ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX
代替 GB/T 29244—2012，GB/T 38558—2020

信息安全技术 办公设备安全规范

Information security technology—Security specification for office devices

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本稿完成时间：2023-08-25）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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 29244—2012《信息安全技术 办公设备基本安全要求》和GB/T 38558—2020《信息安全技术 办公设备安全测试方法》，与GB/T 29244—2012和GB/T 38558—2020相比，除结构调整和编辑性改动外，主要技术变化如下：

——整合了GB/T 29244—2012和GB/T 38558—2020两项标准的内容，修改标准名称为“信息安全技术 办公设备安全规范”

——增加了概述和规范性附录，明确了办公设备安全等级划分（见第5章、附录A、附录B）

——更改了术语和定义（见第3章，GB/T 29244—2012的第3章）；

——增加了“固件安全”相关要求（见6.1.3）和对应测评方法（见7.1.3）；

——增加了“安全保障要求”和对应测评方法（见6.2和7.2）；

——修改“安全审计”为“日志记录与审计”(见6.1.4，GB/T 29244—2012的4.3)。

——修改“会话”为“通信安全”(见6.1.6，GB/T 29244—2012的4.5)。

——修改“数据管理”为“用户数据安全”(见6.1.5，GB/T 29244—2012的5.2)。

——修改“安全属性管理”为“配置安全”(见6.1.8，GB/T 29244—2012的5.1)。

本文件由全国信息安全标准化技术委员会(SAC/TC260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、珠海奔图电子有限公司、北京大学、爱普生（中国）有限公司、富士胶片商业创新（中国）有限公司、长扬科技（北京）股份有限公司、中国惠普有限公司、联想（北京）有限公司、启明星辰信息技术集团股份有限公司、柯尼卡美能达（中国）投资有限公司、佳能（中国）有限公司、广电计量检测集团股份有限公司、国家办公设备及耗材质量检验检测中心（天津天复检测技术有限公司）、理想（中国）科学工业有限公司、北京高德品创科技有限公司、夏普办公设备（常熟）有限公司、珠海天威飞马打印耗材有限公司、兄弟（中国）商业有限公司、杭州安恒信息技术股份有限公司、东芝泰格信息系统（深圳）有限公司、新华三技术有限公司、北京数安行科技有限公司、北京中科微澜科技有限公司、天津光电通信技术有限公司、中国科学院软件研究所、国网区块链科技（北京）有限公司。

本文件主要起草人：孙彦、杨建军、上官晓丽、李奕希、张东举、彭继兵、张芝军、陈韵然、谢安明、喻梁文、王西子、宫艳雯、祝晴、赵华、杨丰辰、李汝鑫、杨天识、陈挺、杨晨、唐迪、张宇、胡权、王正良、范志国、乔怀信、何钢、陈星、陈勇、万晓兰、刘玉红、郭维、孙芳、晏敏、石竹玉。

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GB/T 29244—2012，2020年首次发布GB/T 38558—2020；

——本次为第一次修订。

信息安全技术 办公设备安全规范

1 范围

本文件规定了办公设备的安全技术要求和测评方法。

本文件适用于办公设备的安全采购、测评、维护和管理。

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 18336 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 18336和GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

办公设备 office device

用于产生或处理电子或其他媒体文件的设备。

注：本文件所指办公设备主要是指具有打印、扫描、传真、复印中的一项或多项功能的设备产品。

3.2

管理员 administrator

被授权管理办公设备的某些部分或所有部分的用户，其行为可能影响安全功能策略。

3.3

用户 user

办公设备之外，与办公设备进行交互的实体（人或信息技术实体）。

3.4

用户数据 user data

由用户创建或为用户而创建，且不影响办公设备安全功能运行的数据。

注：用户数据包括用户文档数据和用户功能数据。

3.5

非易失性存储器 nonvolatile storage

存储的数据不因电源关闭而丢失的装置。

注：非易失性存储器主要包括内置或者外接的硬盘、U盘、SD卡、FLASH。

3.6

固件 firmware

实现办公设备接口通信、安全功能、数据解析、图像处理、引擎控制等的程序。

3.7

主控制芯片 master chip

负责数据解析、图像处理、作业管理和控制打印头并直接输出二进制影像数据的集成电路器件。

3.8

数据控制板 data control board

内置于办公设备，集成了主控制芯片且负责数据控制功能的电路板。

注：数据控制功能包括数据通信，作业分配管理，作业数据解析，打印、复印、扫描数据的图像处理，二进制影像数据的输出控制等。

4 缩略语

下列缩略语适用于本文件。

IP：因特网协议（Internet Protocol）

MAC：媒体访问控制（Media Access Control）

PIN：个人标识码（Personal Identification Number）

SNMP：简单网络管理协议(Simple Network Management Protocol)

