ICS 35.020
CCS M 21

T/CSAC

团　　体　　标　　准

T/CSAC 025—2025

家庭物联网信息系统安全运维规范

Specification for security operation and maintenance of home internet of things(iot)information system

2025－12－15 发布　　2026－03－15 实施

中国网络空间安全协会　　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。

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。

本文件由中国网络空间安全协会提出并归口。

本文件起草单位：中移（杭州）信息技术有限公司、杭州电子科技大学、浙江工商大学、北京航空航天大学、北京航空航天大学杭州创新研究院、上海交通大学、国家税务总局湖北省税务局、河南省永城市人民法院、北京信息科技大学、济南大学、北京信息职业技术学院、北京奥音贝科技有限公司、数峦云（杭州）科技有限公司、上海钉加科技有限公司、江苏基久网络科技有限公司、杭州今日头条科技有限公司、亚信科技(成都)有限公司南京雨花分公司。

本文件主要起草人：聂智戈、杨万禄、陈维、邓鑫杰、石娜、李婉、王颖、陈健、庹鑫、李天琦、田镜达、卢骏、徐良、金文斌、汪铎、梁博、蔡倩楠、秦宏、关振宇、杜皓华、黄宝起、蔡文郁、蒋献、袁常顺、赵伟、郭妩君、孙志强、张厚田、杨定壹、蒋家冀、史墨祎、牟霆、贾军伟、杨媛娟、华茂、黄振明、王卫、余思一、马金金、史轲、顾怡哲、吴燕静、汪柳青、黄汇格、程顺宽、张总天、崔寻、傅俊辉、颜星晨、陈美琳、郑天祥、程进、张宁宁、林海峰、陈丹、李浩。

引　言

随着物联网技术在家庭环境中的广泛应用，家庭物联网信息系统（如智能家居系统、智能安防系统、智能家电等）已成为日常生活的重要组成部分。然而，家庭物联网设备普遍存在安全防护能力薄弱、用户安全意识不足、运维管理缺失等问题，导致数据泄露、设备被控、隐私侵犯等安全风险日益突出。为保障家庭用户的信息安全、人身安全和财产安全，规范家庭物联网信息系统的安全运维活动，特制定本文件。

本文件旨在为家庭物联网信息系统的所有者、使用者、运维主体以及设备制造商提供安全运维的基本要求和管理规范，提升家庭物联网环境的安全防护水平。

家庭物联网信息系统安全运维规范

1 范围

本文件提出了家庭物联网信息系统安全运维的基本要求和具体措施、应急预案与演练等内容。

本文件主要适用于接受委托为家庭物联网信息系统提供安全运维服务的实体（包括组织和个人），用于规范其在家庭物联网信息系统“入网-使用-退役”全生命周期的安全运维活动。

注：由家庭用户自行运维的网络，其安全实践可参照本文件提出的技术规范、配置要求及安全理念执行，以提高自身安全防护水平。

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

YD/T 3753 基于策略和计费控制（PCC）架构的移动网络能力开放总体技术要求

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

家庭物联网信息系统 home IoT information system

部署在家庭环境中，由物联网设备（感知层）、家庭网络（网络层）、智能家居平台/应用（应用层）及相关数据处理设施组成的，用于实现家庭设备互联、环境智能感知、自动化控制和信息服务的综合性信息系统。

3.2

家庭物联网设备 home IoT device

构成家庭物联网信息系统的基本单元，具备感知、识别、计算、执行和网络通信能力，部署在家庭环境中的物理设备。如智能网关、智能音箱、智能摄像头、智能门锁、智能家电等。

3.3

安全运维 security operation and maintenance

为确保家庭物联网信息系统的机密性、完整性和可用性，对系统进行的日常监控、维护、管理及响应安全事件的活动总和。

3.4

运维主体 operation and maintenance entity

负责执行家庭物联网信息系统安全运维活动的责任方，包括但不限于委托的专业运维服务人员或服务商。

3.5

安全基线 security baseline

为保证家庭物联网信息系统基本安全状态而需满足的最低安全配置要求集合。

4 缩略语

下列符号和缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

IoT：物联网（Internet of Things）

MAC：媒体访问控制地址（Media Access Control Address）

MFA：多因素认证（Multi-Factor Authentication）
SSID：服务集标识符（Service Set Identifier，无线网络名称）
WPA2/WPA3：Wi-Fi保护访问协议第2版/第3版（Wi-Fi Protected Access 2/3）

