

TC260-PG-202613A

网络安全标准实践指南

——电子产品回收过程中的信息清除管理指引

(v1.0-202609)

全国网络安全标准化技术委员会秘书处

2026 年 9 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：中国电子技术标准研究院、中国科学院信息工程研究所、赛西（深圳）电子信息产品标准化工程中心有限公司、上海万物新生信息科技有限公司、中国资源循环集团电子电器有限责任公司、中国电子装备技术开发协会、中国循环经济协会、中再生城资（北京）环保科技发展有限公司、北京赛西科技发展有限公司、杭州奇立软件技术有限公司、安运数盾科技(杭州)有限责任公司、四川长虹格润环保科技股份有限公司等。

本文件主要起草人：何延哲、王秉政、高晨涛、刘行、朱大立、刘昊鑫、岳帅、田一、王寒生、毕思文、黄加忠、田牧、廖欢乐、黄文、刘欣伟、唐爱军、潘永刚、薛頔、于飞、禹明生、张蕾、梁永喜、侯允、杨雨辰、朵磊、李辉、段雨洪等。



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”。





摘 要

随着电子产品更新迭代加速，二手交易与资源回收行业快速发展，用户数据泄露风险日益突出。GB 46864—2025《数据安全 电子产品信息清除技术要求》作为强制性国家标准，为信息清除技术划定了底线，但行业仍缺乏统一的日志记录、标识追溯与回收过程管理机制，导致信息清除过程不透明、结果难查询，用户权益难以保障。尤其是在二手交易与资源再利用过程中，如无法有效传递信息清除日志，则会出现反复清除导致电子产品可用性下降，也不符合低碳环保的可持续发展理念。为填补这一空白，衔接强标落地执行，规范电子产品回收过程中的信息清除相关行为，特制定本指南。

本指南通过统一电子产品信息清除日志格式和内容，规范电子产品回收信息清除的过程管理、组织管理，建立基于信息清除标识的信任机制，旨在实现信息清除全流程可追溯、可验证，提升回收工作效率的同时充分保障用户切身权益，推动电子产品回收与二手交易行业健康规范发展。



目 录

1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 概述	3
6 信息清除日志记录	4
6.1 通则	4
6.2 日志内容与字段规范	6
6.3 日志格式与编码	7
7 回收经营者管理指引	8
7.1 原则	8
7.2 回收过程管理	9
7.3 组织安全保障	15
7.4 代理回收点管理	18
7.5 上门回收管理	23
7.6 线上回收管理	23
附 录 A（资料性）信息清除标识样式和使用指引	25
附 录 B（资料性）信息清除日志码编码规则	31
附 录 C（资料性）用户数据清除告知同意书模板	33
附 录 D（资料性）用户追溯信息清除状态的方法与路径	36
参考文献	40





1 范围

本文件给出了电子产品信息清除日志记录的格式、内容和回收过程中的信息清除管理指引。

本文件适用于指导回收经营者在回收电子产品过程中形成信息清除日志、建立回收管理体系、规范代理回收点管理、使用信息清除标识和为用户提供信息清除日志查询服务；电子产品厂商设计信息清除功能或提供信息清除服务的也可参考使用部分内容。

