TC260-PG-2026NA

网络安全标准实践指南

——网络安全标识 智能音箱安全要求

（征求意见稿 v1.0-202611）

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

全国网络安全标准化技术委员会秘书处

2026 年 11 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：

本文件主要起草人：

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

摘　要

伴随着智能音箱的广泛应用，相关安全问题引发社会和业界高度关注。为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，全国网络安全标准化技术委员会秘书处组织制定了本文件，给出智能音箱网络安全能力要求，由低到高按照基础级、增强级、领先级划分为三个等级，适用于指导智能音箱的设计、开发、使用、维护和检测。

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

目　录

1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 概述 3
5 基础级要求 4
5.1 物理与硬件安全 4
5.2 系统与软件安全 5
5.3 网络与通信安全 6
5.4 数据安全与个人信息保护 7
5.5 安全保障 9
6 增强级要求 10
6.1 物理与硬件安全 10
6.2 系统与软件安全 10
6.3 网络与通信安全 13
6.4 数据安全与个人信息保护 14
6.5 安全保障 15
7 领先级要求 17
7.1 物理与硬件安全 17
7.2 系统与软件安全 17
7.3 网络与通信安全 18
7.4 数据安全与个人信息保护 18
7.5 安全保障 19
附录 A（规范性）不同安全能力等级的产品应符合的安全要求 22
附录 B（资料性）测试评价方法 24
B.1 基础级测评 24
B.2 增强级测评 37
B.3 领先级测评 53
附录 C（规范性）第三方检测机构能力要求 64
C.1 机构要求 64
C.2 人员要求 64
参　考　文　献 65

1 范围

本文件规定了智能音箱网络安全标识基础级、增强级、领先级的网络安全能力要求，包括安全技术要求和安全保障要求。

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/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 38674—2020 应用软件安全编程指南

GB/T 39276—2020 信息安全技术 网络产品和服务安全通用要求

GB/T 45574—2025 数据安全技术 敏感个人信息处理安全要求

GB 46864—2025 数据安全技术 电子产品信息清除技术要求

GB/T 47694—2026 网络安全技术 移动互联网未成年人模式技术要求

3 术语和定义

3.1

智能音箱　smart speaker

具备语音识别、语音交互、语义理解、语音合成等智能语音功能的，可以通过控制单元进行管理、控制的，联网的独立音箱设备。

注：可以同时具备联网设备控制、网络内容交互、网络支付服务等叠加功能。

3.2

语音识别　speech recognition

将人类的声音信号转化为文字或者指令的过程。

[来源：GB/T 21023—2007]

3.3

语音唤醒　speech wakeup; voice trigger

处于音频流监听状态的语音交互系统，在监测到特定的特征或事件出现后，切换到命令字识别、连续语音识别等其他处理状态的过程。

[来源：GB/T 36464.2—2018]

3.4

设备绑定　device binding

建立用户账号与智能音箱设备间唯一权属关系的过程。

3.5

语音合成　speech synthesis

通过机械的、电子的方法合成人类语音的过程。

[来源：GB/T 21024—2007，有修改]

3.6

唤醒词　wake-up word

用于唤醒智能音箱设备并启动语音交互的特定词语和短语。

3.7

控制单元　device control unit

与智能音箱设备建立绑定关系，用于支持用户对智能音箱设备进行控制、管理等功能的模块。

3.8

主账号　master account

通过控制单元与智能音箱设备建立绑定关系，并拥有对智能音箱设备全部控制、管理权限的唯一账号。

3.9

授权账号　authorized account

经主账号授权，通过控制单元与智能音箱设备建立绑定关系后，可以对智能音箱设备进行控制的账号。

4　概述

本文件从物理与硬件安全、系统与软件安全、网络与通信安

全、数据安全与个人信息保护、安全保障 5 个方面构建智能音箱安全框架（见图 1）。

智能音箱网络安全能力划分为三级，从基础级、增强级、领先级逐级提升。基础级要求产品网络安全能力达到基本的网络安全水平，增强级要求产品网络安全能力达到同类产品先进水平，领先级要求产品网络安全能力达到同类产品领先水平。满足同一等级的所有单项要求，方可获得该网络安全能力等级。各网络安全能力等级的产品应符合的安全要求见附录 A，测试评价方法参考附录 B。

开展基础级、增强级产品检测的第三方检测机构应满足附录 C.1 的要求；开展领先级产品检测的第三方检测机构应满足附录 C.1、C.2 的要求。

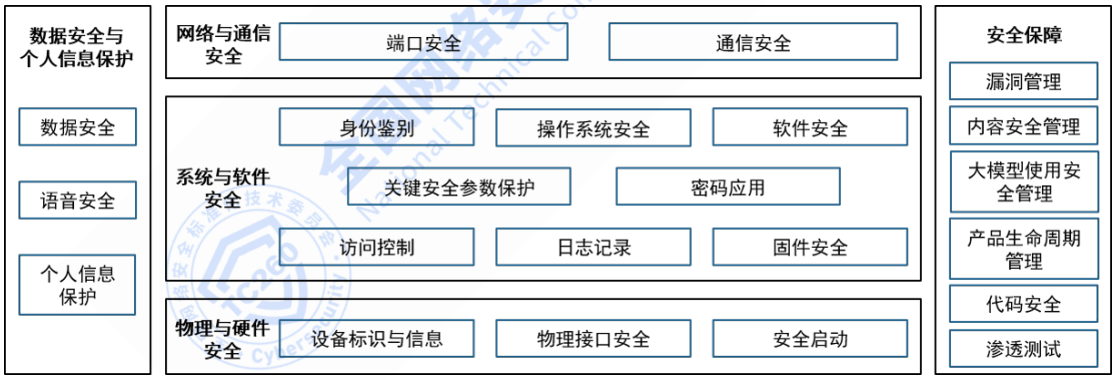


图1 智能音箱安全框架

5 基础级要求

5.1 物理与硬件安全

5.1.1 设备标识与信息

智能音箱应满足如下要求：

a) 具有唯一设备标识;

注：设备标识指用于识别或验证设备身份合法性的唯一标识符号。

b) 在设备外观清晰标识出设备型号、设备名称等信息。

5.2 系统与软件安全

5.2.1 身份鉴别

智能音箱应满足如下要求:

a） 设备绑定后，在智能音箱与主账号控制单元间建立唯一关联，并采取防护措施防止关联被篡改;

b） 不存在未公开的账号和登录方式;