5 概述

办公设备的安全技术要求包括安全功能要求和安全保障要求。其中，安全功能要求是对产品应具备的安全功能提出的具体要求。安全保障要求针对产品的生命周期过程提出具体的保障要求。

本文件将办公设备的安全等级分为基本级和增强级。安全功能的强弱，以及安全保障要求的高低是办公设备安全等级划分的依据。办公设备具体安全功能和等级划分应符合附录A的要求，测评方法及等级划分应符合附录B的要求。

6 安全技术要求

6.1 安全功能要求

6.1.1 标识和鉴别

办公设备：

a) 应在执行办公设备功能、安全功能之前对用户身份进行标识和鉴别。

b) 应支持超时锁定功能；支持设定鉴别失败最大次数，超过设定最大次数时，锁定用户账号。

c) 宜支持通过 PIN 方式执行作业，在 PIN 输入的失败次数超过设定的最大次数后锁定作业；提供 PIN 方式执行作业的删除机制，办公设备关机重启后，按删除机制删除作业。

6.1.2 访问控制

办公设备：

a) 应根据管理员、用户使用办公设备功能、安全功能的差异，提供完成各自承担任务所需的最小访问权限。

b) 应支持授权管理功能，支持管理员对用户使用设备进行授权。

c) 应依据访问控制策略，明确授权或拒绝对办公设备功能、用户数据的访问。

d) 应提供 IP 或 MAC 白名单功能。

6.1.3 固件安全

办公设备：

a) 应提供固件更新管理功能；存在管理员的，应由管理员执行固件更新；不存在管理员的，应由用户单独同意后执行固件更新。
b) 应在更新前验证固件的完整性和真实性，验证不通过的应立即停止更新。
c) 固件不应存在恶意程序。
d) 应在启动时自动检测固件完整性、真实性，发现异常时应立即停止工作。

6.1.4 日志记录与审计

办公设备：

a) 应对下述事件产生审计日志记录：
   1) 审计功能开启和关闭；
   2) 办公设备功能的启动或完成；
   3) 使用身份标识或鉴别机制；
   4) 系统时间变更；
   5) 固件更新；
   6) 带芯片的耗材更换；
   7) 办公设备作业情况，包括但不限于页数和份数等；
   8) 其他与系统安全有关的事件或定义的可审计事件。
b) 审计日志记录应包括但不限于事件发生日期和时间、事件类型、用户身份、事件结果等。
c) 应支持从办公设备直接导出审计日志记录。
d) 应对审计日志记录进行保护，避免未经授权的删除。
e) 不提供审计日志记录发送接口的，审计日志记录在办公设备上的存储时间不应少于 6 个月。

6.1.5 用户数据安全

办公设备：

a) 应在作业完成后，自动删除办公设备相应模块、驱动程序中存在的用户文档数据及相关临时文件和缓存数据。
b) 应采取安全措施保障用户仅能操作自身的用户文档数据。
c) 不应在耗材芯片中存储用户数据。

注：耗材使用情况的统计数据不属于用户数据。

d) 应对存储的日志、配置信息等数据采取安全保护措施，包括但不限于加密、完整性校验等。
e) 发生故障、错误时，用户未在设定时间内采取操作的，应删除用户文档数据。
f) 应提供自动和手动清除耗材上残余信息的功能。

6.1.6 通信安全

办公设备：

a) 应具备抵御常见网络攻击的能力。
b) 应按最小授权原则关闭与办公设备功能使用无关的通信端口、服务和协议。
c) 不应存在隐蔽通道。
d) 应提供关闭通信端口、服务和协议的功能。
e) 应在网络连接保持静默状态达到规定时间后，自动终止通信连接。

f） 应使用安全的 SNMP 协议。
g） 应采取保护措施，保障通信数据的保密性、完整性、可用性。
h） 应支持与驱动程序进行识别，驱动程序应与识别通过的办公设备传输数据；办公设备应与识别通过的驱动程序传输数据。
i） 具备无线通信模块的，应提供关闭功能并默认关闭。

