测试评价方法如下。

a） 测评内容：
产品设计文档是否准确描述如下内容：
1） 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；
2） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
3） 以开发人员使用的形式提供。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2.4 配置管理

配置管理的测试评价方法如下。

a） 测评内容：
1） 检查开发者是否建立了配置管理系统对配置项进行了维护；
2） 检查配置项列表，确认是否包括产品全部配置项；
3） 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
4） 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。实施的配置管理与配置管理计划相一致；
5） 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

b） 预期结果：
开发者提供的文档内容应满足上述要求。

c） 结果判定：
实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2.5 指导性文档

指导性文档的测试评价方法如下。

a） 测评内容：
检查开发者提供的操作用户指南证据，并检查开发者提供的信息是否满足证据的内容和形式

的所有要求：

1） 产品提供者的产品相关文档，能够明确描述产品的功能模块、接口，并阐述未设置恶意程序、隐蔽接口或未明示功能模块等；

2） 描述用户可访问的功能和特权，包含适当的警示信息；

3） 描述如何以安全的方式使用产品提供的可用接口；

4） 是否描述产品安全功能及接口的用户操作方法，包括配置参数的安全值；

5） 是否标识和描述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；

6） 是否描述实现产品安全目的必需执行的安全策略；

7） 是否提供准备程序，描述安全安装产品及其运行环境必需的所有步骤。

b） 预期结果：

开发者提供的文档内容应满足上述要求。

c） 结果判定：

实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.2.6 安全测试

安全测试的测试评价方法如下。

a） 测评内容：

1） 检查开发者提供的测试覆盖文档，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；

2） 检查测试文档是否描述所有测试项与安全设计文档中所描述产品的安全功能和自身安全功能间的对应性；

3） 检查测试文档是否描述了所标识的测试项与安全设计中产品安全功能接口间的对应性，并证实所有安全功能接口都进行了测试；

4） 检查测试文档是否描述所有测试项的测试计划和执行方案，方案包括如测试条件、测试步骤、预期结果和实际结果等内容；

5） 对从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对产品进行脆弱性分析，判断产品是否能够抵抗具有基本型攻击；

6） 对从用户可能破坏安全策略的明显途径出发，按照安全机制定义的安全强度级别，对产品进行脆弱性分析，判断产品是否能够抵抗具有中等型攻击。

b） 预期结果：

1） 开发者提供的文档内容应满足 a)中 1)～4)要求；

2） 脆弱性分析测试结果表明产品能够抵抗基本型攻击；

3） 脆弱性分析测试结果表明产品能够抵抗中等型攻击。

c） 结果判定：

实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.3 生产和交付

生产和交付的测试评价方法如下。

a） 测评内容。

1） 检查产品提供者建立和执行了产品完整性检测流程规范，检查是否包括能够防范自制或采购的组件被篡改、伪造等风险的措施。

2） 检查产品提供者是否建立了内部交付程序，如设计到研发，研发到测试，测试到集成等内部交付管理流程以及相关安全措施，以确保产品在交付过程中不被破坏或篡改。

3） 检查产品是否提供了外部交付的控制程序，规定产品交付给客户的控制程序以及安全措

施，以确保产品在交付过程中不被破坏或篡改。

4） 检查产品提供者提供的相关文档，是否向用户明示包含在产品中的所有功能模块、外部接口和私有协议，告知用户产品中预置的所有账户和默认口令。

b） 预期结果。

开发者提供的文档内容应满足上述要求。

c） 结果判定。

实际评估结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.4 运维服务保障

运维服务保障的测试评价方法如下。

a） 测评内容。

1） 检查产品提供者提供的相关证据（如用户手册、界面提示、用户协议、说明文档等），检查相关证据是否确定了一个满足法律法规规定或与用户约定的期限，检查相关证据是否表明在该期限内产品提供者为产品提供持续的安全维护，声明不会单方面中断或终止安全维护。

2） 检查产品提供者提供的相关证据（如界面提示、用户通知、说明文档等），检查相关证据是否证实了保护用户对软件（包含固件）安装和升级等的知情权和选择权，是否在安装和升级软件时明示用户并获得用户同意。

3） 检查产品提供者是否建立和执行针对产品安全缺陷、漏洞的应急响应机制和流程（如缺陷纠正工具阐述、缺陷纠正文档、应急响应措施程序等），检查相关文档、证据是否包含对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施，是否表明会及时告知用户安全风险和可用的补救措施，是否明确了向有关主管部门报告机制和流程。

b） 预期结果。

1） 产品提供者能够提供相关证据（如用户手册、界面提示、用户协议、说明文档等），相关证据能够确定一个满足法律法规规定或与用户约定的期限，能够表明在该期限内产品提供者为产品提供持续的安全维护，声明不会单方面中断或终止安全维护。

