TC260-PG-2026NA

网络安全标准实践指南

——网络安全标识 儿童智能手表安全要求

（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”）秘书处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

伴随着儿童智能手表的广泛应用，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，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和安全保障5个方面给出儿童智能手表网络安全能力要求，由低到高按照基础级、增强级、领先级划分为三个等级，适用于指导儿童智能手表的设计、开发、使用、维护和检测。

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 4
5.3 数据安全与个人信息保护 8
5.4 安全保障 11
6 增强级要求 13
6.1 物理与硬件安全 13
6.2 系统与软件安全 14
6.3 网络与通信安全 17
6.4 数据安全与个人信息保护 17
6.5 安全保障 18
7 领先级要求 20
7.1 物理与硬件安全 20
7.2 系统与软件安全 21
7.3 网络与通信安全 23
7.4 数据安全与个人信息保护 23
7.5 安全保障 23
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 26
附录 B（资料性）测试评价方法 27
B.1 基础级测评 27
B.2 增强级测评 49
B.3 领先级测评 67
附录 C（规范性）第三方检测机构能力要求 77
C.1 机构要求 77
C.2 人员要求 77
参　考　文　献 78

1 范围

本文件规定了儿童智能手表网络安全标识基础级、增强级、领先级三个等级的安全能力要求，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 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 46859—2025 儿童手表安全技术要求

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

儿童智能手表　children’s watches

供 3 周岁及以上、14 周岁以下儿童使用，具有信息处理功能的手表。

注：信息处理功能一般包括通话、定位、远程监护等。

[来源：GB 46859—2025，有修改]

3.2

关键安全参数　critical security parameter；CSP

与安全有关，其泄露或修改会危及密码模块安全的信息。

示例：秘密和私有密码密钥、口令之类的鉴别数据、个人标识码（PIN）、证书或其他信息锚。

注：儿童智能手表中重点保护的关键安全参数包括设备根密钥、用户身份鉴别信息、设备鉴别信息、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。

[来源：GB/T 25069—2022，有修改]

3.3

儿童智能手表管理端　management terminal for children’s smart watches

儿童智能手表进行管理的设备、应用或网页等。

3.4

单独同意　separate consent

监护人针对儿童个人信息进行特定处理而专门作出具体、明确授

权的行为，不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。

注：单独同意的告知内容与取得同意的方式需要其他处理活动予以区分。

[来源：GB/T 42574—2022，有修改]

3.5

移动互联网未成年人模式　mobile internet minors mode

移动智能终端、移动互联网应用程序和移动互联网应用程序分发平台具有的，专门面向未成年人使用的特定安全功能集合。

注：本文件中的移动互联网未成年人模式指面向3周岁及以上、14周岁以下儿童提供的模式。

[来源：GB/T 47694—2026，有修改]

4　概述

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和安全保障5个方面构建儿童智能手表安全框架（见图1）。

儿童智能手表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。

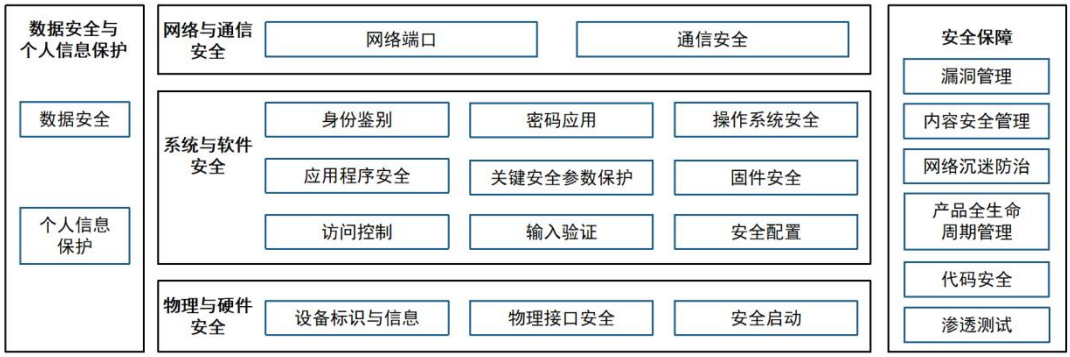


图1 儿童智能手表安全框架

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

儿童智能手表应具有唯一设备识别码。

注：常见不可变更的唯一设备标识码包括括国际移动设备识别码（IMEI）、移动设备识别码（MEID）、设备媒体访问控制地址(MAC 地址)、硬件序列号、集成电路卡识别码（ICCID）、国际移动用户识别码（IMSI）等。

5.2 系统与软件安全

5.2.1 身份鉴别

5.2.1.1 通用要求

儿童智能手表应满足如下要求：

a) 对用户身份进行唯一标识，并采取防护措施防止标识被篡

改；

b) 不存在未公开的账号和登录方式；

c) 通过网络登录设备，对访问主体进行身份鉴别；

注：登录设备方式包括但不限于 WEB 管理界面、管理应用程序等。

d) 身份鉴别错误锁定功能符合 GB 46859—2025 中 4.6.4 的要求；

e) 登录错误密码找回功能符合 GB 46859—2025 中 4.6.5 的要求；

f) 密码组合校验功能符合 GB 46859—2025 中 4.6.6 的要求；

g) 开机和锁屏时的密码保护功能符合 GB 46859—2025 中 4.6.3 的要求。

5.2.1.2 生物特征识别

儿童智能手表具备生物特征识别功能的应满足如下要求：

a) 生物特征识别功能具备防假体呈现攻击检测能力，其中防假体攻击的种类应符合 GB 46859—2025 中附录 C 的要求；

b) 不将生物特征识别功能作为注册和登录、解锁、支付、注销和删除、家长管理控制等功能的唯一验证方式。

5.2.1.3 儿童智能手表管理端身份鉴别

具有儿童智能手表管理端的应满足如下要求：

a) 使用口令登录的，口令在使用过程中禁止明文显示和存储；

b) 使用口令登录的，口令长度不少于 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两类字符，禁

止使用弱口令。

5.2.2 密码应用

儿童智能手表中用于身份鉴别、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密码技术应符合国家密码管理相关规定。