注：无线通信模块包括但不限于无线局域网、蓝牙、红外等模块。

j） 具备网络共享功能、远程管理功能的，应提供关闭功能并默认关闭。
k） 宜提供抗抵赖功能。

6.1.7 非易失性存储器安全

办公设备：

a） 应提供对非易失性存储器中的用户数据进行完整性检查的功能。
b） 应提供删除非易失性存储器中用户数据的功能。
c） 具有可移除非易失性存储器的，应采用公开的数据存储结构，使用公开的协议与其控制系统进行数据交换。
d） 具备外接非易失性存储功能的，应提供由管理员关闭外接非易失性存储功能并默认关闭；用于身份鉴别的外接非易失性存储器，不应存储除身份鉴别信息以外的用户数据。

6.1.8 配置安全

办公设备：

a） 应提供维护安全配置的功能，由管理员对安全配置进行查询、修改。
b） 应提供自检功能，证实全部或部分安全功能操作的正确性。
c） 具备操作面板的，应支持操作面板锁定功能。

6.2 安全保障要求

6.2.1 设计和开发

办公设备提供者：

a） 应识别办公设备在设计、开发环节的安全风险，制定安全策略，采取安全措施保障关键组件的设计和开发安全。
b） 应制定实施安全开发流程，减少设计、开发等过程中恶意程序植入、漏洞引入的风险。
c） 应对设计文档、开发文档等进行配置管理，建立配置管理清单或相应程序，对配置项的变更进行授权和控制。
d） 应自行、联合或委托第三方对办公设备（包括办公设备中使用的第三方软硬件模块）进行安全测试。
e） 应在开发阶段对已发现的安全缺陷、漏洞进行修复；应制定并实施紧急修复的安全管理流程，及时修复未能在开发阶段发现的安全缺陷、漏洞。
f） 应保障安全功能设计与实现之间的一致性。
g） 应具备驱动软件、固件、数据控制板等关键组件的设计、开发能力。

6.2.2 生产和交付

办公设备提供者：

a) 应说明办公设备中所有与用户相关的功能模块和访问接口，包括但不限于人机接口、调试接口等。
b) 应通过用户协议、用户手册或网站通报等途径，声明所提供的办公设备中没有故意留有或者设置漏洞、后门、木马等程序和功能。
c) 应明确标识非易失性存储器容量、耗材芯片可写区域的容量，并说明存储的数据类型和用途。
d) 应在用户手册中说明所有默认账号信息、类型，以及对应的鉴别信息。
e) 应建立和实施规范的产品生产和服务交付流程，在关键环节实施安全检查和验证，减少办公设备生产和服务交付过程中的安全风险。
f) 应为用户提供验证所交付办公设备软硬件完整性的安全措施，减少产品交付过程中的篡改风险。
g) 应为用户提供操作指南等指导性文档，明确办公设备典型部署环境及应满足的安全要求，描述办公设备使用过程中涉及的各用户角色和安全责任，给出风险提示和应急响应措施。

6.2.3 运行和维护

办公设备提供者：

a) 应建立和执行针对办公设备安全缺陷、漏洞的应急响应机制和流程，对办公设备在运行和维护阶段暴露的安全缺陷、漏洞进行响应。
b) 应建立和实施规范的用户信息保护制度，当存在违反法律法规规定或者双方约定收集、使用用户个人信息的情形时，应主动或在用户要求下删除个人信息。
c) 在规定或与用户约定的期限内，不应终止提供安全维护；在用户授权的范围内开展运行维护工作，保障办公设备运行维护过程中的数据安全，防止数据泄露、篡改、损毁；未经用户同意，不应向他人提供数据，或将数据用于除运行维护以外的目的。
d) 应在更新办公设备前告知用户更新的内容，包括变更情况、相关安全风险、风险应对措施等，获得用户授权同意后方可实施更新，允许用户选择不接受更新。
e) 应在发现办公设备存在安全缺陷、漏洞等风险时立即采取补救措施，包括但不限于漏洞修复、安全替代方案等；及时告知合作伙伴和用户相关安全风险，并向有关主管部门报告。
f) 对产品和服务的安全缺陷、漏洞进行修复时，应提前告知用户将采取的处置操作和可能产生的影响。
g) 应为用户提供支持办公设备更新包的完整性、来源真实性等安全校验的方法或工具。
h) 应保护办公设备在运行维护过程中的用户数据，防止用户数据泄露、篡改、损毁、丢失。