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（包括所有修改单）适用于本文件。

GB/T 22080—2025 网络安全技术 信息安全管理体系要求

GB/T 35273 数据安全技术 个人信息安全规范

GB 46864—2025 数据安全技术 电子产品信息清除技术要求

3 术语和定义

3.1 信息清除日志

记录电子产品信息清除活动全流程关键信息的记录或结构化电子文件，可用于验证信息清除结果真实性和追溯信息清除过程。

3.2 唯一识别码

用于唯一标识单台电子产品的官方编码，包括国际移动设备识别



码（IMEI）、移动设备识别码（MEID）、产品序列号（SN）、设备唯一标识符（UUID）等。

3.3 信息清除日志码

与电子产品信息清除结果唯一绑定的电子凭证编码（通常为二维码），包含日志核心信息与防伪校验码，可作为信息清除完成的有效证明。

3.4 信息清除公共服务平台

由第三方建设运维，提供电子产品信息清除日志查询、信息清除工具下载、信息清除标识管理、以及其他社会化服务的网络平台。

3.5 回收

出于循环利用目的,将二手电子产品进行收购、运输、贮存、检测等活动。

注1：回收通常是二手电子产品流通的初始活动,通过回收二手电子产品再进行交易、翻新维修再销售、废弃资源再利用等。收购包括有偿或无偿。

注2：二手电子产品流通有多种情形,包括但不限于:通过线下回收门店、线上交易平台、二手交易市场、上门服务等方式进行回收、交易(含外贸);对二手电子产品进行翻新维修再销售;对废弃电子产品进行处理和资源再利用;对二手电子产品进行竞拍、拆零出售等新型业态等。

[来源：GB 46864—2025，3.9]

3.6 回收经营者

从事二手电子产品回收、销售活动的企业和个体工商户。

注：仅提供交易渠道的不属于回收经营者。

[来源：GB 46864—2025，3.10]



3.7 代理回收点

接受回收经营者管理，提供二手电子产品代理回收服务的经营场所。

3.8 资源再利用

对二手电子产品回收后进行零部件拆解重复利用或原材料回收重复利用。

4 缩略语

APP: Application (应用程序)

CDR: CorelDRAW (矢量图形文件格式)

DPI: Dots Per Inch (每英寸点数)

PET: Polyethylene Terephthalate (聚对苯二甲酸乙二醇酯)

PNG: Portable Network Graphics (便携式网络图形)

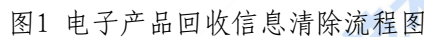
PVC: Polyvinyl Chloride (聚氯乙烯)

SVG: Scalable Vector Graphics (可缩放矢量图形)

5 概述

电子产品回收过程涉及用户、电子产品厂商、回收经营者等相关主体，以及回收前、回收中、回收后、资源再利用、再销售等环节。此外，信息清除公共服务平台可提供信息清除日志查询、信息清除标识管理等服务。

电子产品信息清除流程如下图：



本文件第 6 章给出了信息清除日志记录的内容、格式和编码，第 7 章给出了回收经营者回收电子产品过程和组织安全保障管理相关指引。附录 A 给出了信息清除标识样式和使用指引。附录 B 给出了信息清除日志码编码规则。附录 C 给出了用户数据清除告知同意书模板。附录 D 提出了用户追溯信息清除状态的方法与路径。

a) 信息清除日志需“真实、完整、不可篡改”，其中清除的操作



时间、清除结果等核心字段内容宜以自动生成为准。

注 1：日志通常由信息清除工具或功能等直接生成，因技术条件不具备需要手工录入的除外。

b) 每条信息清除日志需与对应电子产品的唯一识别码进行绑定。

注 2：电子产品包括多个存储用户数据的存储介质的，完成所有存储介质信息清除可形成电子产品信息清除日志，如仅对其中部分存储介质进行信息清除则无法形成完整电子产品信息清除日志；将已完成信息清除的存储介质通过拆解、拆卸方式从电子产品中取出后，可视为单独的电子产品，完成信息清除后可形成信息清除日志。

c) 原则上不得出现多台电子产品共用一条信息清除日志的情况，将多台电子产品整体进行销毁处置等集中处理的情形除外。

d) 电子产品对应多条信息清除日志的，以最近一条信息清除日志为准，用户查询的信息清除日志为最近一条信息清除日志。

e) 电子产品回收全链条过程中，需至少完成一次信息清除，有条件获取信息清除日志的，可予以采信，避免反复执行信息清除降低电子产品二手流通利用价值。

注 3：电子产品回收全链条过程包括第 7 章中的相关步骤，电子产品一旦脱离回收过程再次进入消费环节后，用户则有可能通过使用电子产品形成新的用户数据，已有的信息清除日志则不能被采信。

f) 信息清除日志宜覆盖信息清除活动的全流程关键节点，包括清除任务发起、清除过程执行、清除结果验证等环节，每个节点的时间戳宜精确到秒。

g) 回收经营者宜建立信息清除日志访问权限管理制度，在系统、平台上妥善保管日志，仅授权指定人员可查看和导出日志，并对日志进行备份，日志的保存期限不少于 3 年（自信息清除完成之日起计算）。