5.2.3 操作系统安全

儿童智能手表操作系统应满足如下要求：

a) 操作系统升级功能符合 GB 46859—2025 中 4.6.1 的要求；

b) 不向儿童智能手表上安装的第三方应用程序提供不可变唯一设备标识码；

c) 权限管控功能符合 GB 46859—2025 中 4.7.6 的要求；

d) 出厂时，默认关闭所有敏感权限。

5.2.4 应用程序安全

儿童智能手表应满足如下要求：

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，禁止应用自动安装和更新，第三方应用安装和更新时，检验安装包的完整性和真实性；

c) 预置应用程序卸载功能符合 GB 46859—2025 中 4.7.3 的要求；

d) 恶意应用程序防范功能符合 GB 46859—2025 中 4.6.2 的要

求；

e) 预置应用中包含网络音视频、网络直播、网络游戏、网络社交等服务的，默认为移动互联网未成年人模式，不得提供可退出移动互联网未成年人模式选项；

f) 提供开启或关闭移动互联网未成年人模式选项的预置应用，在应用首次开启前，应通过管理端获得监护人开启或关闭未成年人模式的授权，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

g) 当预置应用中包含应用程序分发平台时，满足如下要求：

1) 应用程序分发平台为儿童提供适宜儿童身心健康和年龄特点的应用程序，并在显著位置清晰标注应用程序的推荐年龄，同时明确标注该应用程序是否支持未成年人模式；

2) 当预置应用中包含应用程序分发平台时，应用程序分发平台应明示未成年人模式与成年人模式在敏感个人信息处理方面、功能方面、未成年人权限管控等方面的区别。

h) 核查安装的应用是否提供未成年人模式，无未成年人模式的，通过管理端向监护人推送该应用不具备未成年人模式的提醒；

i) 预置应用提供网络社交服务、直播服务、浏览器服务、搜索引擎服务、电商服务、游戏服务、教育服务的，满足 GB/T 47694—2026 中 6.3 关于未成年人模式的要求。

5.2.5 关键安全参数保护

儿童智能手表应满足如下要求：

a) 使用密码技术保护身份鉴别信息的机密性、完整性；

b) 不在设备软件代码中硬编码关键安全参数。

5.2.6 访问控制

儿童智能手表管理端应满足如下要求：

a) 在儿童智能手表首次与儿童智能手表管理端绑定时，管理端与儿童智能手表进行交互确认；

注：交互方式包括但不限于按键、蓝牙或无线网络配对、二维码、数字校验码等。

b) 多个儿童智能手表管理端绑定同一个儿童智能手表时，设置主管理端，仅接受主管理端的控制指令；

c) 解绑通过管理端授权等方式确认完成，儿童智能手表不能通过清理后台或重启等方式解除绑定。

5.3 数据安全与个人信息保护

5.3.1 数据安全

儿童智能手表应满足如下要求：

a) 数据销毁符合 GB 46864—2025 要求的信息清除功能；

b) 设备解绑和账号注销功能符合 GB 46859—2025 中 4.7.9 的

要求。

5.3.2 个人信息保护

儿童智能手表应满足如下要求：

a) 为儿童提供信息发布、即时通讯等服务的，儿童智能手表生产者应依法要求儿童或者其监护人提供未成年人真实身份信息，儿童或者监护人不提供未成年人真实身份信息的，儿童智能手表不得为未成年人提供相关服务；

b) 个人信息收集功能符合 GB/T 35273—2020 中 5.1、5.2、5.3 的要求，且不得强制要求儿童或者其监护人同意非必要的个人信息处理行为，不得因为儿童或者其监护人不同意处理儿童非必要个人信息或者撤回同意，拒绝儿童使用其基本功能服务；

c) 收集个人生物识别信息前，单独向监护人告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得监护人的明示同意；个人生物识别信息与个人身份信息分开存储；

d) 制定专门的儿童个人信息处理规则，并在儿童智能手表或手表管理端相关界面展示，个人信息处理规则符合 GB/T 35273—2020 中 5.5 的要求；

e) 传输和存储个人敏感信息时，采用加密等安全措施，存储期限符合 GB/T 35273—2020 中 6.1 的要求；

f) 儿童智能手表个人行使权利满足如下要求：

1) 在手表端或手表管理端提供便捷的查阅儿童个人信息种类、数量等的方法和途径，不得对儿童或者其监护人的合理请求进行限制；

2) 提供便捷的儿童或其监护人复制、更正、补充、删除儿童个人信息的功能，不得设置不合理条件；

3) 在15个工作日或者法律法规规定的期限内受理并处理儿童或其监护人查阅、复制、更正、补充、删除儿童个人信息的申请，拒绝儿童或其监护人行使权利的请求的，应当书面告知申请人并说明理由；

4) 对于儿童个人信息转移、删除等可能对儿童权益产生较大影响的权利行使情形，儿童智能手表需在管理端向监护人明示告知，并支持监护人选择是否行使相关权利。

g) 儿童个人信息对外提供功能符合GB 46859—2025中4.7.7的要求；

h) 涉及使用自动化决策方式处理儿童个人信息的功能符合GB 46859—2025中4.7.4的要求；

i) 儿童智能手表网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止信息

扩散；通过未成年人私密信息发现未成年人可能遭受侵害的，应当立即采取必要措施保存有关记录，并向公安机关报告。

5.4 安全保障

5.4.1 漏洞管理

儿童智能手表应满足如下要求：

a) 确保设备不存在已知的高危及以上等级的漏洞；

注：已知高危漏洞参考 CNVD、CNNVD、NVDB 等国家漏洞库。

b) 明确并公示设备的型号，在规定或当事人约定期限内，持续进行安全更新；

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；

d) 发现设备存在安全缺陷、漏洞时，应按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

5.4.2 内容安全管理

儿童智能手表应满足如下要求：

a) 内容安全要求应满足 GB 46859—2025 中 4.8.1 的要求；

b) 建立网络欺凌行为的预警预防、识别监测和处置机制，并满足：

1) 建立网络欺凌信息特征库，通过技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测；

2) 提供儿童及其监护人保存遭受网络欺凌记录、行使通知权利的功能、渠道；

3) 提供儿童设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。

c) 建立对儿童发布信息内容进行持续内容安全监测的机制，当监测出违法不良信息或不适宜供儿童查看的内容时，应立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施，并保存有关记录，并对制作、复制、发布、传播上述信息的用户采取警示、限制功能、暂停服务、关闭账号等处置措施。

5.4.3 网络沉迷防治

5.4.3.1 时长管控

儿童智能手表时长管控功能应满足GB 46859—2025中4.9.1的要求。

5.4.3.2 应用管控

儿童智能手表应用管控功能应满足GB 46859—2025中4.9.2的要求。

5.4.3.3 付费管控

儿童智能手表付费管控功能应满足 GB 46859—2025 中 4.10 的要求。

5.4.3.4 其他要求

儿童智能手表应满足如下要求:

a) 支持拨打紧急电话，如 110、119、120、紧急联络人等，支持上报信息至儿童智能手表管理端;

b) 当收到骚扰电话、诈骗短信等信息时，儿童智能手表管理端收到相应的预警提示;

c) 不设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，不提供泛娱乐化功能和内容诱导未成年人沉迷网络;

d) 不利用算法推荐服务诱导未成年人沉迷网络;

e) 挂失功能应满足 GB 46859—2025 中 4.11 的要求;