6.2.4 供应链安全

办公设备提供者：

a) 应声明不会通过在办公设备中设置后门，或利用提供办公设备的便利条件非法获取用户数据、控制和操纵用户系统和设备，不会利用用户对办公设备的依赖性谋取不正当利益，不得强迫用户对办公设备进行更新。
b) 应强化采购渠道管理，保障主控制芯片、引擎、数据控制板、耗材等关键部件来源的稳定性或多样性，防范供应链中断风险。
c) 应提供中文版运行维护、二次开发等技术资料。

注：二次开发是为完成办公设备运维开展的功能扩展活动，二次开发工具包括软件开发工具（SDK）和配套资料，或测试工具。

d) 对办公设备研发、制造过程中涉及的第三方实体拥有或控制的已知技术专利等知识产权，已获得授权的，应获得十年以上授权或授权期限覆盖办公设备的上市周期。

e) 应声明办公设备中使用的已知第三方技术；使用的已知第三方技术不应出现以下情况：
   1) 因贸易、服务能力等因素中断办公设备、主控制芯片、引擎、固件等元器件、材料供应；
   2) 停止软件授权、更新或技术支持服务。

7 测评方法

7.1 安全功能要求测评方法

7.1.1 标识和鉴别

本项测试包括：

a) 测试办公设备在用户进行设备功能、安全功能操作之前，是否对用户进行唯一的身份标识并成功进行鉴别，包括但不限于禁止创建相同身份标识的用户、用户身份鉴别失败时阻止用户访问、用户的身份标识和鉴别信息是否存储在办公设备等。
b) 验证办公设备是否提供设置锁定时间的功能；用户登录办公设备后，在设定的时间内不执行产品功能、安全功能，查看设备是否自动退出该用户账号；用户登录时输入错误用户鉴别信息，且输入次数超过最大设定次数时，是否锁定该用户账号。
c) 验证办公设备是否支持通过 PIN 方式执行作业；验证用户输入 PIN 后作业是否正常执行；PIN 输入的失败次数超过设定的最大次数后，验证该作业是否被锁定；办公设备关机重启后，验证通过 PIN 方式执行的作业是否按删除机制删除。

7.1.2 访问控制

本项测试包括：

a) 验证使用管理员、用户账号登录并使用产品功能、安全功能时，检查管理员、用户账号承担对应任务时所需的权限是否为最小访问权限。
b) 使用管理员账号登录办公设备，对用户账号进行授权，检查用户可使用功能是否与管理员授权功能一致。
c) 设置办公设备功能、用户数据的访问控制策略，验证访问控制策略是否生效。
d) 设置 IP 或 MAC 白名单，验证是否只能允许白名单内的设备进行访问。

7.1.3 固件安全

本项测试包括：

a) 存在管理员的，验证固件更新操作是否只能由管理员执行；不存在管理员的，验证固件更新操作是否只能由用户单独同意后执行。
b) 对办公设备执行固件更新操作，验证固件是否通过数字签名等方式进行完整性和真实性的检查；固件更新操作验证不通过时，办公设备是否立即停止更新操作。
c) 使用两款不同的恶意程序扫描工具对固件进行扫描，验证是否存在恶意程序。
d) 验证办公设备启动过程是否自动检测固件的完整性、真实性；固件完整性、真实性检测不通过时，验证办公设备是否立即停止工作。

7.1.4 日志记录与审计

本项测试包括：

a) 验证办公设备是否保存以下事件的审计日志记录：
   1) 审计功能的开启和关闭；

2) 办公设备功能的启动或完成；
3) 使用身份标识或鉴别机制；
4) 系统时间的变更；
5) 固件更新；
6) 带芯片的耗材更换，审计日志记录应包括耗材的唯一标识信息；
7) 办公设备作业情况，包括但不限于页数和份数等；
8) 其他与系统安全有关的事件或定义的可审计事件。

b) 验证办公设备审计日志记录是否包括事件发生日期和时间、事件类型、用户身份以及事件结果等。
c) 验证办公设备是否支持通过打印信息报告等形式直接导出审计日志记录。
d) 验证办公设备是否支持对审计日志记录进行保护；未经授权时，是否无法对审计日志记录执行删除操作。
e) 对不提供审计日志记录发送接口的办公设备，验证审计日志记录是否存储在办公设备中；验证审计日志记录的存储时间是否不少于 6 个月。