注：未公开的账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号。

c） 控制单元对账号身份进行标识和鉴别，对账号身份鉴别凭证进行安全保护;

d） 使用口令进行身份鉴别的，禁止使用弱口令，口令不应少于 8 个字符，至少包含数字、小写字母、大写字母以及特殊字符中的 2 类字符。

5.2.2 操作系统安全

智能音箱独立操作系统应满足最小化权限原则，仅为应用程序分配必要的权限。

5.2.3 软件安全

智能音箱应满足如下要求:

a) 具有预置应用的，在预置应用更新时对更新包进行真实性和完整性校验；

b) 提供第三方应用安装功能的，默认不允许第三方应用软件自动安装。

5.2.4 关键安全参数保护

智能音箱不应在设备软件代码中硬编码关键安全参数。

5.2.5 密码应用

智能音箱中用于身份鉴别、安全更新、网络通信、数据存储、安全启动、关键安全参数保护等场景的加密技术应符合国家密码管理相关规定。

5.2.6 访问控制

智能音箱应满足如下要求：

a) 设备在与主账号的控制单元完成绑定前，拒绝绑定以外的其他操作；

b) 已完成设备绑定的，仅接受来自绑定主账号或其授权账号的控制指令；

c) 已完成设备绑定的，不再接受其它账号绑定，除非绑定设备的主账号主动解除绑定；

d) 支持主账号和授权账号通过控制单元解除与音箱关联，并删除存储的用户所有数据。

5.3 网络与通信安全

5.3.1 端口安全

智能音箱应满足如下要求：

a) 提供文档说明所有网络端口和服务，并告知对业务的影响；

b) 智能音箱所开放端口应默认遵循最小化原则，关闭非必须使用的网络服务和网络端口。

5.3.2 通信安全

智能音箱应满足如下要求：

a) 使用密码技术保护关键安全参数、敏感个人信息等数据传输的机密性、完整性；

b) 向外部传输用户数据时，使用安全传输通道。

5.4 数据安全与个人信息保护

5.4.1 数据安全

智能音箱应为用户提供符合 GB 46864—2025 要求的信息清除功能。

注：功能由产品或其管理端提供，用户自行使用。

5.4.2 语音安全

智能音箱应满足如下要求：

a) 用户语音的唤醒词默认本地存储；

b) 触发唤醒词后，通过灯光、屏幕等明显、持续的方式提示用户智能音箱已唤醒，处于等待用户指令的收音状态；提供夜间模式等允许用户自主关闭持续提示的，在触发唤醒词

后通过语音等方式提示用户智能音箱已唤醒，且处于夜间模式等状态下；

c) 提供实体按键，支持用户一键关闭智能音箱的收音功能；

d) 具备静默状态下防窃听能力，仅在智能音箱端侧检测唤醒词，静默状态下不存储、传输任何用户语音。

5.4.3 个人信息保护

智能音箱应满足如下要求：

a) 处理个人信息的，在产品管理相关界面、说明书等提供的链接页面公开展示个人信息处理规则，供用户查阅、复制或下载后查阅，规则内容包括但不限于：

1) 个人信息处理者的名称和联系方式；

2) 处理个人信息的种类和对应的处理目的、方式；

3) 明确个人信息是否存储在境内，以及存储的期限和到期后的处理方式；

4) 处理个人信息的必要性、对用户个人权益的影响和所采取安全措施的说明；

5) 查阅、复制、转移、更正、补充、删除用户个人信息，以及注销账号、撤回同意的方法和途径。

b) 个人信息收集应符合 GB/T 35273—2020 中 5.2、5.4 的要求；

c) 个人信息存储应符合 GB/T 35273—2020 中 6.1、6.3 的要求；

d) 未经用户同意，不对所收集语音等与个人的身份进行关联分析，履行法定义务和法律法规另有规定的除外；

e) 处理用户敏感个人信息应符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

5.5 安全保障

5.5.1 漏洞管理

智能音箱生产者应满足如下要求：

a) 确保设备不存在已知的高危及以上等级的漏洞；

注：已知高危及以上等级漏洞参考CNVD、CNNVD、NVDB等国家级漏洞库。

b) 在规定或与当事人约定期限内，持续对设备进行安全更新；

c) 建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应、修补；

d) 发现设备存在安全缺陷、漏洞时，按照国家有关规定报送相关漏洞信息，并及时告知用户安全风险。

5.5.2 内容安全管理

智能音箱生产者应满足如下要求：

a) 建立内容安全监测机制，对所提供的信息内容持续进行安全监测，对监测发现的违法不良信息技术进行及时处置；

b) 提供违法和不良网络信息内容举报途径，及时核实处置用户举报。

5.5.3 大模型使用安全管理

智能音箱利用大模型为用户提供服务的，所使用大模型应已通过生成式人工智能服务备案。

6 增强级要求

6.1 物理与硬件安全

6.1.1 设备标识与信息

在满足 5.1.1 的要求的同时，还应采取防护措施保护唯一设备标识在出厂、激活、联网和设备绑定等环节不被篡改。

6.1.2 物理接口安全

智能音箱应满足如下要求：

a) 非拆机状态下，可调试物理接口不可访问；

b) 出厂时默认关闭可调试物理接口。

6.1.3 安全启动

智能音箱应实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验通过后方可正常启动，防范恶意固件替换、启动劫持和系统篡改。