f) 交换电话号码功能应满足 GB 46859—2025 中 4.18 的要求。

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识别码不被篡改。

6.1.2 物理接口安全

儿童智能手表在出厂时应关闭非必要物理接口和调试接口。

6.1.3 安全启动

儿童智能手表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。

6.2 系统与软件安全

6.2.1 身份鉴别

6.2.1.1 通用要求

应满足 5.2.1.1 的要求。

6.2.1.2 生物特征识别

应满足 5.2.1.2 的要求。

6.2.1.3 儿童智能手表管理端身份鉴别

在满足 5.2.1.3 的要求的同时，儿童智能手表管理端使用短信验证码登录的，还应满足短信验证码具有防重放攻击机制。

6.2.2 密码应用

应满足 5.2.2 的要求。

6.2.3 操作系统安全

在满足 5.2.3 的要求的同时，还应满足如下要求：

a) 操作系统升级具备安全校验机制，验证更新系统的真实性和完整性；

b) 具备非授权操作系统版本防回退校验机制；

c) 有新操作系统版本时，在手表管理端提示监护人进行安全更新，支持自动或手动方式进行升级，更新中止后能重新更新；

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。

6.2.4 应用程序安全

在满足 5.2.4 的要求的同时，还应满足如下要求：

a) 默认关闭儿童智能手表操作系统基本功能外的服务，操作系统基本功能详见 GB 46859—2025 中 4.7.3 的要求；

b) 儿童智能手表操作系统升级时，已卸载的预置应用软件不在未经儿童智能手表管理端授权的情况下被恢复，且升级后的预置应用软件仍满足本文件要求；

c) 允许监护人通过儿童智能手表管理端对儿童智能手表进行应用管理，应用市场的内容在监护人授权的情况下安装、禁用/卸载；

d) 儿童智能手表外链打开和下载操作，要求监护人验证，提供监护人外链打开一键豁免功能；

e) 儿童智能手表支持通过非预置应用程序分发平台安装应用的，建立应用程序分发平台准入白名单，白名单内的应用程序分发平台满足 5.2.4 的要求；

f) 所有预置应用默认启用移动互联网未成年人模式，若提供

可退出移动互联网未成年人模式选项的，需经管理端监护人授权后方可关闭，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

g) 儿童智能手表不得安装无未成年人模式的应用。

6.2.5 关键安全参数保护

在满足 5.2.5 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。

6.2.6 访问控制

应满足 5.2.6 的要求。

6.2.7 固件安全

儿童智能手表应满足如下要求：

a) 固件升级具备安全校验机制，验证更新系统的真实性和完整性；

b) 具备非授权固件版本防回退校验机制；

c) 有新固件版本时，在手表管理端提示监护人进行安全更新，支持自动或手动方式进行升级，更新中止后能重新更新；

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。

6.2.8 输入验证

儿童智能手表应对通过用户界面输入的数据进行安全验证，以避免数据处理过程中出现意外行为。

注：数据处理过程中出现的意外行为包括但不限于 SQL 注入、操作系统命令注入和路径遍历等。

6.2.9 安全配置

儿童智能手表应默认提供安全的配置，并向用户提供安全设置的指导。

6.3 网络与通信安全

6.3.1 通信安全

儿童智能手表应满足如下要求：

a) 采用密码技术保证通信过程中数据的机密性和完整性；

b) 具有抵抗重放攻击的能力。

6.3.2 网络端口

儿童智能手表应满足如下要求：

a) 网络服务和网络端口开放遵循最小化原则，默认关闭非必须使用的网络服务和网络端口；

b) 未认证状态下减少网络端口暴露信息；

c) 监护人可在管理端关闭非必要的网络服务。

6.4 数据安全与个人信息保护

6.4.1 数据安全

在满足 5.3.1 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，明确告知监护人数据采集方式、范围、目的，经监护人同意后上传；

b) 当数据存储在儿童智能手表端时，为数据提供访问控制机制，防止未授权访问。

6.4.2 个人信息保护

在满足 5.3.2 的要求的同时，还应满足如下要求：

a) 设置便捷的交互式页面提供功能或选项，便于用户在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

b) 具有生物识别功能的，仅存储个人生物识别的摘要信息，不存储原始个人生物识别信息。

6.5 安全保障

6.5.1 漏洞管理

应满足 5.4.1 的要求。

6.5.2 内容安全管理

应满足 5.4.2 的要求。

6.5.3 网络沉迷防治

6.5.3.1 时长管控

在满足 5.4.3.1 的要求的同时，还应满足防止通过修改儿童智能手表系统日期、时间的设置绕过使用时间和时长的管理。

6.5.3.2 应用管控

在满足 5.4.3.2 的要求的同时，还应满足支持管理端屏蔽儿童智能手表内安装的应用程序，应急类和基本功能类应用除外。

6.5.3.3 付费管控

应满足 5.4.3.3 的要求。

6.5.3.4 其他要求

应满足 5.4.3.4 的要求。

6.5.4 产品全生命周期管理

儿童智能手表生产者应满足如下要求：

a) 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；

b) 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) 启用儿童智能手表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。

c) 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；

d) 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；

e) 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；

f) 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；

g) 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。

6.5.5 代码安全

儿童智能手表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，确保开源代码来源可信；

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

7.2.1.1 通用要求

在满足 6.2.1.1 的要求的同时，还应满足对于修改网络安全配置、访问儿童个人信息等重要操作，使用与设备登录不同的因子进行认证，或对操作环境进行安全校验。

注：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。

7.2.1.2 生物特征识别

应满足 6.2.1.2 的要求。

7.2.1.3 儿童智能手表管理端身份鉴别

应满足 6.2.1.3 的要求。

7.2.2 密码应用

应满足 6.2.2 的要求。

7.2.3 操作系统安全

在满足 6.2.3 的要求的同时，还应满足当儿童智能手表访问恶意网址信息时，管理端即收到相应的预警提示。

7.2.4 应用程序安全

在满足 6.2.4 的要求的同时，还应满足如下要求：

a) 应用程序发生安全事件时，生产者通过管理端向监护人推送安全告警；

b) 支持监护人在管理端对预置应用程序进行敏感权限管控；

c) 基本功能软件内附带扩展功能软件（模块）时，提供卸载或禁用扩展功能软件（模块）的方式；

d) 所有预置应用默认启用移动互联网未成年人模式，不提供移动互联网未成年人模式的退出选项；

e) 建立应用未成年人模式符合性监测机制，在应用更新、版本迭代或收到相关风险信息时，重新评估其符合性；若监测发现不符合未成年人模式要求，通过管理端向监护人推送预警提示。

7.2.5 关键安全参数保护

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 固件安全

应满足 6.2.7 的要求。

7.2.8 输入验证

应满足 6.2.8 的要求。

7.2.9 安全配置

应满足 6.2.9 的要求。

7.3 网络与通信安全

7.3.1 通信安全

应满足 6.3.1 的要求。

7.3.2 网络端口

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 个人信息保护

在满足 6.4.2 的要求的同时，儿童智能手表具有生物识别功能的，还应满足生物特征值仅在儿童智能手表端侧存储和处理。

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

应满足 6.5.2 的要求。

7.5.3 网络沉迷防治

7.5.3.1 时长管控

在满足 6.5.3.1 的要求的同时，还应满足移动互联网应用程序卸载后，儿童智能手表不得对应用程序的使用时长进行归零统计。

7.5.3.2 应用管控

应满足 6.5.3.2 的要求。

7.5.3.3 付费管控

应满足 6.5.3.3 的要求。

7.5.3.4 其他要求

应满足 6.5.3.4 的要求。

7.5.4 产品全生命周期管理

应满足 6.5.4 的要求。

7.5.5 代码安全

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，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