7.1.5 用户数据安全

本项测试包括：

a) 向办公设备下发作业请求，作业完成后，验证相应模块、驱动程序中的用户文档数据及临时文件和缓存数据是否被删除，删除方式包括但不限于多次覆盖式写入等。
b) 使用不同用户登录办公设备，验证是否仅能对自身的用户文档数据进行操作。
c) 验证耗材芯片中是否存储用户数据。
d) 验证办公设备是否支持对存储的日志、配置信息等采用密码算法进行加密保护或完整性校验。
e) 设定办公设备错误、故障的处理时间，当办公设备发生错误、故障且用户未在设定时间内进行操作，验证办公设备是否自动删除用户文档数据。
f) 向办公设备下发作业任务，验证作业完成后办公设备是否清除耗材上的残余信息；当办公设备发生错误、故障等时，验证错误、故障恢复后是否能够通过手动方式清除耗材上的残余信息。

7.1.6 通信安全

本项测试包括：

a) 验证办公设备是否具备抵御常见网络攻击的能力。
b) 验证办公设备是否支持按最小授权原则关闭与功能使用无关的通信端口、服务和协议。
c) 验证办公设备是否存在隐蔽通道。
d) 验证办公设备是否提供关闭通信端口、服务和协议的功能；验证办公设备关闭通信端口、服务和协议的功能是否有效。
e) 设定办公设备的网络连接超时时间间隔，保持办公设备处于静默状态，在超过设定的时间后，验证办公设备是否自动终止通信连接。
f) 验证办公设备所使用 SNMP 的协议是否安全。
g) 验证办公设备是否采取保护措施；验证办公设备采取的保护措施是否能够有效保障通信数据的保密性、完整性、可用性。
h) 验证办公设备识别驱动程序且驱动程序识别办公设备后，是否正常进行作业数据传输；验证办公设备未能识别驱动程序或驱动程序未能识别办公设备时，是否不进行作业数据传输。

i） 办公设备具备无线通信模块的，验证办公设备无线通信模块是否默认关闭；验证办公设备是否提供关闭无线通信模块的功能；验证办公设备无线关闭模块功能是否生效。
j） 办公设备具备网络共享功能、远程管理功能的，验证办公设备网络共享功能、远程管理功能是否默认关闭；验证办公设备是否提供关闭网络共享、远程管理的功能；验证办公设备关闭网络共享、远程管理的功能是否生效。
k） 验证办公设备是否具备抗抵赖功能。

7.1.7 非易失性存储器安全

本项测试包括：
a） 验证办公设备提供的对非易失性存储器中的用户数据进行完整性检查的功能是否生效。
b） 验证办公设备提供的删除非易失性存储器中用户数据的功能是否生效。
c） 办公设备具有可移除非易失性存储器的，验证可移除非易失性存储装置是否采用公开的数据存储结构；验证可移除非易失性存储装置是否通过公开的协议与其控制系统进行数据交换。
d） 办公设备具备外接非易失性存储功能的，验证办公设备外接非易失性存储功能是否默认关闭；验证关闭非易失性存储功能是否由管理员提供；办公设备支持身份鉴别类外接非易失性存储器的，验证外接非易失性存储器是否存储身份鉴别信息以外的用户数据。

7.1.8 配置安全

本项测试包括：
a） 使用管理员、用户账号登录办公设备，验证是否仅能使用管理员账号对安全配置进行查询、修改。
b） 验证办公设备是否提供自检功能；验证自检信息是否包含全部或部分办公设备安全功能操作的正确性。
c） 办公设备具备操作面板的，验证是否支持面板锁定功能。

7.2 安全保障要求测评方法

7.2.1 设计与开发

本项测试包括：
a） 检查办公设备提供者是否在办公设备及其关键组件设计、开发过程中进行了安全风险识别；检查其制定的安全策略是否包含应对安全风险的措施，检查采取的安全措施是否能够保护办公设备及其关键组件的设计和开发安全。
b） 检查办公设备提供者是否制定了安全开发相关的管理制度、开发规范和工作流程；检查安全开发的管理制度、开发规范和工作流程是否实施，是否起到了降低恶意程序植入、漏洞引入风险的作用。
c） 检查办公设备提供者是否制定了文档配置管理方案，检查是否对设计文档和开发文档进行了配置管理，是否对配置变更设置了授权管理和控制。
d） 检查办公设备提供者是否制定了安全测试管理制度，以通过自行、联合或委托第三方的方式进行安全测试；检查办公设备（包括办公设备中使用的第三方软硬件模块）测试报告内容是否合理,是否包含明确的安全结论。
e） 检查办公设备提供者是否制定了办公设备产品安全缺陷、漏洞的管理制度；检查管理制度是否包含安全缺陷、漏洞的发现和修复流程；检查管理制度是否包含紧急修复的安全管理流程，包括在用户侧修复安全缺陷、漏洞的流程。

f) 检查办公设备提供者提供的办公设备设计和开发材料是否包含了保障安全功能与产品实现一致性的策略和措施。
g) 检查办公设备提供者提供的设计和开发能力证明材料，检查其是否具备驱动软件、固件、数据控制板等关键组件的设计、开发能力。