5 基本要求

5.1 责任落实

5.1.1 应明确家庭物联网信息系统的安全运维责任主体；若为委托运维，需与运维服务机构签订书面协议，明确安全责任边界。若由用户（家庭）自行维护，用户应负责执行设备或供应商提供的易于操作的基本安全维护措施（如及时确认并安装更新、设置管理密码等），并承担相应安全风险。

5.2 安全意识

5.2.1 运维主体应通过推送、宣贯等方式，定期向家庭用户提供安全意识相关内容，内容包括常见风险、防范措施、AI 安全防护要点等，推送频率不低于每季度 1 次。
5.2.2 运维主体应定期监控设备安全状态，及时向家庭用户同步安全提醒，如“警惕仿冒智能家居 App”、“及时更新路由器固件”、“AI 功能安全使用提示”等。

5.3 最小化原则

5.3.1 设备配置应遵循“最小功能启用”原则，禁用未使用的服务、关闭不必要的端口。
5.3.2 权限分配应遵循“最小必要”原则，如访客仅授予网络访问权限，不允许控制智能门锁、摄像头等敏感设备。

5.4 纵深防御

应构建多层级安全防护体系，包括设备层、网络层、数据层、应用层等。针对高风险设备，应额外采取增强防护措施，如摄像头视频流加密、门锁本地口令与远程控制分离。

5.5 持续运维

入网前应检查设备安全功能；定期监控设备状态、更新配置；设备更换或废弃时应清除设备数据、恢复出厂设置。

5.6 合规性

5.6.1 接受委托的运维服务机构不得非法采集、传输、存储家庭用户个人信息。
5.6.2 设备选型与使用应符合 YD/T 3753 的安全要求，优先选择通过国家网络安全等级保护测评的产品。

6 安全运维要求

6.1 运维组织与人员管理

6.1.1 人员能力要求

运维人员应熟悉所管理设备的基本功能与安全配置入口、能识别常见安全风险并执行基础应急操作，委托运维的服务人员还应提供身份证明与运维资质证明。

6.1.2 培训与考核

运维主体应建立定期培训机制，内容包括 AI 安全运维、新设备安全配置、近期家庭物联网安全事件案例等，并进行考核。

6.2 资产与配置管理

6.2.1 资产清单建立与维护

应建立家庭物联网资产清单，记录内容至少包括：

——设备基本信息：名称、类型、品牌型号、序列号/MAC 地址、部署位置；
——网络信息：IP 地址、接入方式、所属子网；
——管理信息：关联账号、登记日期；
——安全信息：固件版本、上次配置更新时间、是否启用 MFA。

注：资产清单应随设备及配置变更及时更新，新增设备需在入网后24小时内登记，移除设备需标注移除原因并更新清单状态。

6.2.2 口令管理

所有设备应设置口令，满足以下要求：
——长度≥12 位；
——包含大小写字母、数字、特殊符号；
——不与家庭成员手机号、生日等个人信息相关联。

注：口令应定期更换，若发现口令可能泄露，应24小时内更换；设备关联的App账号口令应与设备口令区分，避免“一套口令用到底”。

6.2.3 安全配置

应参照设备制造商提供的安全指南，完成禁用设备默认账号口令、关闭设备远程管理功能、启用设备本地日志记录、配置设备超时自动退出的基础安全配置，高风险设备中摄像头还应启用视频流加密、关闭默认访客查看权限，智能门锁宜禁用远程开锁功能。