2） 产品提供者能够提供相关证据（如界面提示、用户通知、说明文档等），相关证据能够证实保护了用户对软件（包含固件）安装和升级等的知情权和选择权，能够在安装和升级软件时明示用户并获得用户同意。

3） 建立和执行了针对产品安全缺陷、漏洞的应急响应机制和流程（如缺陷纠正工具阐述、缺陷纠正文档、应急响应措施程序等），相关文档、证据能够包含对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施，能够表明会及时告知用户安全风险和可用的补救措施，能够明确向有关主管部门报告机制和流程。

c） 结果判定。

实际测试结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

7.4.5 用户信息保护

用户信息保护的测试评价方法如下。

a） 测评内容：

1） 检查产品提供者提供的相关文档或声明，是否明示了收集用户信息的目的、方式、范围、种类、存储位置和处理方式；

2） 检查产品提供者提供的相关文档或声明，是否建立和执行用户信息管理制度和流程；检查制度和流程是否明确阐述在产品设计、生产、升级等各阶段保障用户信息的安全，且不超范围使用用户信息。

b） 预期结果：

1） 产品提供者提供了相关文档或声明，明示了收集用户信息的目的、方式、范围、种类、存储位置和处理方式；

2） 产品提供者提供了相关文档或声明，能够表明建立和执行了用户信息管理制度和流程；制度和流程能够明确阐述在产品设计、生产、升级等各阶段保障用户信息的安全，且不超范围使用用户信息。

c） 结果判定：

实际测试结果与上述预期结果一致则判定为“符合”，其他情况判定为“不符合”。

附 录 A
（规范性）
终端计算机安全技术要求分级表

表 A.1 以表格形式列举了终端计算机基本级、增强级 2 个安全等级的相关技术要求。

表 A.1 终端计算机安全技术要求分级表

序号	安全技术要求			基本级	增强级
1	安全功能要求	硬件接口安全		6.1.1 a)、b)	6.1.1 a)、c)、d)
2		BIOS 固件安全		6.1.2 a)、c)	6.1.2
3		个人信息安全		6.1.3	6.1.3
4		身份标识与鉴别		6.1.4 b)1)、2)、5)、6)、c)1)、c)2)、d)	6.1.4
5		访问控制	本地访问控制	6.1.5.1 a)	6.1.5.1
6			网络访问控制	6.1.5.2 a)、b)、c)、d)、f)	6.1.5.2
7		运行时防护	漏洞修复	6.1.6.1 a)	6.1.6.1
8			恶意代码防护	6.1.6.2 a)、c)、e)	6.1.6.2
9			外设防护	—	6.1.6.3
10			资源监测	6.1.6.4 a)、b)	6.1.6.4
11		安全审计		6.1.7 a)1)、2)、3)、b) 1)、2)、3)、4)	6.1.7
12		安全性分析	操作系统安全分析	—	6.1.8.1
13			硬件系统安全分析	—	6.1.8.2
14			应用程序安全分析	—	6.1.8.3
15		备份和恢复	数据备份	—	6.1.9.1
16			数据恢复	—	6.1.9.2
17		可信度量		—	6.1.10
18		无线安全		6.1.11a)、b)、c)	6.1.11
19		配置基线检查		—	6.1.12
20	安全保障要求	供应链安全		6.2.1	6.2.1
21		设计与开发	通用要求	6.2.2.1	6.2.2.1
22			安全设计	6.2.2.2 a)～f)	6.2.2.2
23			实现表示	—	6.2.2.3
24			配置管理	6.2.2.4 a)、b)	6.2.2.4
25			指导性文档	6.2.2.5	6.2.2.5
26			安全测试	6.2.2.6 a)～d)	6.2.2.6
27		生产和交付		6.2.3	6.2.3
28		运维服务保障		6.2.4	6.2.4
29		用户信息保护		6.2.5	6.2.5

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/Z 24294.4—2017 信息安全技术 基于互联网电子政务信息安全实施指南 第4部分：终端安全防护
[3] GB/T 29829—2022 信息安全技术 可信计算密码支撑平台功能与接口规范
[4] GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
[5] GB/T 32925—2016 信息安全技术 政府联网计算机终端安全管理基本要求
[6] GB/T 34976—2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法
[7] GB/T 34977—2017 信息安全技术 移动智能终端数据存储安全技术要求与测试评价方法
[8] GB/T 35278—2017 信息安全技术 移动终端安全保护技术要求
[9] GB/T 38558—2020 信息安全技术 办公设备安全测试方法
[10] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求