儿童智能手表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。

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 列出了儿童智能手表基础级、增强级和领先级应符合的安全要求。

表A.1 不同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
	密码应用	5.2.2	6.2.2	7.2.2
	操作系统安全	5.2.3	6.2.3	7.2.3
	应用程序安全	5.2.4	6.2.4	7.2.4
	关键安全参数保护	5.2.5	6.2.5	7.2.5
	访问控制	5.2.6	6.2.6	7.2.6
	固件安全	—	6.2.7	7.2.7
	输入验证	—	6.2.8	7.2.8
	安全配置	—	6.2.9	7.2.9
网络与通信安全	通信安全	—	6.3.1	7.3.1
	网络端口	—	6.3.2	7.3.2
数据安全与个人信息保护	数据安全	5.3.1	6.4.1	7.4.1
	个人信息保护	5.3.2	6.4.2	7.4.2
安全保障	漏洞管理	5.4.1	6.5.1	7.5.1
	内容安全管理	5.4.2	6.5.2	7.5.2
	网络沉迷防治	5.4.3	6.5.3	7.5.3
	产品全生命周期管理	—	6.5.4	7.5.4
	代码安全	—	6.5.5	7.5.5
	渗透测试	—	—	7.5.6

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:

检查设备是否具有唯一设备识别码（包括但不限于 IMEI、MEID、MAC、硬件序列号、ICCID、IMSI 等），查阅产品设计文档，确认该识别码不可变更。

b) 预期结果:

儿童智能手表具有唯一设备识别码。

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

B.1.2.1.1 通用要求

身份鉴别的测评方法如下：

a) 测试方法：

1) 检查唯一标识生成算法，分析是否存在防止标识被篡改的防护措施；

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) 查阅产品说明文档，检查核对设备所有 WEB 管理界面、管理应用程序等网络登录方式，是否都需要身份鉴别；

4) 审查儿童智能手表身份鉴别错误锁定机制是否符合 GB 46859—2025 中 4.6.4 的要求；

5) 审查儿童智能手表登录错误限制和密码找回机制是否符合 GB 46859—2025 中 4.6.5 的要求；

6) 审查儿童智能手表密码组合校验机制是否符合 GB 46859—2025 中 4.6.6 的要求；

7) 检查开机和锁屏时的密码保护功能是否符合 GB 46859—2025 中 4.6.3 的要求。

b) 预期结果：

1) 产品对用户身份进行唯一标识，并采取防护措施防止标识被篡改；

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) 所有通过网络登录设备的方式，对访问主体进行身份鉴别；

4) 儿童智能手表身份鉴别错误锁定符合 GB 46859—2025 中 4.6.4 的要求；

5) 儿童智能手表登录错误限制和密码找回符合 GB 46859—2025 中 4.6.5 的要求；

6) 儿童智能手表密码组合校验符合 GB 46859—2025 中 4.6.6 的要求；

7) 开机和锁屏时的密码保护功能符合 GB 46859—2025 中 4.6.3 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”，其他情况判定为“不符合”。

B.1.2.1.2 生物特征识别

生物特征识别的测评方法如下：

a) 测试方法：

1) 审查儿童智能手表生物特征识别功能是否具备防假体呈现攻击检测能力，防假体攻击的种类是否符合 GB 46859—2025 中附录 C 的要求；对具有声纹识别功能的产品，按附录 C.3 选择不少于 2 种假体类型进行攻击测试；

2) 检查生物特征识别功能是否作为注册和登录、解锁、支付、注销和删除、家长管理控制等功能的唯一验证方式。

b) 预期结果：

1) 生物特征识别功能具备防假体呈现攻击检测能力，防假体攻击的种类符合 GB 46859—2025 中附录 C 的要求；

2) 生物特征识别功能未作为注册和登录、解锁、支付、注销和删除、家长管理控制等功能的唯一验证方式。

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.1.2.1.3 儿童智能手表管理端身份鉴别

儿童智能手表管理端身份鉴别的测评方法如下：

a) 测试方法：

1) 检查管理端口令在输入、修改及本地存储等环节的呈现方式，验证口令在使用过程中是否明文显示和存储；

2) 检查口令长度是否不少于 8 个字符、是否包含数字、小写字母、大写字母以及特殊字符中的两类字符，是否禁止使用弱口令。

b) 预期结果：

1) 管理端口令在使用过程中不明文显示和存储；

2) 管理端口令长度不少于 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两类字符，未使用弱口令。

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 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、安全启动和关键安全参数保护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、安全启动和

关键安全参数保护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.1.2.3 操作系统安全

操作系统安全的测评方法如下：

a) 测试方法：

1) 审查操作系统升级功能是否符合 GB 46859—2025 中 4.6.1 的要求；

2) 审查操作系统是否向所安装的第三方应用程序提供不可变唯一设备标识码；

3) 审查操作系统权限管控功能是否符合 GB 46859—2025 中 4.7.6 的要求；

4) 检查产品出厂时是否默认关闭所有敏感权限。

b) 预期结果：

1) 操作系统升级功能符合 GB 46859—2025 中 4.6.1 的要求；

2) 操作系统不向所安装的第三方应用程序提供不可变唯一设备标识码；

3) 操作系统权限管控功能符合 GB 46859—2025 中 4.7.6

的要求；

4) 产品出厂时默认关闭所有敏感权限。

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.1.2.4 应用程序安全

应用程序安全的测评方法如下：

a) 测试方法：

1) 检查具有预置应用的产品，在预置应用更新时是否对更新包进行真实性和完整性校验；

2) 检查提供第三方应用安装功能的产品，是否禁止应用自动安装和更新，第三方应用安装和更新时，应检验安装包的完整性和真实性；

3) 审查预置应用卸载功能是否符合 GB 46859—2025 中 4.7.3 的要求；

4) 审查恶意应用程序防范机制是否符合 GB 46859—2025 中 4.6.2 的要求；

5) 审查预置应用中包含网络音视频服务、网络直播服务、网络游戏服务、网络社交服务等，是否默认为移动互联网未成年人模式，且未提供可退出移动互联网未成年人模式选项；

6) 审查提供开启或关闭移动互联网未成年人模式选项的预置应用，在应用首次开启前，是否通过管理端获得监护人开启或关闭未成年人模式的授权，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

7) 审查预置应用中包含应用程序分发平台的，是否为儿童提供适宜儿童身心健康和年龄特点的应用程序，并在显著位置清晰标注应用程序的推荐年龄，同时明确标注该应用程序是否支持未成年人模式；是否明示未成年人模式与成年人模式在敏感个人信息处理方面、功能方面、未成年人权限管控等方面的区别；