6.2.4 配置备份与恢复

6.2.4.1 关键设备的配置由运维主体提供自动备份功能，备份内容包括网络参数与安全配置等核心设置，备份文件可存储在本地加密存储设备或具备安全资质的云存储。

6.2.4.2 运维主体宜每半年协助家庭用户测试 1 次配置恢复功能，模拟配置丢失场景，验证备份文件是否能正常恢复，恢复后需检查安全配置是否完整。

6.3 设备物理与环境安全管理

6.3.1 物理位置选择

设备应放置在远离水源、热源以防止短路或过热的物理风险规避位置，高风险设备需避免被遮挡且防止非法接触，网络设备则应置于家庭中心区域以确保信号覆盖均匀，同时避免靠近金属障碍物影响信号。

6.3.2 供电与环境控制

关键设备应使用稳压电源，避免电压波动导致设备故障；长期外出时，可关闭非必要设备电源，但需保持安防设备正常供电。智能设备应避免长期不间断通电，运维主体可提供定期断电检查提醒服务。设备运行环境应满足以下要求：
——温度：0℃～40℃；
——湿度：30%RH～70%RH；
——通风：设备周围预留不低于 10 cm 的通风空间，避免密闭环境导致过热。

6.3.3 设备维护与退役

6.3.3.1 设备应定期清洁，用干燥软布擦拭表面以避免灰尘堆积影响散热或功能，清洁时需断开电源，禁止用水或清洁剂直接喷洒。

6.3.3.2 设备退役前，应通过物理按键或管理 App 执行恢复出厂设置以清除所有用户数据，存储敏感数据的设备需拆除存储芯片并物理销毁以防数据恢复，转售设备前还应再次确认已执行出厂设置，可通过连接设备查看是否仍存在个人信息残留。

6.4 访问控制管理

6.4.1 网络访问控制

6.4.1.1 家庭 Wi-Fi 网络应采用 WPA3 或 WPA2 协议，禁止使用 WEP 协议。

6.4.1.2 SSID 不宜包含家庭个人信息，可设置为随机字符，若需增强隐私可启用路由器“隐藏 SSID”功能，避免 SSID 被非法扫描。

6.4.2 账号与权限管理

6.4.2.1 应支持分配差异化账号权限，管理员账号具备设备配置修改、权限分配、固件更新等全部权限，普通成员账号仅具备设备控制权限且无配置修改权限，儿童账号则限制高风险设备控制权限。

6.4.3 多因素认证启用

支持MFA的设备或App应启用MFA功能，优先选择硬件令牌、手机验证码或生物识别的认证方式。MFA认证信息应妥善保管。

6.5 网络安全管理

6.5.1 防火墙与端口控制

6.5.1.1 家庭网关/路由器应启用防火墙功能，日志保存期限不少于 30 天。
6.5.1.2 家庭网关/路由器宜关闭 Telnet、FTP、UPnP 等非必要服务端口。

6.5.2 异常流量监控

运维主体在取得用户显式授权后应定期检查路由器流量统计信息，重点关注单设备异常上传、未知IP连接及流量突增三类异常情况。发现异常流量后，应立即断开相关异常设备的网络连接，检查其配置。若无法定位原因，必要时可恢复该设备出厂设置并重新配置。

6.5.3 DNS 与网络协议安全

应配置安全的DNS服务，优先选择公共安全DNS或运营商官方DNS，禁止设备自动获取DNS地址。同时应限制IoT设备使用不安全的网络协议。

6.6 系统与软件安全管理

6.6.1 固件与软件更新监控

6.6.1.1 运维主体应建立固件与软件更新监控机制，需关注设备制造商官方网站、App 推送的安全公告并订阅漏洞通知，同时跟踪国家漏洞库（CNNVD）、中国网络空间安全协会发布的家庭物联网漏洞信息，及时获取设备相关漏洞预警。
6.6.1.2 固件与软件更新应遵循优先级要求。远程代码执行、口令绕过等高危漏洞更新宜在 24 小时内完成；功能优化、非核心漏洞修复等中低危漏洞更新可在 1 周内完成；不应更新来源不明的固件，避免植入恶意程序。

6.6.2 更新实施与验证

6.6.2.1 更新前需备份设备当前配置；应选择家庭网络使用低谷期进行更新，避免影响正常使用。
6.6.2.2 更新过程中应保持设备供电稳定，禁止断开电源。
6.6.2.3 更新后需检查设备功能是否正常、安全配置是否保留。
6.6.2.4 若更新后出现设备故障，应立即恢复备份配置；若无法恢复，应联系设备制造商售后支持，不应自行刷入非官方固件修复。