- h) 支持生成信息清除日志的电子产品，宜在电子产品本地或云端服务器存储原始日志文件，便于用户进行查询。

注：生成信息清除日志时，可选择通过生成信息清除日志码的方式向用户展示。

- i) 接入信息清除公共服务平台的回收经营者，宜在信息清除完成后 24 小时内，将日志同步至信息清除公共服务平台。

6.2 日志内容与字段规范

信息清除日志需包含表 1 规定的必选内容，可根据实际业务需求增加可选内容，新增内容不得影响必选字段的完整性和可读性。

表 1 信息清除日志内容与字段规范

类别	字段名称	字段说明	必选/可选
产品基础信息	唯一识别码	电子产品的设备唯一标识，可选 IMEI/MEID/SN/UUID 中一个或多个，具备多个识别码时用分号分隔。 注：对于部分老旧电子产品由于损坏、磨损等客观原因导致无法获得设备唯一识别码的，可以专门生成的唯一批次号或临时编码替代	必选
	产品类型	手机、平板电脑、电脑、服务器、智能手表、智能玩具、摄像头、相机、无人机等	必选
	产品品牌	电子产品的品牌名称	必选
	产品型号	电子产品的具体型号全称	可选
	存储容量	电子产品内置存储介质的标称容量，单位为 GB	可选
清除活动信息	清除任务编号	实施主体生成的唯一清除任务编号	可选
	清除状态	清除中/已清除/清除失败	必选
	清除主体	实施信息清除的回收经营者/代理回收点名称（适用回收过程信息清除）	必选
	操作人员	现场执行清除操作的工作人员姓名或系统账号，电子产品用户/本人	可选
	清除开始时间	清除操作启动的时间，格式为 YYYY-MM-DD HH:mm:ss	可选



类别	字段名称	字段说明	必选/可选
	清除完成时间	清除操作结束的时间，格式为 YYYY-MM-DD HH:mm:ss	必选
	清除实施节点	回收前/回收中/回收后/资源再利用	可选
	清除方法	数据覆写（注明覆写次数）/块擦除/物理销毁等	必选
	清除工具名称	实施信息清除所使用的专用工具名称	可选
	清除工具版本	清除工具的软件版本号	可选
	验证时间	验证操作结束的时间，格式为 YYYY-MM-DD HH:mm:ss	可选
	验证结果	清除效果验证的结果：合格/不合格	可选
	验证人员	负责清除效果验证的工作人员姓名或系统账号	可选
日志码关联信息	日志码唯一编号	生成的信息清除日志码唯一编号	可选
	日志码生成时间	信息清除日志码生成的时间，格式为 YYYY-MM-DD HH:mm:ss	可选
	日志码哈希值	信息清除日志码的哈希值，用于防伪校验	可选
平台同步信息	同步状态	未同步、已同步、同步失败	可选
	同步时间	日志同步至公共服务平台的时间，格式为 YYYY-MM-DD HH:mm:ss	可选

6.3 日志格式与编码

日志格式与编码方式包括：

- 信息清除日志宜采用电子结构化格式，优先使用 JSON 格式，也可使用 XML 格式，便于跨平台数据交换和解析。
- 日志文件宜采用 UTF-8 编码，避免出现乱码问题。
- 日志格式宜具备向后兼容性，当新增可选字段时，旧版本日志解析程序宜能正常读取核心必选字段内容。