7.2.2 生产和交付

本项测试包括：
a) 检查办公设备提供者的说明材料是否包含了办公设备对应的功能模块和访问接口说明；检查说明材料是否描述了与用户相关的功能模块和访问接口，包括但不限于人机接口、调试接口等。
b) 检查办公设备对应的用户协议、用户手册或办公设备提供者网站是否有发布声明；检查声明内容是否描述了所提供的办公设备中没有故意留有或者设置漏洞、后门、木马等程序和功能。
c) 检查办公设备提供者是否明确标识非易失性存储容量、耗材芯片可写区域的容量；检查办公设备提供者是否说明存储的数据类型和用途。
d) 检查用户手册中是否说明了所有默认账号信息、类型，以及对应的鉴别信息。
e) 检查办公设备提供者提供的材料是否包含了生产和服务交付流程说明文档；验证生产和服务交付流程是否能够减少办公设备生产和服务交付过程中的安全风险；检查办公设备提供者的办公设备生产和服务交付过程是否按照指定的流程实施；检查关键环节的安全检查和验证是否有效。
f) 验证办公设备提供者提供的材料是否包含了验证办公设备软硬件完整性的安全措施；验证安全措施是否保障办公设备软硬件设备完整性。
g) 检查办公设备提供者提供的材料是否包含了操作指南等指导性文档；检查操作指南等指导性文档是否对办公设备典型部署环境应满足的安全要求进行了描述，是否对办公设备使用过程中涉及的各用户角色和安全责任进行了描述，是否描述了办公设备典型应用过程的风险提示和应急响应措施。

7.2.3 运行和维护

本项测试包括：
a) 检查办公设备提供者提供的材料，确认是否建立了应急响应机制和流程，是否执行了应急响应机制和流程，包括但不限于应急预案、应急响应记录等。
b) 检查办公设备提供者提供的材料是否包含用户信息保护制度，是否描述了存在违反法律法规规定或者双方约定收集、使用用户个人信息的情形时主动或在用户要求下删除个人信息的规定；检查办公设备提供者提供的文件是否包含实施用户信息保护制度的记录。
c) 检查办公设备提供者提供的材料是否描述了安全维护的期限及服务承诺；检查是否描述了安全运维的范围需由用户授权，是否描述了保障办公设备运行维护过程中的用户数据安全；检查是否存在向他人提供数据，或将数据用于除运行维护以外目的的记录。
d) 检查办公设备更新时是否向用户告知了更新的内容，包括变更情况、相关安全风险、风险应对措施等；检查更新时是否给用户提供了不接受更新的选项；检查办公设备是否是在用户选择了接受更新的条件下才执行更新操作。
e) 检查办公设备提供者提供的材料是否包含了对于设备安全缺陷、漏洞等风险发生时的处理流程；检查办公设备提供者制定的流程是否描述了安全缺陷、漏洞发生后应采取的补救措施，包括但不限于漏洞修复、安全替代方案等；检查办公设备提供者提供的文件是否包含及时告知合作伙伴和用户相关风险，并向有关主管部门报告的机制。

f) 检查办公设备提供者提供的安全缺陷、漏洞修复操作相关材料是否包含提前告知用户将采取的处置操作和可能产生的影响的说明。
g) 检查办公设备提供者提供的材料，是否包含为用户提供支持办公设备更新包的完整性、来源真实性等安全校验的方法或工具，验证方法或工具的有效性。
h) 检查办公设备提供者提供的材料是否有针对用户数据的保护措施，防止用户数据泄露、篡改、损毁、丢失。