6.2 系统与软件安全

6.2.1 身份鉴别

在满足 5.2.1 的要求的同时，还应满足如下要求：

a) 具备授权功能的，支持对授权账号的身份认证，以防止非授权的操作；

b) 具备声纹识别功能的，在采集声纹语音样本前结合其它身份鉴别手段对用户身份进行认证。

6.2.2 操作系统安全

在满足 5.2.2 的要求的同时，智能音箱还应默认禁止系统进程或应用获取系统的超级用户权限。

6.2.3 软件安全

在满足 5.2.3 的要求的同时，还应满足如下要求：

a) 提供第三方应用安装功能的，校验应用安装包或更新包的完整性和来源的真实性；

b) 具有预置应用的或提供第三方应用安装功能的，具备对应用访问权限的控制功能。

6.2.4 关键安全参数保护

在满足 5.2.4 的要求的同时，还应满足如下要求：

a) 采用密码技术对关键安全参数进行机密性和完整性保护；

b) 建立规范的关键安全参数的安全管理流程；

注1：管理对象包括但不限于根密钥，以及用于通信安全保护、安全更新保护、敏感个人信息保护的关键安全参数。

注2：管理流程包括但不限于密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等。

c) 保证设备重要的关键安全参数对每个设备是唯一的。

注：设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

6.2.5 密码应用

应满足 5.2.5 的要求。

6.2.6 访问控制

在满足 5.2.6 要求的同时，还应满足如下要求：

a) 其他账号只能由主账号授权后，方可具备访问权限；

b) 仅允许与设备唯一关联的主账号通过控制单元远程修改设备配置；具有交互屏幕的，提供口令等验证方式对通过交互屏幕修改设备配置进行保护；

c) 具有授权功能的：

1) 设备访问控制策略满足最小授权原则，默认不允许授权账号访问受控资源或使用关键功能；

注：仅允许主账号关联的控制单元更改访问控制策略。

2) 只有主账号具备访问权限分享功能，且能够取消授权用户的访问权限；

3) 采取防护措施保障分享的安全性。

注：保障分享的安全性防护措施包括但不限于分享权限即时回收、设置被分享者查看权限、设置分享有效期等措施。

6.2.7 日志记录

智能音箱应满足如下要求：

a) 能对开关机、创建用户、更改安全配置、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，记录应包括

事件类型、事件发生时间、触发事件的主体、事件处理结果等信息；

b) 具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏；

c) 具备日志记录存储保护机制，保障日志存储量超过阈值后审计日志正常记录最新事件；

d) 日志保存于非易失性存储介质。

6.2.8 固件安全

智能音箱应满足如下要求：

a) 固件升级具备安全校验机制，验证更新固件的真实性和完整性；

b) 具备新的固件版本时，提示用户通过自动、人工方式进行安全更新，更新中止后能重新更新；

c) 具备非授权固件版本防回退校验机制；

d) 设备在第一次使用或恢复出厂设置后检查并提示进行安全更新。

6.3 网络与通信安全

6.3.1 端口安全

在满足5.3.1的要求的同时，还应满足如下要求：

a) 未认证状态下最小化网络端口暴露信息；

b) 支持用户对网络端口和服务进行配置。

6.3.2 通信安全

在满足 5.3.2 的要求的同时，智能音箱还应具有抵抗重放攻击的能力。

6.4 数据安全与个人信息保护

6.4.1 数据安全

在满足 5.4.1 的要求的同时，还应满足如下要求：

a) 通过上传设备日志进行故障诊断时，明确告知用户数据采集方式、范围、目的，经用户同意后上传；

b) 采取加密等安全措施保护用户数据的机密性和完整性；

6.4.2 语音安全

在满足5.4.2的要求的同时，还应满足如下要求：

a) 用户的语音指令识别处理完成后，默认丢弃或使用安全方式存储在本地；

b) 征得用户明示同意后，上传的语音指令等数据方可留存；支持用户删除留存数据或撤回留存许可；

c) 上传的语音指令，默认不加入语料库、不输入大模型、不进行识别处理以外的语音分析。

6.4.3 个人信息保护

在满足 5.4.3 的要求的同时，还应满足如下要求：

a) 个人信息处理规则中涉及收集和向其他个人信息处理者提供个人信息的目的、方式、种类以及接收方信息的，以清单等形式予以列明；

b) 用户通过控制单元等便捷通道行使个人信息权利的，不设置不合理条件限制用户的合理请求。

6.5 安全保障

6.5.1 漏洞管理

应满足 5.5.1 的要求。

6.5.2 内容安全管理

应满足 5.5.2 的要求。

6.5.3 大模型使用安全管理

在满足 5.5.3 的要求的同时，智能音箱利用大模型为用户提供服务的，还应征得用户明示同意。

6.5.4 产品生命周期管理

智能音箱生产者应满足如下要求：

a) 建立产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节；

b) 建立产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁；

c) 编制开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程；

d) 建立产品安全开发机制，满足 GB/T 39276—2020 第 5.1.2.1 项相关要求；

e) 建立安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等；

f) 建立安全交付机制，在产品交付和重要版本发布前进行安全审查和加固，包括但不限于：

1) 删除非必要的账号、测试账号；

2) 从发布的版本中删除所有调试代码；

3) 禁用不必要的物理接口、网络服务、网络端口、网络接口；

4) 启用智能音箱终端侧操作系统的安全功能，包括身份鉴别、访问控制、数据加密等功能。

g) 建立安全运维机制和流程，满足 GB/T 39276—2020 第 5.2.2.3 项相关要求。

6.5.5 代码安全

智能音箱生产者应满足如下要求：

a) 建立开源代码来源审查机制，使用开源组件和开源软件的，宜从国家可信开源代码库中获取；

b) 建立开源代码安全漏洞跟踪和处置机制，对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

7 领先级要求

7.1 物理与硬件安全

7.1.1 设备标识与信息

应满足 6.1.1 的要求。

7.1.2 物理接口安全

应满足 6.1.2 的要求。

7.1.3 安全启动

应满足 6.1.3 的要求。

7.2 系统与软件安全

7.2.1 身份鉴别

在满足 6.2.1 的要求同时，智能音箱还应在数据传输前，对智能音箱设备与云平台、控制单元之间进行双向身份认证。

7.2.2 操作系统安全

应满足 6.2.2 的要求。

7.2.3 软件安全

在满足 6.2.3 的要求的同时，智能音箱具有预置应用或提供第三方应用安装功能的，还应对应用软件安装、更新的传输通道进行加密。

7.2.4 关键安全参数保护

在满足 6.2.4 的要求的同时，智能音箱还应采用硬件方式保护设备根密钥。

注：硬件方式包括但不限于使用安全芯片、芯片的安全存储区等。

7.2.5 密码应用

应满足 6.2.5 的要求。

7.2.6 访问控制

应满足 6.2.6 的要求。

7.2.7 日志记录

应满足 6.2.7 的要求。

7.2.8 固件安全

应满足 6.2.8 的要求。

7.3 网络与通信安全

7.3.1 端口安全

在满足 6.3.1 的要求的同时，对于必须使用的端口，智能音箱还应在使用后关闭。

7.3.2 通信安全

应满足 6.3.2 的要求。

7.4 数据安全与个人信息保护

7.4.1 数据安全

应满足 6.4.1 的要求。

7.4.2 语音安全

在满足 6.4.2 的要求的同时，还应满足如下要求：

a) 智能音箱处于唤醒状态时，接收到的与用户语音指令无关的用户谈话等内容直接丢弃，不存储、不传输；

b) 具备声纹识别功能的，具备检测和抵御常见声纹呈现攻击的能力；

注：常见的声纹呈现攻击包括但不限于：语音模仿、语音转换及合成、录音重放、录音拼接。

c) 提供声纹支付功能的，声纹支付功能默认关闭，并支持双因子认证方式保障支付安全。

7.4.3 个人信息保护

在满足 6.4.3 的要求的同时，智能音箱还应对敏感个人信息进行脱敏。

注：对敏感个人信息进行脱敏的方式包括但不限于去除声纹信息等。

7.5 安全保障

7.5.1 漏洞管理

应满足 6.5.1 的要求。

7.5.2 内容安全管理

在满足 6.5.2 的要求的同时，智能音箱还应支持面向未成年人用户健康使用的未成年人模式，满足 GB/T 47694—2026 第 6.2 项相关要求。

7.5.3 大模型使用安全管理

应满足 6.5.3 的要求。

7.5.4 产品生命周期管理

应满足 6.5.4 的要求。

7.5.5 代码安全

智能音箱生产者在满足 6.5.5 的要求的同时，还应满足如下要求：

a) 委托第三方检测机构针对设备自身代码进行检测，确保软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误；

b) 使用应用程序对设备进行管理的，委托第三方检测机构针对设备管理应用程序进行检测，确保软件、第三方库和第三方组件中不存在中危及以上安全漏洞，不存在硬编码身份鉴别信息和关键安全参数等错误。