- d) 单条日志的文件大小不宜超过 1MB，对于包含大量验证数据的日志，宜将验证数据作为附件单独存储，并在日志中记录附件的哈希值和存储路径。
- e) 信息清除日志可提供信息清除日志码的展示形式，方便用户查看和回收经营者提取、同步信息清除日志。

注：信息清除日志码编码规则见附录 B。

7 回收经营者管理指引

7.1 原则

电子产品回收经营者在符合GB 46864—2025中第7章的基本要求基础上，宜基于以下原则开展信息清除活动：

- a) **合法正当原则**：信息清除活动严格遵循数据安全相关法律法规要求，采取技术和管理等措施保障用户数据安全；
- b) **告知同意原则**：向用户明示告知电子产品信息清除的目的、方式、范围和清除后产生的影响等，并提示用户主动实施信息清除或用户同意后信息进行信息清除；
- c) **责任明确原则**：明确回收经营者在代理回收、回收再售、资源再利用等二手电子产品回收环节中的主体责任，并接受外部监督；
- d) **分类处置原则**：根据设备、系统类型和存储介质、数据敏感程度不同，按照GB 46864—2025要求可分类采取差异化信息清除技术和方案，做到信息清除精准处理、安全高效；



- e) **追溯验证原则：**信息清除操作留存设备信息、清除方法、操作时间、清除结果等关键信息，形成可追溯台账，确保过程可核查、结果可确认。

7.2 回收过程管理

7.2.1 回收前

回收前的安全管理措施主要包括：

- a) **信息登记：**为履行法定义务、落实监管政策或为履行合同所必须，如实记录用户身份、联系方式、产品状态信息、回收需求等，核验产品合法来源，拒收来源不明或涉盗抢产品，拒绝为无民事行为能力未成年人提供回收服务，信息登记涉及的个人信息保护，需符合相关法律法规和标准要求；
- b) **明示告知：**通过书面、电子告知同意书或其他有效形式主动提示用户进行信息清除，明确告知用户信息清除的范围、方法、不可逆性及未清除数据的泄露风险；

注1：用户数据清除告知同意书见附录C。

- c) **引导用户自行清除：**如电子产品可用且内置符合 GB 46864—2025 的信息清除功能，可指导用户在设备交付前自行备份用户数据并执行产品内置信息清除功能。

注2：未激活的电子产品未保存用户数据，无需进行信息清除。

7.2.2 回收中

回收中的安全管理措施主要包括：



- a) **操作流程：**回收中工作人员宜佩戴工作证，能出示相关授权证明，回收中如未取得用户授权，不得擅自开启、联网或操作用户数据，完成回收操作工作流程后，处于开机状态的电子产品，需在用户见证下关机封存。
- b) **回收中现场清除：**若因用户不便操作、放弃自清除、产品功能缺失等原因无法实现回收前信息清除的，需获得用户授权同意后由回收经营者（包括代理回收点、上门回收等）按照 GB 46864—2025 要求进行信息清除，信息清除过程涉及多个步骤（如有）的，均需用户自行操作或授权后由回收人员操作。
- 注 1：授权同意方式可采取用户签署书面、电子告知同意书等方式，告知同意相关内容可参考附录 C。
- 注 2：步骤包括：退出账号、关闭找回、解绑或删除智能卡等。
- c) **临时保管：**临时保管电子产品宜存于带锁、带监控的专用设备和场所，并建立电子产品台账，监控录像保存不少于半年。
- d) **物流管理：**选信誉良好、有封闭运输、货物溯源能力的物流方，并能在运输中实时追踪货物物流轨迹，货物交接过程需可查可溯。
- e) **运输与贮存安全：**运输和贮存过程中，宜采取物理安全措施（如使用带锁运输箱、密封包装等），防止丢失、被盗或未经授权访问。其中未完成清除数据的电子产品需清晰标记、隔离存放。
- f) **交接保护：**电子产品交接过程中电子产品不能被再次开机，通过工厂模式等无需访问用户数据的方式、用户数据已被清