7.2.4 供应链安全

本项测试包括：

a) 检查办公设备提供者提供的材料是否包含声明文件；检查声明内容是否覆盖：不会在办公设备中设置后门；不会利用提供产品的便利条件非法获取用户数据、控制和操纵用户系统和设备；不会利用用户对办公设备的依赖性谋取不正当利益；不会强迫用户对办公设备进行升级或更新换代等。
b) 检查办公设备提供者提供的供应链管理相关制度文件和证明材料，验证相关措施能否有效保障主控制芯片、引擎、数据控制板、耗材等关键零部件供应的稳定性或多样性。
c) 检查办公设备提供者提供的产品运行维护、二次开发相关技术资料是否为中文资料。
d) 检查办公设备提供者提供的相关材料，验证办公设备提供者对办公设备研发、制造过程中涉及的第三方实体拥有或控制的已知技术专利等知识产权，已获得授权的，是否获得十年以上授权或授权期限覆盖办公设备的上市周期。
e) 检查办公设备提供者提供的办公设备使用第三方技术的声明材料，验证使用的第三方技术不得存在以下情况：
   1) 因贸易、服务能力等因素中断办公设备、主控制芯片、引擎、固件等元器件、材料供应；
   2) 停止软件授权、更新或技术支持服务。

附 录 A
（规范性）
办公设备分类及安全技术要求等级划分

A.1 概述

本附录分别列出具有打印、扫描、传真、复印功能的办公设备安全技术要求，明确了各类办公设备基本级和增强级安全技术要求的最小集合。

A.2 具有打印功能的办公设备

表A.1列出了具有打印功能办公设备安全技术要求的等级划分。

表 A.1 具有打印功能办公设备安全技术要求等级划分表

安全技术要求		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	6.1.1
	访问控制	—	6.1.2
	固件安全	6.1.3 a）、b）	6.1.3
	日志记录与审计	—	6.1.4
	用户数据安全	6.1.5 a）、b）	6.1.5
	通信安全	6.1.6 a）～c）	6.1.6
	非易失性存储器安全	6.1.7 a）、b）	6.1.7
	配置安全	—	6.1.8
安全保障要求	设计和开发	6.2.1 a）～e）	6.2.1
	生产和交付	6.2.2 a）～d）	6.2.2
	运行和维护	6.2.3 a）～d）	6.2.3
	供应链安全	6.2.4 a）	6.2.4
注：“—”表示不适用。			

A.3 具有扫描功能的办公设备

表A.2列出了具有扫描功能办公设备安全技术要求的等级划分。

表 A.2 具有扫描功能办公设备安全技术要求等级划分表

安全技术要求		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	6.1.3 a）、b）	6.1.3 a）、b）
	日志记录与审计	—	—
	用户数据安全	6.1.5 a）	6.1.5 a）
	通信安全	—	—
	非易失性存储器安全	6.1.7 a）	6.1.7 a）
	配置安全	—	—

表A.2　具有扫描功能办公设备安全技术要求等级划分表（续）

安全技术要求		基本级对应章节号	增强级对应章节号
安全保障要求	设计和开发	6.2.1 a）～e）	6.2.1 a）～e）
	生产和交付	6.2.2 a）～b）	6.2.2 a）～b）
	运行和维护	6.2.3 a）～d）	6.2.3
	供应链安全	6.2.4 a）	6.2.4 a）
注：“—”表示不适用。			

A.4　具有复印功能的办公设备

表A.3列出了具有复印功能办公设备安全技术要求的等级划分。

表 A.3 具有复印功能办公设备安全技术要求等级划分表

安全技术要求		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	6.1.3 a）、b）	6.1.3
	日志记录与审计	—	6.1.4
	用户数据安全	6.1.5 a）、b）	6.1.5
	通信安全	—	—
	非易失性存储器安全	6.1.7 a）、b）	6.1.7
	配置安全	—	—
安全保障要求	设计和开发	6.2.1 a）～e）	6.2.1
	生产和交付	6.2.2 a）～c）	6.2.2 a）～c）、e）～g）
	运行和维护	6.2.3 a）～d）	6.2.3
	供应链安全	6.2.4 a）	6.2.4
注：“—”表示不适用。			

A.5　具有传真功能的办公设备

表A.4列出了具有传真功能办公设备安全技术要求的等级划分。

表 A.4 具有传真功能办公设备安全技术要求等级划分表

安全技术要求		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	6.1.3 a）、b）	6.1.3 a）、b）
	日志记录与审计	—	6.1.4 c）
	用户数据安全	6.1.5 a）	6.1.5 a）
	通信安全	6.1.6 c）	6.1.6 c）、h）、i）
	非易失性存储器安全	6.1.7 a）、b）	6.1.7
	配置安全	—	—
安全保障要求	设计和开发	6.2.1 a）～e）	6.2.1