7.5.6 渗透测试

智能音箱生产者应委托众测平台开展网络安全众测，并满足如下要求：

a) 测试时间应不少于 14 天，发现高危及以上级别漏洞，测试立即终止，本轮测试结束；

b) 参与测试主体不少于 20 个，且具备相关领域漏洞发现能力，以及相关领域漏洞发现项目经验；

c) 对测试中发现的可被利用的中危漏洞进行修复，经众测平台确认后，获得网络安全众测报告。

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

附录 A

（规范性）

不同安全能力等级的产品应符合的安全要求

表A.1列出了智能音箱基础级、增强级和领先级应符合的安全要求。

表A.1 不同网络安全能力等级的产品应符合的安全要求

技术要求		基础级要求对应章条号	增强级要求对应章条号	领先级要求对应章条号
物理与硬件安全	设备标识与信息	5.1.1	6.1.1	7.1.1
	物理接口安全	—	6.1.2	7.1.2
	安全启动	—	6.1.3	7.1.3
系统与软件安全	身份鉴别	5.2.1	6.2.1	7.2.1
	操作系统安全	5.2.2	6.2.2	7.2.2
	软件安全	5.2.3	6.2.3	7.2.3
	关键安全参数保护	5.2.4	6.2.4	7.2.4
	密码应用	5.2.5	6.2.5	7.2.5
	访问控制	5.2.6	6.2.6	7.2.6
	日志记录	—	6.2.7	7.2.7
	固件安全	—	6.2.8	7.2.8
网络与通信安全	端口安全	5.3.1	6.3.1	7.3.1
	通信安全	5.3.2	6.3.2	7.3.2
数据安全与个人信息保护	数据安全	5.4.1	6.4.1	7.4.1
	语音安全	5.4.2	6.4.2	7.4.2
	个人信息保护	5.4.3	6.4.3	7.4.3
安全保障	漏洞管理	5.5.1	6.5.1	7.5.1
	内容安全管理	5.5.2	6.5.2	7.5.2
	大模型使用安全管理	5.5.3	6.5.3	7.5.3
	产品生命周期管理	—	6.5.4	7.5.4
	代码安全	—	6.5.5	7.5.5
	渗透测试	—	—	7.5.6

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

附录 B

（资料性）

测试评价方法

B.1 基础级测评

B.1.1 物理与硬件安全

B.1.1.1 设备标识与信息

设备标识与信息的测评方法如下：

a) 测试方法：

1) 检查设备标识是否具有保证设备标识唯一性的说明；尝试通过管理界面、接口、平台等对设备标识进行修改；

2) 检查设备外观的名称、型号等信息是否清晰；核查用户配置界面、管理 APP 等位置的相关信息是否与外观一致。

b) 预期结果：

1) 设备具有保证设备标识唯一性的说明；

2) 设备外观清晰标识出设备的名称、型号等信息，并且与用户配置界面、管理 APP 等位置的信息一致；无法对唯一性标识进行修改。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2 系统与软件安全

B.1.2.1 身份鉴别

身份鉴别的测评方法如下:

a) 测试方法:

1) 检查控制单元与音箱绑定后，在控制单元未解除绑定前，是否可以由其他账号绑定音箱;

2) 查阅产品说明文档，检查产品中是否存在未公开的账号和登录方式，账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键;

3) 针对控制单元为移动互联网应用程序的，检查控制单元是否对用户身份进行了标识和鉴别，以及是否采取了用户身份鉴别凭证安全保护措施;

4) 针对使用口令进行身份鉴别的，检查是否禁止使用弱口令，口令是否少于 8 个字符，是否至少包含数字、小写字母、大写字母以及特殊字符中的 2 类字符。

b) 预期结果:

1) 控制单元与音箱进行唯一关联，并采取防护措施防止关联关系被篡改;

2) 产品中不存在未公开的账号和登录方式，账号包括但不限于测试账号、运维账号、第三方软件中不使用的账号，登录方式包括但不限于特殊组合键；

3) 控制单元为移动互联网应用程序的，控制单元对用户身份进行标识和鉴别，对用户身份鉴别凭证进行安全保护；

4) 针对使用口令进行身份鉴别的，禁止使用弱口令，口令不少于 8 个字符，至少包含数字、小写字母、大写字母以及特殊字符中的 2 类字符。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.2 操作系统安全

操作系统安全的测评方法如下：

a) 测评方法：

查看音智能箱操作系统的应用程序信息,是否满足最小化原则；

b) 预期结果：

智能音箱操作系统的应用程序权限满足最小化原则；

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况

判定为“不符合”。

B.1.2.3 软件安全

软件安全的测评方法如下

a) 测评方法：

1) 具有预置应用的，检查在预置应用更新时对更新包进行真实性和完整性校验；

2) 提供第三方应用安装功能的，检查是否默认不允许第三方应用软件自动安装。

b) 预期结果：

1) 具有预置应用的，在预置应用更新时对更新包进行真实性和完整性校验；

2) 提供第三方应用安装功能的，默认不允许第三方应用软件自动安装。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.4 关键安全参数保护

关键安全参数保护的测评方法如下：

a) 测试方法：

查看设备软件代码，检查代码中是否存在硬编码的关键安全参数。

b) 预期结果:

设备软件代码中不存在硬编码的关键安全参数。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.5 密码应用

密码应用的测评方法如下:

a) 测试方法:

查阅设备设计文档，确认身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术是否符合国家密码管理相关规定。

b) 预期结果:

身份鉴别、安全更新、网络通信、数据存储和安全启动等场景使用的加密技术符合国家密码管理相关规定。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.2.6 访问控制

a） 测试方法:

1) 查看音箱未绑定时，是否可以进行语音业务交互;

2) 账号 A 已绑定音箱，解除绑定关系，确认用户数据是

否清除；

3) 账号 A 已绑定音箱，账号 B 再绑定该音箱，确认账号 A 是否绑定该音箱；

4) 账号 A 和账号 B 通过控制单元，与音箱解除关联，确认用户数据是否清除。

b） 预期结果：

1) 音箱未绑定时，不能进行语音业务交互；

2) 账号 A 已绑定音箱，解除绑定关系，确认用户数据全部清除；

3) 账号 A 已绑定音箱，账号 B 再绑定该音箱，确认账号 A 与该音箱解绑。

4) 账号 A 和账号 B 通过控制单元，与音箱解除关联，确认用户数据已经清除。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.3 网络与通信安全

B.1.3.1 端口安全

a） 测试方法：

1) 查看智能音箱设备说明书中是否明确说明所有网络端口和服务，并说明对业务的影响；

2) 使用端口扫描工具识别设备在默认状态下开放的端口情况，与设备说明书中说明情况进行比对，检查。

b） 预期结果:

1) 说明书中明确说明所有网络端口和服务，并说明对业务的影响;

2) 设备网络端口开放遵循最小化原则，默认关闭非必须使用及未使用的网络端口。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.3.2 通信安全

通信安全的测评方法如下:

a） 测试方法:

1) 使用网络抓包工具查看数据传输（如设备与管理端、设备与服务器交互）是否采用加密技术;

2) 检查用户数据向外传输时是否使用安全传输通道。

b） 预期结果:

1) 设备使用了加密技术保护数据传输的真实性、机密性、完整性;

2) 用户数据向外传输时使用安全传输通道。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4 数据安全与个人信息保护

B.1.4.1 数据安全

数据安全的测评方法如下:

a） 测试方法:

查阅产品说明书、管理端操作指南等文档，确认是否明确标注信息清除功能的提供主体及操作路径，检查产品本地界面或管理端是否存在信息清除功能入口，使用专业数据恢复工具对清除后的存储介质进行数据恢复尝试，验证是否残留可识别的原始数据。

b） 预期结果:

产品的数据销毁为用户提供符合 GB 46864—2025 要求的信息清除功能，以简单便捷的方式从设备中删除数据。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4.2 语音安全

语音安全的测评方法如下:

a） 测试方法:

1) 音箱未联网时，是否可以唤醒，确认唤醒词是否存在本

地；

2) 唤醒后，是否有明显持续的指示灯提示；

3) 确认物理按键静音后，是否可以唤醒；

4) 静默状态，用户语音是否传输上云，是否本地存储用户语音。

b） 预期结果：

1) 音箱未联网时，可以正常唤醒；

2) 唤醒后，有明显持续的指示灯提示；

3) 确认物理按键静音后，不能唤醒；

4) 静默状态，用户语音未传输上云，用户语音未本地存储。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.4.3 个人信息保护

个人信息保护的测评方法如下：

a） 测试方法：

1) 检查产品管理相关界面、说明书、外包装盒等载体确认是否提供个人信息处理规则的访问入口或明确链接，验证是否提供在线查阅、复制文本或下载功能；核查处理规则内容是否符合 5.3.2 a）的要求；

2) 审查产品的个人信息收集流程，核查收集的个人信息种

类；验证同意的可撤回性，审查产品是否存在未经用户同意，通过隐蔽方式（如后台静默收集）获取个人信息的情况；

3) 审查产品个人信息处理规则、隐私政策等文档，核查存储期限的合理性，检查存储方式的安全性，验证跨境存储合规性，敏感个人信息的传输和存储的合规性；

4) 审查未经用户同意，是否对所收集语音等与个人的身份进行关联分析；

5) 审查产品个人信息处理规则，处理用户敏感个人信息是否符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

b） 预期结果：

1) 产品提供了个人信息处理规则并符合 5.3.2a）的要求；

2) 产品个人信息收集符合 GB/T 35273—2020 中 5.2、5.4 的要求；

3) 产品个人信息存储符合 GB/T 35273—2020 中 6.1、6.3 的要求；

4) 审查未经用户同意，不对所收集语音等与个人的身份进行关联分析；

5) 处理用户敏感个人信息符合 GB/T 45574—2025 中第 5 章及 6.1 的要求。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判为“不符合”。

B.1.5 安全保障

B.1.5.1 漏洞管理

漏洞管理的测评方法如下:

a） 测试方法:

1) 检查产品的所有漏洞，核查产品是否存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及以上级别漏洞;

2) 验证产品是否在规定或当事人约定期限内持续进行安全更新，核查产品是否建立和执行产品安全缺陷、漏洞的应急响应机制和流程，并对在运行和维护阶段发现的安全缺陷、漏洞进行响应;

3) 检查产品生产者管理制度和相关文件，是否建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应;

4) 检查产品生产者管理制度和相关文件，是否在发现设备存在安全缺陷、漏洞时，按照《网络产品安全漏洞管理规定》，向工业和信息化部网络安全威胁和漏洞信息共享平台报送相关漏洞信息，并及时告知用户安全

风险。

b） 预期结果：

1) 产品不存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及高危以上级别漏洞；

2) 持续进行安全更新，建立和执行产品安全缺陷、漏洞的应急响应机制和流程，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应；

3) 建立和执行产品的软硬件及相关组件的安全缺陷、漏洞的跟踪和应急响应机制，对产品在运行和维护阶段发现的安全缺陷、漏洞进行响应；

4) 发现安全缺陷、漏洞时，产品立即按照国家网络安全监测预警和信息通报制度等相关规定采取修复或替代方案等补救措施，并及时告知用户安全风险，向有关主管部门报告。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.5.2 内容安全管理

内容安全管理的测评方法如下：

a） 测试方法：

1) 查看企业制度文档、内容安全监测日志等，确认是否建

立内容安全机制，对所提供的信息内容进行持续安全监测，是否及时对监测发现的违法不良信息技术进行处置；

2) 查阅产品说明书、管理端操作指南等文档，确认是否提供违法和不良网络信息内容举报途径。

b） 预期结果：

1) 建立内容安全机制，对所提供的信息内容进行持续安全监测，是否及时对监测发现的违法不良信息技术进行处置；

2) 明确提供违法和不良网络信息内容举报途径。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.1.5.3 大模型使用安全管理

大模型使用安全管理的测评方法如下：

a） 测试方法：

确认所使用的大模型是否已通过生成式人工智能服务备案。

b） 预期结果：

使用的大模型已通过生成式人工智能服务备案。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况

判定为“不符合”。

B.2 增强级测评

B.2.1 物理与硬件安全

B.2.1.1 设备标识与信息

在满足 B.1.1.1 的测评方法的同时，还应满足如下测试方法、预期结果和结果判定:

a） 测试方法:

检查产品是否采取防护措施保护唯一标识不被篡改，审查产品设计文档，确认唯一设备标识的存储位置及防篡改机制。

b） 预期结果:

产品采取防护措施保护唯一标识不被篡改。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.1.2 物理接口安全

物理接口安全的测评方法如下:

a） 测试方法:

1) 检查产品非拆机状态下，调试接口出厂时是否不可访问;

2) 检查产品哪些物理接口与调试接口的功能和相关性，核

查非相关的物理接口与调试接口出厂时是否全部关闭。

b） 预期结果:

1) 非拆机状态下，可调试物理接口不可访问;

2) 产品在出厂时关闭非必要物理接口和调试接口。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.1.3 安全启动

安全启动的测评方法如下:

a） 测试方法:

检查产品是否对固件和启动组件的真实性和完整性进行校验；核查校验后产品的安全启动机制能否正常启动。

b） 预期结果:

产品实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验通过后方可正常启动。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2 系统与软件安全

B.2.2.1 身份鉴别

在满足 B.1.2.1 的测评方法的同时，还满足如下测试方法、预期

结果和结果判定:

a） 测试方法:

1) 使用未授权用户、伪造授权信息或过期授权信息尝试操作;

2) 检查具备声纹识别功能的，在采集声纹语音样本前是否结合其它身份鉴别手段对用户身份进行认证。

b） 预期结果:

1) 未授权用户、伪造授权信息或过期授权信息均无法对智能音箱进行操作;

2) 具备声纹识别功能的，在采集声纹语音样本前采取了其它身份鉴别手段。

c） 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.2 操作系统安全

在满足 B.1.2.1 的测评方法的同时，满足如下测试方法、预期结果和结果判定:

a） 测试方法:

检查系统进程和应用默认权限; 尝试获得 root、administrator 或同等超级用户权限。

b） 预期结果:

系统进程和应用不能取得超级用户权限。

c） 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.3 软件安全

在满足 B.1.2.3 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测评方法：

1) 提供第三方应用的，检查是否校验应用安装包或更新包的完整性和来源的真实性；

2) 具有预置应用以及提供第三方应用安装功能的，检查是否具备对应用访问权限进行控制。

b) 预期结果：

1) 提供第三方应用的，校验应用安装包或更新包的完整性和来源的真实性；

2) 具有预置应用以及提供第三方应用安装功能的，检查是否具备对应用访问权限进行控制。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.4 关键安全参数保护

在满足 B.1.2.4 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

1) 查阅产品设计文档，检查是否采用了密码技术对关键安全参数进行保护;

2) 查阅产品设计文档，检查是否建立了规范的关键安全参数的安全管理流程，例如密钥生成、密钥配置、密钥使用、密钥存储、密钥吊销、密钥销毁等;

3) 查阅产品设计文档，检查是否保证设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

b) 预期结果:

1) 产品采用了密码技术对关键安全参数进行保护;

2) 建立了规范的关键安全参数的安全管理流程;

3) 设备重要的关键安全参数对每个设备是唯一的，设备重要的关键安全参数包括但不限于设备根密钥、保证安全更新真实性和完整性的密钥、保证网络通信机密性和完整性的密钥。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.5 密码应用

应满足 B.1.2.5 的测评方法。

B.2.2.6 访问控制

在满足 B.1.2.6 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 审查其他账号是否需要主账号授权，才具备访问权限；

2) 审查是否只有主账号可以修改设备配置；具有屏幕的音箱，是否提供口令验证等方式对通过屏幕修改设备配置进行保护；

3) 具有授权功能的产品：

(1) 查阅产品设计文档，检查访问控制策略是否满足最小授权原则，尝试用设备管理员以外的用户访问受控资源或使用关键功能验证是否成功；

(2) 尝试用设备管理员以外的用户访问权限分享功能，验证是否能访问成功；

(3) 查阅产品设计文档，检查是否采取防护措施保障

分享的安全性。

b) 预期结果：

1) 具有设备绑定功能的产品；

2) 只有主账号可以修改设备配置；具有屏幕的音箱，提供口令验证等方式对通过屏幕修改设备配置进行保护；

3) 具有授权功能的产品：

(1) 设备访问控制策略满足最小授权原则，不允许主账号以外的用户访问受控资源或使用关键功能；

(2) 只能由主账号具备访问权限分享功能，其它用户不具备权限分享功能；

(3) 产品具备防护措施保障分享的安全性。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.7 日志记录

日志审计的测评方法如下：

a) 测试方法：

1) 检测产品日志，是否对开关机、创建用户、更改配置、安装与卸载软件、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，审计记录应包括

事件类型、事件发生时间、触发事件的主体、事件处理结果等信息；

2) 查阅设计文档，对于审计日志有哪些保护机制，检查产品是否具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏。尝试对日志进行非授权修改和删除；

3) 检测产品日志，检查产品是否具备审计日志存储保护机制，日志存储量超过阈值后是否正常记录最新事件；

4) 检查日志是否存储于非易失性存储介质。

b) 预期结果：

1) 能对开关机、创建用户、更改配置、软件升级、修改口令、登录失败、特权用户登录等事件进行记录，审计记录应包括事件类型、事件发生时间、触发事件的主体、事件处理结果等信息；

2) 产品具备对日志记录的访问权限控制等保护机制，使其免遭非法访问、篡改及破坏；

3) 产品具备审计日志存储保护机制，日志存储量超过阈值后正常记录最新事件；

4) 日志保存于非易失性存储介质。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.2.8 固件安全

固件安全的测评方法如下：

a) 测试方法：

1) 查阅开发者文档是否具有对固件升级包进行完整性校验和真实性校验的方法说明；分别使用满足完整性和真实性的固件升级包和不满足完整性和真实性的固件升级包进行验证，查看是否具有完整性和真实性校验过程和结果，查看升级是否成功；

2) 查阅设备说明文档，检查系统是否具备自动或人工更新、更新中止后重新更新的功能；

3) 查阅设备说明文档，检查系统更新是否具备防非授权回退校验机制；尝试非授权更新低版本固件，验证是否成功；

4) 查阅设备说明文档，检查设备第一次使用或恢复出厂设置后是否提示进行安全更新。

b) 预期结果：

1) 固件升级具备安全校验机制，会验证更新固件的真实性和完整性；

2) 设备可通过自动、人工方式进行安全更新，更新中止

后可重新更新；

3) 系统更新具备防非授权回退校验机制，无法通过非授权方式更新低版本固件；

4) 设备在第一次使用或恢复出厂设置后会检查并提示进行安全更新。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.3 网络与通信安全

B.2.3.1 端口安全

在满足 B.1.3.1 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 未登录认证时，查看网络端口暴露的信息是否简化；

2) 验证是否可手动对网络端口和服务进行配置。

b) 预期结果：

1) 设备未认证状态下未暴露网络端口信息；

2) 用户可手动对网络端口和服务进行配置。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.3.2 通信安全

在满足 B.1.3.2 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

尝试重复发送已捕获的传输数据，验证是否能抵抗重放攻击。

b) 预期结果:

设备具有抵抗重放攻击的能力。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4 数据安全与个人信息保护

B.2.4.1 数据安全

在满足 B.1.4.1 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

1) 查阅设备说明书、管理端操作指南等文档，确认是否明确说明故障诊断日志上传的触发条件、告知方式及用户同意流程；模拟设备故障场景，观察是否触发日志上传告知流程；核查告知内容的完整性；验证告知方式的显著性；核查同意机制的有效性；

2) 查阅设备安全设计文档、技术白皮书，确认是否明确说明保护用户数据机密性和完整性的具体安全措施；用抓包工具捕获数据包，验证传输是否采用加密技术。

b) 预期结果：

1) 设备告知用户数据采集方式、范围、目的，并经用户同意后上传，告知内容完整，告知方式显著；

2) 设备采取加密等安全措施保护用户数据的机密性和完整性。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4.2 语音安全