除、取得用户单独授权后或根据合同约定条件进行操作的除外。

7.2.3 回收后

回收后的安全管理措施主要包括：

- a) **库存、档案管理：**电子产品入库时宜记录唯一识别码，与回收记录、清除日志（如已清除）关联。库存区域需具备物理安全措施（如门禁、监控），防止未经授权接触。宜建立电子产品库存台账，标记电子产品状态（待清除、已清除、已验证等）。
- b) **回收后集中清除：**如电子产品回收中未实现信息清除，需在回收后由授权人员在受控环境（如专用工位、视频监控下）按照 GB 46864—2025 要求进行信息清除并参照第 6 章生成信息清除日志，执行信息清除操作的工作人员需经过专业技能、安全保密培训。
- c) **采信已清除结果：**用户已自行清除且签署告知同意书、代理回收点或上门回收过程中已完成信息清除、参照第 6 章生成信息清除日志且日志已同步（同步方式包括通过业务系统同步日志或将日志同步至信息清除公共服务平台）的，回收后无需对电子产品进行再次信息清除。
- d) **信息清除效果验证：**宜对已完成信息清除的电子产品进行信息清除效果整体抽样验证，抽样率不低于 5%，同一品类不



超过 30 个，并记录验证的相关记录（包括抽样信息、验证方法、验证结果、操作人员、验证时间等），相关内容可一并纳入信息清除日志。

- e) **清除失败处理：**对于清除失败的电子产品，需隔离存放，交由有相关资质和能力的组织进行销毁处置（具体见 7.2.4），并通过信息清除日志记录处理过程和结果。
- f) **日志上传及用户追溯：**对于完成信息清除及效果验证的电子产品，宜向用户提供信息清除日志查询渠道或将信息清除日志同步至信息清除公共服务平台，供用户查看电子产品信息清除状态。

注 1：用户追溯信息清除状态的方法与路径见附录 D。

注 2：回收企业用户的批量电子产品时可根据合同约定向企业用户提供信息清除日志查询渠道。

7.2.4 资源再利用

对于无法通过常规方式开机（如主板损坏、电池失效、系统崩溃无法打开等）的电子产品，暂时缺乏有效清除技术手段的电子产品，或没有再售价值的电子产品（废旧电子产品），可通过物理拆解提取可用零部件或整体销毁的方式进行资源再利用，其过程宜采取以下安全管理措施：

- a) **环境与场所安全：**在具有资质和能力的单位和场所实施拆解销毁，确保拆解销毁全过程安全可靠。

注：资质主要指符合相关管理要求的环保处置资质。

- b) **技术判定：**由工作人员在受控环境（如防静电工作台）上对



无法开机电子产品进行技术判定，确认无法通过软件方式启动且无法使用信息清除工具清除的，进行拆解销毁。

- c) **直接销毁：**确认没有拆解再售价值的电子产品，需交由有资质单位进行物理销毁，物理销毁需确保存储介质被完全破碎，无法恢复数据。
- d) **物理拆解：**拆解过程中宜取出主板上的磁存储介质（如 HDD 等）或半导体存储芯片（包括但不限于 eMMC、UFS、NAND Flash、eMCP、NOR Flash 等），并对其进行清洁、编号，记录来源信息（如设备型号、回收批次等）。
- e) **磁存储介质信息清除：**拆解出的磁存储介质需选用符合 GB 46864—2025 第 6 章要求的信息清除工具进行信息清除，数据覆写次数不低于 3 次。
- f) **存储芯片信息清除：**拆解出的存储芯片需选用符合 GB 46864—2025 第 6 章要求的信息清除工具（如具备底层擦除能力的编程器/烧录器，可读取存储芯片的同类型设备等，设备确保电器连接可靠），向芯片发送底层擦除命令（如全片擦除、块擦除等），对芯片中存储的数据进行不可逆清除。
- g) **清除效果核验：**抽样对完成清除后存储芯片进行验证，抽样比例不低于 5%，确认其存储单元已恢复为空白状态（通常为 0xFF 或 0x00）。