表A.4　具有传真功能办公设备安全技术要求等级划分表（续）

安全技术要求		基本级对应章节号	增强级对应章节号
安全保障要求	生产和交付	6.2.2 a）～c）	6.2.2 a）～c）、e）～g）
	运行和维护	6.2.3 a）～d）	6.2.3
	供应链安全	6.2.4 a）	6.2.4 a）
注：“—”表示不适用。			

附 录 B
（规范性）
办公设备分类及测评方法等级划分

B.1 概述

本附录根据附录A的要求，分别列出具有打印、扫描、传真、复印功能的办公设备相关要求对应的测评方法。

B.2 具有打印功能的办公设备

表B.1列出了具有打印功能办公设备测评方法的等级划分。

表 B.1 具有打印功能办公设备测评方法等级划分表

测评方法		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	7.1.1
	访问控制	—	7.1.2
	固件安全	7.1.3 a）、b）	7.1.3
	日志记录与审计	—	7.1.4
	用户数据安全	7.1.5 a）、b）	7.1.5
	通信安全	7.1.6 a）～c）	7.1.6
	非易失性存储器安全	7.1.7 a）、b）	7.1.7
	配置安全	—	7.1.8
安全保障要求	设计和开发	7.2.1 a）～e）	7.2.1
	生产和交付	7.2.2 a）～d）	7.2.2
	运行和维护	7.2.3 a）～d）	7.2.3
	供应链安全	7.2.4 a）	7.2.4
注：“—”表示不适用。			

B.3 具有扫描功能的办公设备

表B.2列出了具有扫描功能办公设备测评方法的等级划分。

表 B.2 具有扫描功能办公设备测评方法等级划分表

测评方法		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	7.1.3 a）、b）	7.1.3 a）、b）
	日志记录与审计	—	—
	用户数据安全	7.1.5 a）	7.1.5 a）
	通信安全	—	—
	非易失性存储器安全	7.1.7 a）	7.1.7 a）
	配置安全	—	—

表B.2　具有扫描功能办公设备测评方法等级划分表（续）

测评方法		基本级对应章节号	增强级对应章节号
安全保障要求	设计和开发	7.2.1 a）～e）	7.2.1 a）～e）
	生产和交付	7.2.2 a）～b）	7.2.2 a）～b）
	运行和维护	7.2.3 a）～d）	7.2.3
	供应链安全	7.2.4 a）	7.2.4 a）
注：“—”表示不适用。			

B.4　具有复印功能的办公设备

表B.3列出了具有复印功能办公设备测评方法的等级划分。

表 B.3 具有复印功能办公设备测评方法等级划分表

测评方法		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	7.1.3 a）、b）	7.1.3
	日志记录与审计	—	7.1.4
	用户数据安全	7.1.5 a）、b）	7.1.5
	通信安全	—	—
	非易失性存储器安全	7.1.7 a）、b）	7.1.7
	配置安全	—	—
安全保障要求	设计和开发	7.2.1 a）～e）	7.2.1
	生产和交付	7.2.2 a）～c）	7.2.2 a）～c）、e）～g）
	运行和维护	7.2.3 a）～d）	7.2.3
	供应链安全	7.2.4 a）	7.2.4
注：“—”表示不适用。			

B.5　具有传真功能的办公设备

表B.4列出了具有传真功能办公设备测评方法的等级划分。

表 B.4 具有传真功能办公设备测评方法等级划分表

测评方法		基本级对应章节号	增强级对应章节号
安全功能要求	标识和鉴别	—	—
	访问控制	—	—
	固件安全	7.1.3 a）、b）	7.1.3 a）、b）
	日志记录与审计	—	7.1.4 c）
	用户数据安全	7.1.5 a）	7.1.5 a）
	通信安全	7.1.6 c）	7.1.6 c）、h）、i）
	非易失性存储器安全	7.1.7 a）、b）	7.1.7
	配置安全	—	—
安全保障要求	设计和开发	7.2.1 a）～e）	7.2.1

表B.4　具有传真功能办公设备测评方法等级划分表（续）

测评方法		基本级对应章节号	增强级对应章节号
安全保障要求	生产和交付	7.2.2 a）～c）	7.2.2 a）～c）、e）～g）
	运行和维护	7.2.3 a）～d）	7.2.3
	供应链安全	7.2.4 a）	7.2.4 a）
注：“—”表示不适用。			