在满足 B.1.4.2 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 模拟实际处理场景，查看用户语音数据处理完成后，是否默认丢弃，或者或使用可信执行环境等方式安全存储在本地；

2) 上传用户语音数据时，是否征得用户明示同意；

3) 上传的语音指令，是否默认不加入语料库、不输入大模型、不进行识别处理以外的语音分析。

b) 预期结果：

1) 用户语音数据处理完成后，应默认丢弃，或者或使用可信执行环境等方式安全存储在本地，不存储、传输与用户语音指令无关的用户谈话等内容；

2) 上传用户语音数据时，征得用户明示同意；

3) 上传的语音指令，默认不加入语料库、不输入大模型、不进行识别处理以外的语音分析。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.4.3 个人信息保护

在满足 B.1.4.5 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 查阅个人信息处理规则，确认对外提供个人信息的目的、方式、种类及接收方是否以清单形式列明；

2) 验证音箱控制单元是否有便捷通道（如设置页、客服入口）供用户行使个人信息权利，是否设置不合理限制条件。

b) 预期结果：

1) 设备对外提供个人信息相关内容以清单形式清晰列明；

2) 设备有便捷通道（如设置页、客服入口）供用户行使个人信息权利，无不合理限制条件。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5 安全保障

B.2.5.1 漏洞管理

应满足 B.1.5.1 的测评方法。

B.2.5.2 内容安全管理

应满足 B.1.5.2 的测评方法。

B.2.5.3 大模型使用安全管理

在满足 B.1.5.3 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

确认利用大模型为用户提供服务的，是否有明示信息征得用户同意。

b) 预期结果：

利用大模型为用户提供服务的，征得用户明示同意。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5.4 产品生命周期管理

产品生命周期管理的测评方法如下:

a) 测试方法:

1) 查阅产品管理文档，确认是否建立覆盖设计、开发、测试、交付、运维等环节的全生命周期网络安全管理机制;

2) 核查安全设计机制文档，是否参考 GB/T 39276—2020 第 5.2.2.1 项进行威胁建模，包含威胁识别、分析及缓解措施;

3) 查看开发安全文档，是否描述设计和开发过程中保障数据存储与传输机密性、完整性的机制和流程;

4) 核查安全开发机制相关文件，是否满足 GB/T 39276—2020 第 5.1.2.1 项要求;

5) 查阅安全测试机制文档及测试记录，确认定期或在重要版本发布前是否开展静态安全测试、动态安全测试等规定测试类型;

6) 检查安全交付机制文档及交付记录，确认产品交付和重要版本发布前是否执行安全审查和加固;

7) 核查安全运维机制和流程文档，是否满足 GB/T 39276—2020 第 5.1.2.3 项要求。

b) 预期结果:

1) 产品生产者建立了产品全生命周期网络安全管理机制，覆盖设计、开发、测试、交付、运维等环节；

2) 产品生产者建立了产品安全设计机制，参考 GB/T 39276—2020 第 5.1.2.1 项相关要求进行威胁建模，以识别、分析和缓解对设备的安全威胁；

3) 产品生产者编制了开发安全文档，描述设备设计和开发过程中实现数据存储和传输的机密性和完整性的机制和流程；

4) 产品生产者建立了产品安全开发机制，应满足 GB/T 39276—2020 第 5.1.2.1 项相关要求；

5) 产品生产者建立了安全测试机制，定期或在重要版本发布前进行安全测试，包括但不限于：静态安全测试、动态安全测试、API 测试、模糊测试、代码审查等；

6) 产品生产者建立了安全交付机制，在产品交付和重要版本发布前进行安全审查和加固；

7) 产品生产者建立安全运维机制和流程，应满足 GB/T 39276—2020 第 5.1.2.3 项相关要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.2.5.5 代码安全

代码安全的测评方法如下:

a) 测试方法:

1) 查验是否建立开源代码来源审查机制,使用开源组件和开源软件的，验证开源代码来源是否可信;

2) 查验是否建立开源代码安全漏洞跟踪和处置机制,对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

b) 预期结果:

1) 建立了开源代码来源审查机制,使用开源组件和开源软件的，开源代码来源可信;

2) 建立了开源代码安全漏洞跟踪和处置机制,对开源代码及制品中发现的高危及以上漏洞及时进行修复或缓解。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3 领先级测评

B.3.1 物理与硬件安全

B.3.1.1 设备标识与信息

应满足 B.2.1.1 的测评方法。

B.3.1.2 物理接口安全

应满足 B.2.1.2 的测评方法。

B.3.1.3 安全启动

应满足 B.2.1.3 的测评方法。

B.3.2 系统与软件安全

B.3.2.1 身份鉴别

在满足 B.2.2.1 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

登录系统尝试进行修改网络安全配置、访问敏感个人信息等操作，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

b) 预期结果:

进行修改网络安全配置，安全校验方式包括但不限于登录设备校验、网络环境、操作行为。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.2 操作系统安全

应满足 B.2.2.2 的测评方法。

B.3.2.3 软件安全

在满足 B.2.2.3 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

确认是否对应用软件安装、更新的传输通道进行加密。

b) 预期结果:

对应用软件安装、更新的传输通道进行加密。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.4 关键安全参数保护

在满足 B.2.2.4 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

查阅设备说明文档，检查是否采用安全芯片等硬件方式保护和使用密钥。

b) 预期结果:

设备采用安全芯片等硬件方式保护和使用密钥。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.2.5 密码应用

应满足 B.2.2.5 的测评方法。

B.3.2.6 访问控制

应满足 B.2.2.6 的测评方法。

B.3.2.7 日志记录

应满足 B.2.2.7 的测评方法。

B.3.2.8 固件安全

应满足 B.2.2.8 的测评方法。

B.3.3 网络与通信安全

B.3.3.1 端口安全

在满足 B.2.3.1 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

打开必须使用的端口开展业务，业务结束后验证端口是否自动或按设计关闭。

b) 预期结果:

打开必须使用的端口开展业务，业务结束后端口自动或按设计关闭。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.3.2 通信安全

应满足 B.2.3.2 的测评方法。

B.3.4 数据安全与个人信息保护

B.3.4.1 数据安全

应满足 B.2.4.1 的测评方法。

B.3.4.2 语音安全

在满足 B.2.4.2 的测评方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

1) 模拟实际处理场景，查看是否存在存储、传输与用户语音指令无关的用户谈话等内容的情况;

2) 具备声纹识别功能的，构建语音模仿、语音转换及合成、录音重放、录音拼接等常见声纹呈现攻击进行测试;

3) 提供声纹支付功能的智能音箱，查看声纹支付功能是否默认关闭，使用声纹支付时，是否要求双因子认证保障支付安全。

b) 预期结果:

1) 用户语音数据处理完成后，应默认丢弃，或者或使用可信执行环境等方式安全存储在本地，不存储、传输与用户语音指令无关的用户谈话等内容;