8) 审查儿童智能手表安装的应用无未成年人模式的，是否通过管理端向监护人推送该应用不具备未成年人模式的提醒；

9) 审查预置应用提供网络社交服务、直播服务、浏览器服务、搜索引擎服务、电商服务、游戏服务、教育服务的，是否满足 GB/T 47694—2026 中 6.3 的要求。

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，禁止应用自动安装和更

新，在第三方应用安装和更新时对安装包进行完整性和真实性校验；

3) 预置应用卸载功能符合 GB 46859—2025 中 4.7.3 的要求；

4) 恶意应用程序防范符合 GB 46859—2025 中 4.6.2 的要求；

5) 预置应用中包含网络音视频服务、网络直播服务、网络游戏服务、网络社交服务等，默认为移动互联网未成年人模式，且未提供可退出移动互联网未成年人模式选项；

6) 预置应用中包含应用程序分发平台的，提供开启或关闭移动互联网未成年人模式选项的预置应用，在应用首次开启前，通过管理端获得监护人开启或关闭未成年人模式的授权，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

7) 预置应用中包含应用程序分发平台的，为儿童提供适宜儿童身心健康和年龄特点的应用程序，并在显著位置清晰标注应用程序的推荐年龄，同时明确标注该应用程序是否支持未成年人模式；明示了未成年人模式与成年人模式在敏感个人信息处理方面、功能方面、

未成年人权限管控等方面的区别；

8) 儿童智能手表安装的应用无未成年人模式的，通过管理端向监护人推送该应用不具备未成年人模式的提醒；

9) 预置应用提供网络社交服务、直播服务、浏览器服务、搜索引擎服务、电商服务、游戏服务、教育服务的，满足 GB/T 47694—2026 中 6.3 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”，其他情况判定为“不符合”。

B.1.2.5 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：

1) 检查是否采用了密码技术保障身份鉴别信息的机密性和完整性；

2) 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：

1) 产品使用了密码技术保护身份鉴别信息的机密性和完整性；

2) 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.1.2.6 访问控制

访问控制的测评方法如下:

a) 测试方法:

1) 在儿童智能手表首次绑定儿童智能手表管理端时，核验管理端与儿童智能手表是否进行交互确认，交互方式包括但不限于按键、蓝牙、无线网络配对、二维码、数字校验码等;

2) 核验多个管理端绑定同一儿童智能手表时，是否设置主管理端，并验证设备是否仅接受主管理端的控制指令;

3) 核验已完成设备绑定的产品，尝试通过清理后台、重启等方式解除绑定，检查解绑是否通过管理端授权等方式确认完成。

b) 预期结果:

1) 儿童智能手表首次绑定儿童智能手表管理端时，管理端与儿童智能手表进行交互确认，非设备所属用户无法完成绑定;

2) 多个管理端绑定同一儿童智能手表时设置主管理端，设备仅接受主管理端的控制指令;

3) 解绑通过管理端授权等方式确认完成，儿童智能手表无法通过清理后台或重启等方式解除绑定。

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.1.3 数据安全与个人信息保护

B.1.3.1 数据安全

数据安全的测评方法如下：

a) 测试方法：

1) 审查儿童智能手表数据销毁功能是否符合 GB 46864—2025 要求的信息清除功能；

2) 审查儿童智能手表设备解绑和账号注销功能是否符合 GB 46859—2025 中 4.7.9 的要求。

b) 预期结果：

1) 儿童智能手表的数据销毁符合 GB 46864—2025 要求的信息清除功能；

2) 儿童智能手表设备解绑和账号注销功能符合 GB 46859—2025 中 4.7.9 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”，其他情况判定为“不符合”。

B.1.3.2 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) 检查儿童智能手表为儿童提供信息发布、即时通讯等服务的，儿童智能手表生产者是否依法要求儿童或者其监护人提供未成年人真实身份信息，儿童或者监护人不提供未成年人真实身份信息的，儿童智能手表是否为未成年人提供相关服务;

2) 审查个人信息收集是否符合 GB/T 35273—2020 中 5.1、5.2、5.3 的要求，且是否强制要求儿童或者其监护人同意非必要的个人信息处理行为，因为儿童或者其监护人不同意处理儿童非必要个人信息或者撤回同意，是否拒绝儿童使用其基本功能服务;

3) 检查收集个人生物识别信息前，是否单独向监护人告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得监护人的明示同意；个人生物识别信息应与个人身份信息是否分开存储;

4) 审查儿童个人信息处理规则是否符合 GB/T 35273—2020 中 5.5 的要求，是否在儿童智能手表或手表管理端相关界面展示;

5) 审查个人敏感信息的传输和存储是否采用加密等安全

措施，存储期限是否符合 GB/T 35273—2020 中 6.1 的要求；

6) 检查儿童智能手表在手表端或手表管理端是否提供便捷的查阅儿童个人信息种类、数量等的方法和途径，是否对儿童或者其监护人的合理请求进行限制；是否提供便捷的儿童或其监护人复制、更正、补充、删除儿童个人信息的功能，并设置不合理条件；是否在 15 个工作日或者法律法规规定的期限内受理并处理个人行使权利的请求，如存在拒绝儿童或其监护人行使权利的请求的，是否书面告知申请人并说明理由；对于儿童个人信息转移、删除等可能对儿童权益产生较大影响的权利行使情形，儿童智能手表是否在管理端向监护人明示告知，并支持监护人选择是否行使相关权利；

7) 审查儿童个人信息对外提供是否符合 GB 46859—2025 中 4.7.7 的要求；

8) 审查涉及使用自动化决策方式处理儿童个人信息的功能是否符合 GB 46859—2025 中 4.7.4 的要求；

9) 检查未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息时，是否及时提示并采取停止传输等必要保护措施；未成年人私密信息发现未成

年人可能遭受侵害的，是否立即采取必要措施保存有关记录，并向公安机关报告。

b) 预期结果：

1) 儿童智能手表为儿童提供信息发布、即时通讯等服务的，儿童智能手表生产者依法要求儿童或者其监护人提供未成年人真实身份信息，儿童或者监护人不提供未成年人真实身份信息的，儿童智能手表未对未成年人提供相关服务；

2) 个人信息收集符合 GB/T 35273—2020 中 5.1、5.2、5.3 的要求，未强制要求儿童或者其监护人同意非必要的个人信息处理行为，未因为儿童或者其监护人不同意处理儿童非必要个人信息或者撤回同意，拒绝儿童使用其基本功能服务；