6.6.3 软件与应用管理

6.6.3.1 智能家居 App 应从官方渠道下载。
6.6.3.2 手机 App 仅可从设备制造商官方网站、正规应用商店获取，不应下载第三方平台的破解版、修改版 App；电脑管理软件仅可从设备官方网站下载，安装前应检查文件 MD5 值，确认文件未被篡改。
6.6.3.3 应定期清理冗余软件，卸载不再使用的智能家居 App，将保留的 App 更新至最新版本并关闭后台自启动功能，禁止 App 获取非必要权限。

6.6.4 恶意代码防范

6.6.4.1 个人设备应安装杀毒软件，定期扫描恶意代码，重点扫描从外部导入的设备配置文件、智能家居 App 安装包及设备本地存储的敏感数据。
6.6.4.2 应避免设备接入公共 Wi-Fi 等不安全网络，防止设备被植入恶意代码；若需在公共网络控制家庭设备，应通过 VPN（虚拟专用网络）连接家庭网络，禁止直接访问。

6.7 数据安全管理

6.7.1 数据收集与权限控制

6.7.1.1 应通过设备说明书、隐私政策及 App 权限申请确认设备数据收集范围，重点核查设备收集的个人信息类型及 App 申请权限与功能的匹配性；若发现设备收集非必要数据，应拒绝授权或选择不使用该设备。
6.7.1.2 数据上传应遵循“本地优先、按需上传”原则，支持本地存储的设备应设置数据本地存储，禁止默认上传至公共云；仅允许设备上传必要数据，不应上传敏感数据。

6.7.2 数据存储与加密

6.7.2.1 本地存储的敏感数据应采取加密保护措施，应使用加密 U 盘、加密硬盘作为存储介质，禁止使用未加密的公共云存储；加密方式宜采用 AES-256 加密算法。
6.7.2.2 云端存储的数据应选择具备国家网络安全等级保护三级及以上资质的云服务商，确认数据上传采用 HTTPS 协议以避免明文传输。

6.7.3 数据清理与销毁

6.7.3.1 应定期开展冗余数据清理工作，本地存储的过期数据清理后需通过数据粉碎工具彻底删除，防止数据恢复；应定期检查云端数据，删除过期数据并取消不再使用的云服务订阅；同时需定期清理 AI 模型训练产生的冗余数据、缓存数据，保障数据安全。
6.7.3.2 存储介质退役前，应使用专业工具进行全盘数据粉碎；高敏感存储介质应采取物理销毁方式处理，禁止随意丢弃或转售。

6.7.4 AI 数据安全管理

6.7.4.1 AI 智能体介入家庭物联网系统时，应明确 AI 数据处理的范围、目的，禁止 AI 非法采集、传输、存储家庭成员个人信息及敏感数据。
6.7.4.2 应建立 AI 数据安全审计机制，定期检查 AI 数据处理日志，确保数据处理合规。
6.7.4.3 家庭用户有权要求运维主体或设备制造商删除 AI 训练过程中收集的个人相关数据。

6.7.5 一键关闭功能

家庭物联网信息系统应支持快速解绑支付签约或“一键停止增值服务扣费”功能，参照银行一键冻结机制，当发生安全风险时，家庭用户可快速关闭所有家庭物联网账号及相关资金关联功能。

6.8 监测与审计

6.8.1 设备状态监测

6.8.1.1 应定期检查设备运行状态，包括但不限于通过智能家居 App 核查设备在线运行情况。高风险设备应增加监测频率，摄像头需检查录像功能是否正常、镜头是否被遮挡及是否存在异常移动，智能门锁需核查开锁记录是否异常及电池电量是否充足。

6.8.2 日志审计与分析

6.8.2.1 应定期查看关键设备日志，包括路由器的连接记录与流量记录、智能家居网关的设备接入/断开记录及指令执行记录、智能门锁的开锁记录。
6.8.2.2 日志分析发现异常时，应通过 MAC 地址确认陌生连接设备类型，对非法设备立即禁止接入；截图或导出异常日志并保存至加密存储介质；若发现异常指令执行，需检查设备是否存在固件漏洞并及时更新固件。