2) 具备声纹识别功能的，具备检测和抵御常见声纹呈现攻

击的能力；

3) 提供声纹支付功能的智能音箱，声纹支付功能默认关闭，使用声纹支付时，要求双因子认证保障支付安全。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.4.3 个人信息保护

在满足 B.2.4.3 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

查阅智能音箱的敏感个人信息处理相关文档，确认是否明确规定敏感个人信息脱敏处理的范围、方式及相关技术标准；确认是否包含至少一种及以上脱敏方式，确认脱敏方式的有效性、稳定性，是否能持续对敏感个人信息进行可靠脱敏，无明显漏洞。

b) 预期结果：

智能音箱生产者已制定完善的敏感个人信息脱敏处理相关文档，明确脱敏范围、方式及技术标准，覆盖拍摄、预览、存储、传输全环节；确认至少包含一种及以上脱敏方式，确认脱敏方式的有效性、稳定性，能持续对敏感个人信息进行可靠脱敏，无明显漏洞。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.5 安全保障

B.3.5.1 漏洞管理

应满足 B.2.5.1 的测评方法。

B.3.5.2 内容安全管理

在满足 B.2.5.2 的测评方法的同时，还满足如下测试方法、预期结果和结果判定：

a) 测试方法：

确认是否有未成年人模式选项，用户是否可以开启智能音箱未成年人模式，是否满足 GB/T 47694—2026 第 6.2 项相关要求。

b) 预期结果：

用户可以开启未成年人模式，满足 GB/T 47694—2026 第 6.2 项相关要求。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

B.3.5.3 大模型使用安全管理

应满足 B.2.5.3 的测评方法。

B.3.5.4 产品生命周期管理

应满足 B.2.5.4 的测评方法。

B.3.5.5 代码安全

在满足 B.2.5.4 的测试方法的同时，还满足如下测试方法、预期结果和结果判定:

a) 测试方法:

1) 进行代码检测，或查阅第三方检测机构出具的代码检测报告，检测对象为源代码或二进制程序，覆盖以下检测内容：是否存在软件安全漏洞和错误、第三方库和第三方组件中的安全漏洞、硬编码身份鉴别信息和关键安全参数；确认检测机构具备相应检测资质，检测流程符合规范；核查检测报告中的检测过程记录、原始数据及检测结论，确认检测内容无遗漏、检测方法科学合理，检测结果真实有效;

2) 核查产品是否存在使用应用程序进行设备管理的情况；若存在，进行管理应用程序检测，或查阅第三方检测机构出具的设备管理应用程序检测报告，检测对象为源代码或二进制程序，覆盖以下检测内容：是否存在硬编码关键安全参数、通过明文存储或传输关键安全参数和敏感个人信息、违规收集敏感个人信息；确认检测机构具备相应检测资质，检测流程符合规范；核

查检测报告中的检测过程记录、原始数据及检测结论，确认检测内容无遗漏、检测方法科学合理，检测结果真实有效。

b) 预期结果：

1) 委托第三方检测的，检测机构具备相应资质；对设备自身代码进行全面检测，检测内容覆盖软件安全漏洞和错误、第三方库和第三方组件中的安全漏洞、硬编码身份鉴别信息和关键安全参数，检测结论为合格（无中风险及以上漏洞）；核查检测报告中的检测过程记录、原始数据及检测结论，检测内容无遗漏、检测方法科学合理，检测结果真实有效。

2) 使用应用程序对设备进行管理的，如委托第三方检测，检测机构具备相应资质；对设备管理应用程序进行全面检测，检测内容覆盖硬编码关键安全参数、通过明文存储或传输关键安全参数和敏感个人信息、违规收集敏感个人信息，检测结论为合格（无相关违规问题，或发现的问题已完成整改）；核查检测报告中的检测过程记录、原始数据及检测结论，检测内容无遗漏、检测方法科学合理，检测结果真实有效。

c) 结果判定：

实际测试结果与预期结果一致则判定为“符合”，其他情况

判定为“不符合”。

B.3.5.6 渗透测试

智能音箱应委托众测平台开展网络安全众测，并满足如下测试方法、预期结果和结果判定：

a) 测试方法：

1) 众测平台搭建隔离仿真测试环境，明确测试边界，执行完整六阶段众测流程；测试时间应不少于 14 天，测试参与主体应不少于 20 个；

2) 终端设备测试应包含设备固件、OTA 升级程序；开展物理硬件安全、系统软件安全测试，覆盖安全启动、口令鉴别、固件安全、访问控制、日志审计等安全维度；设备管理应用程序测试应包含测试身份认证、会话管理、本地数据存储、输入校验、敏感信息保护等；还应包含设备、配套 app 与管理平台的数据传输、身份认证、权限服务等；

3) 测试过程中如发现高危及以上级别漏洞，测试立即终止，本轮测试结束；测试过程中发现的可被利用的中危漏洞，厂商进行修复，并交众测平台进行确认。

b) 预期结果：

1) 由众测平台搭建的隔离仿真测试环境，测试时间不少于 14 天，参与测试主体（推荐包含智能体）不少于 20 个，

执行完整六阶段众测流程;

2) 在测试中未发现高危漏洞，发现的可被利用的中危漏洞厂商均已进行修复，并经平台确认。

3) 检测报告完整规范，包含检测资质证明、检测流程、检测内容、检测数据、检测结论等核心要素，检测过程符合相关标准要求。

c) 结果判定:

实际测试结果与预期结果一致则判定为“符合”，其他情况判定为“不符合”。

附录 C
（规范性）
第三方检测机构能力要求

C.1 机构要求

第三方检测机构应满足如下要求：取得检验检测机构资质认定(CMA)或通过中国合格评定国家认可委员会(CNAS)实验室认可，CMA 批准的检验检测能力范围或 CNAS 认可能力范围涵盖网络安全检测相关内容。

C.2 人员要求

进行渗透测试的第三方检测机构应至少有 5 人专职从事渗透测试相关工作，相关人员应至少满足下列章条中的任意 1 项要求：

a) 具有 CISP-PTE、CISP-PTS 等渗透测试相关证书；

b) 具有渗透测试相关项目经历；

c) 具有 5 年内通过合法方式挖掘安全漏洞并向国家权威漏洞库报送的经历；

d) 在国家级、省部级网络安全赛事获得奖励的人员。

参 考 文 献

[1] GB/T 38626—2020 信息安全技术 智能联网设备口令保护指南

[2] GB/T 38632—2020 信息安全技术 智能音视频采集设备应用安全要求

[3] GB/T 39720—2020 信息安全技术 移动智能终端安全技术要求及测试评价方法

[4] GB/T 41387—2022 信息安全技术 智能家居通用安全规范

全国网络安全标准化技术委员会 National Technical Committee 260 on Cybersecurity of SAC