3) 收集个人生物识别信息前单独向监护人告知目的、方式和范围以及存储时间等规则，并征得监护人的明示同意；

4) 儿童个人信息处理规则符合 GB/T 35273—2020 中 5.5 的要求，并在儿童智能手表或手表管理端相关界面展示；

5) 个人敏感信息传输和存储采用加密等安全措施，存储期限符合 GB/T 35273—2020 中 6.1 的要求；

6) 儿童智能手表在手表端或手表管理端提供便捷的查阅儿童个人信息种类、数量等的方法和途径，未对儿童或者其监护人的合理请求进行限制；提供便捷的儿童或其监护人复制、更正、补充、删除儿童个人信息的功能，未设置不合理条件；在 15 个工作日或者法律法规规定的期限内受理并处理个人行使权利的请求，如存在拒绝儿童或其监护人行使权利的请求的，书面告知申请人并说明理由；对于儿童个人信息转移、删除等可能对儿童权益产生较大影响的权利行使情形，儿童智能手表在管理端向监护人明示告知，并支持监护人选择是否行使相关权利；

7) 儿童个人信息对外提供符合 GB 46859—2025 中 4.7.7 的要求；

8) 涉及使用自动化决策方式处理儿童个人信息的，符合 GB 46859—2025 中 4.7.4 的要求；

9) 发现未成年人私密信息或涉及私密信息的个人信息时，及时提示并采取停止传输等必要保护措施；未成年人私密信息发现未成年人可能遭受侵害的，立即采取必要措施保存有关记录，并向公安机关报告。

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.1.4 安全保障

B.1.4.1 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) 检查产品生产者是否明确并公示设备的型号，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;

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) 检查设备存在安全缺陷、漏洞时，是否按照《网络产品安全漏洞管理规定》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) 设备不存在 CNVD、CNNVD、NVDB 等国家漏洞库已公布的高危及以上级别漏洞;

2) 产品明确并公示设备的型号，在规定或当事人约定期

限内持续进行安全更新；

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) 发现设备存在安全缺陷、漏洞时，应按照《网络产品安全漏洞管理规定》报送相关漏洞信息，并及时告知用户安全风险。

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 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) 审查儿童智能手表内容安全要求是否符合 GB 46859—2025 中 4.8.1 的要求；

2) 检查是否建立了网络欺凌行为的预警预防、识别监测和处置机制，并满足：

(1) 建立网络欺凌信息特征库，通过技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测；

(2) 提供儿童及其监护人保存遭受网络欺凌记录、行

使通知权利的功能、渠道；

(3) 提供儿童设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。

3) 检查是否建立对儿童发布信息内容进行持续内容安全监测的机制；核查监测范围是否覆盖评论、留言、社区发帖、昵称头像等儿童发布的信息内容，是否持续开展监测；模拟发布违法不良信息或不适宜供儿童查看的内容，检查手表端是否立即停止传输该信息，是否采取删除、屏蔽、断开链接等处置措施并保存有关记录；检查对制作、复制、发布、传播上述信息的用户是否采取警示、限制功能、暂停服务、关闭账号等处置措施。

b) 预期结果：

1) 儿童智能手表内容安全要求符合 GB 46859—2025 中 4.8.1 的要求；

2) 已建立网络欺凌行为的预警预防、识别监测和处置机制，并满足：

(1) 建立网络欺凌信息特征库，通过技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测；

(2) 提供儿童及其监护人保存遭受网络欺凌记录、行使通知权利的功能、渠道；

(3) 提供儿童设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。

3) 建立了对儿童发布信息内容的持续内容安全监测机制，监测范围覆盖儿童发布的信息内容并持续开展监测；监测出违法不良信息或不适宜供儿童查看的内容时，立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施，并保存有关记录；对制作、复制、发布、传播上述信息的用户采取警示、限制功能、暂停服务、关闭账号等处置措施。

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 网络沉迷防治

B.1.4.3.1 时长管控

时长管控的测评方法如下：

a) 测试方法：

审查儿童智能手表时长管控功能是否满足 GB 46859—2025 中 4.9.1 的要求。

b) 预期结果：

儿童智能手表符合 GB 46859—2025 中 4.9.1 要求的时长管控功能。

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.1.4.3.2 应用管控

应用管控的测评方法如下：

a) 测试方法：

审查儿童智能手表应用管控功能是否覆盖 GB 46859—2025 中 4.9.2 的要求。

b) 预期结果：

应用管控功能符合 GB 46859—2025 中 4.9.2 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”，其他情况判定为“不符合”。

B.1.4.3.3 付费管控

付费管控的测评方法如下：

a) 测试方法：

审查儿童智能手表付费管控功能是否符合 GB 46859—2025 中 4.10 的要求。

b) 预期结果：

付费管控功能符合 GB 46859—2025 中 4.10 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”，其他情况判定为“不符合”。

B.1.4.3.4 其他要求

其他要求的测评方法如下：

a) 测试方法：

1) 在手表端发起紧急呼叫，检查是否支持拨打 110、119、120 及紧急联系人，并验证呼叫信息是否上报至监护人侧终端；

2) 模拟骚扰电话、诈骗短信等信息，检查监护人管理端是否收到相应的预警提示；

3) 检查手表端及预置应用是否设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，是否提供泛娱乐化功能；

4) 检查是否利用算法推荐服务诱导未成年人沉迷网络；

5) 儿童智能手表挂失功能是否满足 GB 46859—2025 中 4.11 的要求；

6) 儿童智能手表交换电话号码功能是否满足 GB 46859—2025 中 4.18 的要求。

b) 预期结果：

1) 支持拨打 110、119、120 及紧急联系人，并将呼叫信息上报至监护人侧终端；

2) 收到骚扰电话、诈骗短信等信息时，监护人管理端收到相应的预警提示；

3) 未设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，未提供泛娱乐化功能；

4) 未利用算法推荐服务诱导未成年人沉迷网络；

5) 儿童智能手表手表挂失功能满足 GB 46859—2025 中 4.11 的要求；

6) 儿童智能手表交换电话号码功能满足 GB 46859—2025 中 4.18 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：

尝试通过管理界面、接口、平台等对设备标识进行篡改，检查设备是否采取防护措施保护唯一设备识别码不被篡改。

b) 预期结果：

设备标识具有防护措施，无法被篡改。

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：

检查儿童智能手表物理接口与调试接口的功能，核查非必要的物理接口和调试接口出厂时是否全部关闭。

b) 预期结果：

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：

检查设备是否实现安全启动机制，对设备固件和启动组件的真实性和完整性进行校验。

b) 预期结果：

设备实现安全启动机制，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

B.2.2.1.1 通用要求

应满足 B.1.2.1.1 的测评方法。

B.2.2.1.2 生物特征识别

应满足 B.1.2.1.2 的测评方法。

B.2.2.1.3 儿童智能手表管理端身份鉴别

在满足 B.1.2.1.3 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：

重复提交同一短信验证码登录管理端，检查验证码是否具有防重放机制。

b) 预期结果：

短信验证码具有防重放机制，重复使用已失效的验证码无法登录。

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 密码应用

应满足 B.1.2.2 的测评方法。

B.2.2.3 操作系统安全

在满足 B.1.2.3 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：

1) 检查是否具有对操作系统升级具备安全校验机制，进行完整性校验和真实性校验；

2) 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操作系统，验证是否成功；

3) 检查操作系统更新时是否可以通过手表管理端提示监护人进行安全更新，是否具备自动或人工更新、更新中止后重新更新的功能；

4) 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) 操作系统升级具备安全校验机制，会验证更新操作系统的真实性和完整性；