6.9 漏洞与风险管理

6.9.1 漏洞信息获取

6.9.1.1 运维主体应通过设备制造商官网安全公告、App 漏洞通知、售后服务邮件等官方渠道，国家漏洞库（CNNVD）、中国网络空间安全协会漏洞平台、国家网络安全应急中心（CNCERT）预警等权威机构渠道，以及正规网络安全媒体发布的相关信息，获取家庭物联网漏洞信息。

6.9.1.2 应建立漏洞信息登记制度，记录漏洞名称、影响设备、风险等级（高危/中危/低危）、发布时间及修复建议，登记后 24 小时内完成对家庭物联网系统影响的评估。

6.9.2 漏洞响应与修复

6.9.2.1 针对不同风险等级的漏洞，应采取差异化响应修复措施。高危漏洞应立即断开受影响设备的网络连接，24 小时内获取并安装设备制造商发布的修复固件/补丁，修复后需验证漏洞是否已修复；中危漏洞应在 1 周内完成修复，修复前应限制设备相关功能；低危漏洞可在下次常规固件更新时同步修复，无需紧急处理。

6.9.2.2 若设备制造商不再提供漏洞修复，应采取限制设备功能、更换设备等替代措施。

6.9.3 风险评估与改进

6.9.3.1 应定期开展家庭物联网安全风险评估，评估内容包括资产风险、网络风险、数据风险及运维风险。

6.9.3.2 风险评估后应生成评估报告，明确风险等级（高/中/低）与具体改进措施，改进措施应明确责任人与完成时限，完成后需验证改进效果。

6.10 变更管理

6.10.1 变更前评估

家庭物联网系统发生设备变更、网络变更或配置变更时，应提前开展安全评估。评估内容应包括变更是否引入新风险、是否影响其他设备的依赖关系，以及变更失败后的回滚方案。

6.10.2 变更实施与验证

6.10.2.1 变更应选取影响最小的时段实施，设备变更宜选择家庭成员较少、设备使用频率低的时段，网络变更宜选取家庭网络使用低谷期，避免对远程办公、在线学习等关键场景造成影响。

6.10.2.2 变更实施前应备份相关配置，实施过程中按评估方案执行，实施后需检查设备功能是否正常、安全配置是否完整，以及是否对其他设备产生连锁影响。

6.10.3 变更记录与恢复

6.10.3.1 变更完成后应完整记录相关信息，包括变更内容、实施时间、实施人、验证结果及恢复方案。

6.10.3.2 若变更后出现问题，应立即执行恢复方案。配置变更需恢复备份配置，设备变更需移除新增设备或恢复已移除设备；恢复后应验证系统是否恢复正常，分析变更失败原因，调整方案后重新评估实施。

6.11 备份与恢复管理

6.11.1 备份策略制定

6.11.1.1 应根据数据与配置的重要性制定差异化备份策略。关键配置应进行全量备份，且变更前需补充增量备份；重要数据应进行全量备份，敏感数据需定期开展增量备份；普通数据仅需进行全量备份，无需增量备份。

6.11.1.2 备份介质选择应满足安全要求。本地介质优先选用加密 U 盘、加密硬盘，禁止使用未加密的移动存储；云端介质应选择具备安全资质的云服务商，并启用云端数据加密；关键配置应同时备份至两种不同介质，避免因单一介质损坏导致备份丢失。

6.11.2 备份实施与检查

6.11.2.1 准备阶段需确认备份介质可用、备份内容完整；执行阶段按备份策略完成备份操作；校验阶段需检查备份文件的完整性和加密性。

6.11.2.2 应定期检查备份有效性，随机抽取 1 个备份文件验证是否能正常恢复，同时检查备份介质状态，对损坏介质及时更换并重新备份。

6.11.3 恢复流程与验证

6.11.3.1 系统故障时，首先评估故障类型与影响范围，再根据故障类型选择对应备份；配置恢复通过设备后台“导入配置”功能实现，数据恢复将备份数据复制至原存储位置；恢复后需检查设备功能是否正常、恢复的数据是否完整、安全配置是否有效。

6.11.3.2 若恢复失败，应采取替代措施：配置恢复可手动重新配置；数据恢复方面，敏感数据应联系专业数据恢复机构处理，普通数据可重新采集或下载。

6.12 事件管理

6.12.1 事件类型与识别

6.12.1.1 家庭物联网常见安全事件类型包括设备安全事件、网络安全事件、数据安全事件及账号安全事件。

6.12.1.2 安全事件应通过以下方式识别：

——设备 App 告警、监测工具告警等实时告警手段；

——查看设备日志发现异常的日志分析方式；

——设备功能异常、网络速度突降等功能异常表现。

6.12.2 事件响应流程

6.12.2.1 发现安全事件后，宜按以下流程响应：

a) 紧急处置（0～1 小时）：
   1) 隔离：断开受影响设备网络；
   2) 止损：修改管理员密码、禁用被泄露的权限；
   3) 保护证据：截图或导出事件相关日志，保存至加密存储。
b) 分析与处置（1～24 小时）：
   1) 定位原因：通过日志、设备状态分析事件原因；
   2) 彻底处置：如固件未更新导致的设备被劫持，更新固件并恢复出厂设置；密码弱导致的账号被盗，修改所有关联设备密码并启用 MFA。
c) 恢复与验证（24～48 小时）：
   1) 恢复：重新连接隔离设备、恢复正常网络配置；
   2) 验证：检查设备功能是否正常、安全配置是否完整、是否存在残留风险。

6.12.2.2 不同类型安全事件应采取差异化处置措施。账号被盗时，应立即冻结账号、修改口令、解绑所有陌生设备，并通知家庭成员警惕诈骗；数据泄露时，需停止数据上传、删除泄露数据，联系设备厂商协助追溯泄露源头；设备被劫持时，应恢复设备出厂设置、更新固件并重新配置安全参数。

6.12.3 事件记录与改进

6.12.3.1 事件处置完成后，应完整记录相关信息，包括事件基本信息、处置过程及原因与改进。

6.12.3.2 应定期回顾事件记录，分析高频事件类型并优化运维策略。针对弱口令等问题，强化强口令设置相关指引；针对设备被劫持等事件，增加固件更新频率；针对网络安全事件，提高陌生设备检查频率。

7 应急预案与演练

7.1 应急预案制定

7.1.1 预案内容要求

7.1.1.1 应制定《家庭物联网信息系统安全应急预案》，确保预案内容全面覆盖应急处置关键环节。

7.1.1.2 演练通讯录宜涵盖设备制造商售后电话、第三方运维机构电话、网络安全应急机构联系方式，保障应急处置过程中可及时获取专业支持。

7.1.1.3 针对常见安全事件，预案应制定步骤化处置流程，明确不同事件的响应环节、操作要点及责任主体，确保应急处置规范有序。同时，需明确应急工具与备用设备的存放位置，确保应急资源可快速调取使用；还应制定事件处置后的系统恢复流程，明确恢复步骤、验证标准，保障系统及时恢复正常运行。

7.1.2 预案更新与保管

应急预案应定期更新，若家庭物联网系统发生变更、相关标准更新或发生安全事件，需及时修订预案内容。

7.2 应急演练

运维主体应定期组织应急演练，演练内容应涵盖预案讲解、实战操作及案例分析。演练结束后，须进行评估总结，并根据结果优化应急预案及处置流程。

参 考 文 献

[1] GB/T 25069 信息安全技术 术语
[2] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[3] GB/T 35273 信息安全技术 个人信息安全规范
[4] GB/T 38645 信息安全技术 网络安全事件应急演练指南
[5] GB/T 20984 信息安全技术 信息安全风险评估规范
[6] GB/T 20261 信息安全技术 信息系统安全工程管理要求
[7] ISO/IEC 27002:2022 信息安全管理指南
[8] NISTIR 8259A (IoT Device Cybersecurity Capability Core Baseline)
[9] EN 303 645 V2.1.1 消费物联网网络安全标准