2) 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操作系统；

3) 操作系统更新时可以通过手表管理端提示监护人进行安全更新，具备自动或人工更新、更新中止后重新更新的功能；

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.2.2.4 应用程序安全

在满足 B.1.2.4 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：

1) 检查是否具备默认关闭儿童智能手表操作系统基本功能外的服务，仅保留业务功能所需的最小服务，操作系统基本功能详见 GB 46859—2025 中 4.7.3 的要求；

2) 卸载部分预置应用软件后执行操作系统升级，检查已卸载的预置应用软件是否在未经监护人授权的情况下

被恢复，升级后的预置应用软件是否仍满足本文件要求；

3) 使用监护人账号在管理端对应用市场的应用执行安装、禁用/卸载操作，验证监护人是否可对儿童智能手表进行应用管理；

4) 在手表端触发外链打开和下载操作，检查是否要求监护人验证，是否提供外链打开一键豁免功能；

5) 儿童智能手表支持通过非预置应用程序分发平台安装应用的，是否建立应用程序分发平台准入白名单，白名单内的应用程序分发平台是否满足 5.2.4 的要求；

6) 所有预置应用是否默认启用移动互联网未成年人模式，若提供可退出移动互联网未成年人模式选项的，是否需经管理端监护人授权后方可关闭，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

7) 儿童智能手表是否可以安装无未成年人模式的应用。

b) 预期结果：

1) 默认关闭儿童智能手表操作系统基本功能外的服务，仅保留业务功能所需的最小服务；

2) 操作系统升级后，已卸载的预置应用软件未在未经监护人授权的情况下被恢复，升级后的预置应用软件仍

满足本文件要求；

3) 监护人可在管理端对儿童智能手表进行应用管理，应用市场的内容在监护人授权的情况下安装、禁用/卸载；

4) 外链打开和下载操作需经监护人验证，可为监护人提供外链打开一键豁免功能；

5) 儿童智能手表支持通过非预置应用程序分发平台安装应用的，建立了应用程序分发平台准入白名单，白名单内的应用程序分发平台满足 5.2.4 的要求；

6) 所有预置应用默认启用移动互联网未成年人模式，若提供可退出移动互联网未成年人模式选项的，需经管理端监护人授权后方可关闭，并明示未成年人模式与成年人模式在敏感个人信息处理、功能、未成年人权限管控等方面的区别；

7) 儿童智能手表不可以安装无未成年人模式的应用。

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 关键安全参数保护

在满足 B.1.2.5 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：

1) 检查是否采用了密码技术对关键安全参数进行机密性保护;

2) 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) 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。

b) 预期结果:

1) 产品采用了密码技术对关键安全参数进行机密性保护;

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。

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.2.2.6 访问控制

应满足 B.1.2.6 的测评方法。

B.2.2.7 固件安全

固件安全的测评方法如下:

a) 测试方法:

1) 查阅设备设计文档，检查固件升级是否具备安全校验机制；分别使用满足和不满足真实性与完整性的固件

升级包进行升级，验证校验失败时设备是否拒绝升级；

2) 尝试通过非授权方式将设备固件回退至低版本，验证设备是否具备防回退校验机制；

3) 在管理端检查有新固件版本时是否提示监护人进行安全更新，是否支持自动或手动升级，更新中止后能否重新更新；

4) 将设备恢复出厂设置或首次使用，检查是否检查并提示进行安全更新。

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，校验不通过时拒绝升级；

2) 设备具备非授权固件版本防回退校验机制，无法通过非授权方式回退至低版本固件；

3) 有新固件版本时在手表管理端提示监护人进行安全更新，支持自动或手动升级，更新中止后能重新更新；

4) 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。

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 输入验证

输入验证的测评方法如下:

a) 测试方法:

检查是否存在对通过用户界面输入的数据的安全校验措施;在用户界面输入框中提交可触发 SQL 注入、操作系统命令注入、路径遍历等异常行为的非法数据，验证系统是否拦截非法输入。

b) 预期结果:

存在对通过用户界面输入的数据的安全校验措施，未出现 SQL 注入、操作系统命令注入、路径遍历等意外行为，非法输入被拦截。

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.2.2.9 安全配置

安全配置的测评方法如下:

a) 测试方法:

查看设备管理操作界面或控制应用程序界面，核查设备是否提供设备配置项列表，是否默认为安全的，所有网络服务、端口为默认最小化的；查看设备配置过程，核查设备是否向用户进行安全设置的指导。

b) 预期结果：

设备提供默认安全的配置，向用户提供安全设置的指导。

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 通信安全

通信安全的测评方法如下：

a) 测试方法：

1) 检查是否采用加密技术及安全协议保证通信过程中数据的机密性和完整性；

2) 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：

1) 设备采用密码技术保证通信过程中数据的机密性和完整性；

2) 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.2.3.2 网络端口

网络端口的测评方法如下:

a) 测试方法:

1) 检查设备在默认状态下开放的端口情况，核查设备网络端口开放是否遵循最小化原则，是否默认关闭非必须使用及未使用的网络端口;

2) 未登录认证时，查看网络端口暴露的信息是否简化;

3) 使用监护人账号验证是否可手动关闭非必要的网络服务。

b) 预期结果:

1) 设备网络服务和网络端口开放遵循最小化原则，默认关闭非必须使用的网络服务和网络端口;

2) 设备未认证状态下未暴露网络端口信息;

3) 监护人可关闭非必要的网络服务。

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.1.3.1 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：

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、告知方式及监护人同意流程；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，检查存储在儿童智能手表端的用户数据是否提供访问控制机制；尝试以未授权方式（如越权接口调用、非授权应用读写）访问用户数据，验证是否被拒绝。

b) 预期结果：

1) 设备告知监护人数据采集方式、范围、目的，并经监护人同意后上传，告知内容完整，告知方式显著；

2) 存储在儿童智能手表端的用户数据提供访问控制机制，未授权方式无法访问用户数据。

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.2.4.2 个人信息保护

在满足 B.1.3.2 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：

1) 验证管理端是否有便捷通道（如设置页、客服入口）供用户在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

2) 对具有生物识别功能的产品，检查生物特征模板的存储方式，确认是否仅存储个人生物识别的摘要信息。

b) 预期结果：

1) 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，用户可以在线行使其访问、更正、删除、撤回授权同意、注销账户等权利；

2) 仅存储个人生物识别信息的摘要信息，不存储原始个人生物识别信息。

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.1.4.1 的测评方法。

B.2.5.2 内容安全管理

应满足 B.1.4.2 的测评方法。

B.2.5.3 网络沉迷防治

B.2.5.3.1 时长管控

在满足 B.1.4.3.1 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:

尝试在手表端修改系统日期和时间，检查儿童智能手表是否禁止修改，验证使用时间和时长管理能否被绕过。

b) 预期结果:

儿童无法修改儿童智能手表的系统日期和时间，无法通过修改系统时间绕过使用时间和时长的管理。

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.2.5.3.2 应用管控

在满足 B.1.4.3.2 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:

使用监护人账号在管理端屏蔽儿童智能手表内已安装的应用程序，检查应急类和基本功能类应用是否不受屏蔽限制。

b) 预期结果:

支持管理端屏蔽儿童智能手表内安装的应用程序，应急类

和基本功能类应用除外。

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.2.5.3.3 付费管控

应满足 B.1.4.3.3 的测评方法。

B.2.5.3.4 其他要求

应满足 B.1.4.3.4 的测评方法。

B.2.5.4 产品全生命周期管理

产品全生命周期管理的测评方法如下：

a) 测试方法：

1) 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；

2) 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，包括但不限于：删除非必要的账号、测试账号；从发布的版本中删除所有调试代码；禁用不必要的物理接口、网络服务、网络端口、网络接口；启用儿童智能手表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；

3) 核查安全运维机制和流程文档，是否满足 GB/T 39276—2020 第 5.2.2.3 项要求；

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

5) 核查安全设计机制文档，确认是否参考 GB/T 39276—2020 第 5.1.2.1 项要求进行威胁建模，是否包含威胁识别、分析及缓解措施；

6) 查阅开发安全文档，确认是否描述设备设计和开发过程中实现数据存储和传输机密性、完整性的机制和流程；

7) 核查产品安全开发机制相关文件，确认是否满足 GB/T 39276—2020 第 5.1.2.1 项相关要求。

b) 预期结果：

1) 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；

2) 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，包括但不限于：删除非必要的账号、测试账号；从发布的版本中删除所有调试代码；禁用不必要的物理接口、网络服务、网

络端口、网络接口；启用儿童智能手表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；

3) 产品生产者建立安全运维机制和流程，应满足 GB/T 39276—2020 第 5.2.2.3 项相关要求；

4) 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；

5) 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；

6) 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；

7) 产品生产者建立了产品安全开发机制，满足 GB/T 39276—2020 第 5.1.2.1 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) 核查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，核查开源代码来源是否可信；

2) 核查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是否及时进行修复或缓解。

b) 预期结果：

1) 使用的开源组件和开源软件来源可信；

2) 已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。

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

B.3.2.1.1 通用要求

在满足 B.2.2.1.1 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:

登录系统尝试进行修改网络安全配置、访问儿童个人信息等操作，验证是否使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，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、访问儿童个人信息等重要操作使用与设备登录不同的因子进行认证，或对操作环境进行安全校验，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.3.2.1.2 生物特征识别

应满足 B.2.2.1.2 的测评方法。

B.3.2.1.3 儿童智能手表管理端身份鉴别

应满足 B.2.2.1.3 的测评方法。

B.3.2.2 密码应用

应满足 B.2.2.2 的测评方法。

B.3.2.3 操作系统安全

在满足 B.2.2.3 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:

使儿童智能手表访问恶意网址信息，检查监护人管理端是否即时收到相应的预警提示。

b) 预期结果:

儿童智能手表访问恶意网址信息时，监护人管理端收到相应的预警提示。

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 应用程序安全

在满足 B.2.2.4 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：

1) 检查应用程序发生安全事件时，生产者是否在管理端向监护人推送安全告警；

2) 检查是否支持监护人在管理端对预置应用程序进行敏感权限管控；

3) 检查基本功能软件内附带扩展功能软件（模块）时，是否提供卸载或禁用扩展功能软件（模块）的方式；

4) 检查是否所有预置应用默认启用移动互联网未成年人模式，是否提供移动互联网未成年人模式的退出选项；

5) 审查是否建立应用未成年人模式符合性监测机制，在应用更新、版本迭代或收到相关风险信息时，是否重新评估其符合性；若监测发现不符合未成年人模式要求，是否通过管理端向监护人推送预警提示。

b) 预期结果：

1) 应用程序发生安全事件时，生产者通过管理端向监护人推送安全告警；

2) 监护人可在管理端对预置应用程序进行敏感权限管控；

3) 基本功能软件内附带扩展功能软件（模块）时，提供卸载或禁用扩展功能软件（模块）的方式；

4) 所有预置应用默认启用移动互联网未成年人模式，未提供移动互联网未成年人模式的退出选项；

5) 建立了应用未成年人模式符合性监测机制，在应用更新、版本迭代或收到相关风险信息时，重新评估其符合性；若监测发现不符合未成年人模式要求，通过管理端向监护人推送预警提示。

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 关键安全参数保护

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 固件安全

应满足 B.2.2.7 的测评方法。

B.3.2.8 输入验证

应满足 B.2.2.8 的测评方法。

B.3.2.9 安全配置

应满足 B.2.2.9 的测评方法。

B.3.3 网络与通信安全

B.3.3.1 通信安全

应满足 B.2.3.1 的测评方法。

B.3.3.2 网络端口

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 个人信息保护

在满足 B.2.4.2 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:

检查具有生物识别功能的，生物特征值是否仅在儿童智能手表端侧存储和处理。

b) 预期结果:

具有生物识别功能的，生物特征值仅在儿童智能手表端侧存储和处理。

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

应满足 B.2.5.2 的测评方法。

B.3.5.3 网络沉迷防治

B.3.5.3.1 时长管控

在满足 B.2.5.3.1 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:

卸载指定的移动互联网应用程序后，重新安装并查看使用时长统计，检查儿童智能手表是否对该应用程序的使用时长进行归零统计。

b) 预期结果:

移动互联网应用程序卸载后，儿童智能手表不对应用程序的使用时长进行归零统计。

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.3.5.3.2 应用管控

应满足 B.2.5.3.2 的测评方法。

B.3.5.3.3 付费管控

应满足 B.2.5.3.3 的测评方法。

B.3.5.3.4 其他要求

应满足 B.2.5.3.4 的测评方法。

B.3.5.4 产品全生命周期管理

应满足 B.2.5.4 的测评方法。

B.3.5.5 代码安全

在满足 B.2.5.5 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:

1) 查阅第三方检测机构出具的代码检测报告，核查检测是否由第三方检测机构实施，检测对象是否覆盖设备自身软件、第三方库和第三方组件，结论是否为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;

2) 使用应用程序对设备进行管理的，查阅第三方检测机构出具的设备管理应用程序检测报告，核查结论是否为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) 预期结果:

1) 委托第三方检测机构针对设备自身代码开展检测，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；

2) 使用应用程序对设备进行管理的，设备管理应用程序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。

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

儿童智能手表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) 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) 终端设备测试应包含硬件接口、外置存储、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 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

[3] GB/T 41411—2022 儿童手表

[4] GB/T 44445—2024 智能移动终端未成年人保护通用规范

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