注：清除效果验证方法参考如下：对于容量 $\leq 64\text{GB}$ 的芯片，进行全片读取校验；对于容量 $> 64\text{GB}$ 的芯片，可按照统计学原则进行抽样验证，抽样数量不少于 5 个物理块，抽样容量大小不小于 64GB，且覆盖芯片的不同区域。如清除验证方



法另有规定的，根据规定执行。

- h) **清除与验证记录：**对清除和验证过程进行记录，记录至少包含芯片型号、唯一标识信息（如激光刻字、芯片 ID）、清除时间、所用工具、验证结果、坏块信息记录等。
- i) **合格存储介质再利用：**通过空片验证且无物理损伤的合格存储介质（包括磁存储介质和存储芯片），宜标注“信息已清除”及必要的寿命等级，附验证报告后，方可进入二手存储介质流通市场（包括境内或境外市场），并留存销售记录。销售记录宜包含存储介质标识、购买方信息、验证报告编号等，销售记录至少保留半年。
- j) **不合格存储介质处置：**对无法建立电气连接、清除操作失败、验证不通过或在清除过程中损坏的存储介质，交由有资质单位进行物理销毁，物理销毁需确保存储介质被完全破碎，无法恢复数据。
- k) **其他零部件处置：**拆解过程产生的废电路板（不含存储介质的主板基板等）作为危险废物，分类暂存于符合环保要求的危废间，并委托有资质单位处置。

7.2.5 面向组织用户的回收过程管理

回收经营者回收企事业单位等组织用户的批量电子产品时，需通过签署合同协议等形式，明确向用户告知电子产品信息清除相关事项，合同协议签署生效后根据7.2.1-7.2.4中相关内容进行回收过程的信



息清除管理。合同另有约定的，以及组织用户所在行业、领域另有规定的按照约定或规定执行。

7.3 组织安全保障

7.3.1 基本条件

相关内容包括：

- a) **基础保障条件：**回收经营者需具备回收作业的基本条件，如满足相应国家标准的场所、资质、人员等保障条件；
- b) **资质及能力公示：**向用户公示二手电子产品回收等相关的营业资质、信息清除能力证明（如信息清除标识等）、操作规范及数据安全保障措施，接受用户监督；

7.3.2 组织制度

相关内容包括：

- a) 回收经营者宜设立数据安全与个人信息保护的负责人或管理部门，建立部门管理和人员安全管理相关制度，明确各部门、各岗位、各人员的职责和操作规程；
- b) 建立二手电子产品信息清除全流程管理制度，涵盖回收告知确认、物流运输、库存管理、信息清除操作、日志管理、再销售核验等环节，明确各环节操作规范、责任主体及考核要求；
- c) 制定网络和数据安全突发事件应急预案，针对数据泄露、清



除失误、产品丢失被盗、存储介质处置不当等情形，明确应急流程、责任人员及处置措施，每年至少组织 1 次演练；

- d) 建立制度动态更新机制，根据法律法规、标准规范及运营实际，及时修订完善信息清除管理制度，保障合规适用；
- e) 建立代理回收点合约管理制度，签订正式合作协议，明确双方在信息清除、产品安全、数据保密等方面的权利义务，并定期监督检查；
- f) 回收经营者基于自身建立的管理体系对代理回收点纳入管理的，宜按照本文件 7.4 管理。

7.3.3 人员管理

相关内容包括：

- a) 设立或明确负责培训与考核的部门或人员，定期对回收环节相关员工（特别是回收、技术、仓储等人员）进行网络安全、数据安全、个人信息保护法律法规和内部制度的培训与考核；
- b) 建立人员权限管理制度，遵循最小必要原则分配系统访问和数据操作权限；
- c) 建立人员招聘与背景审查制度，对信息清除、档案管理、产品保管等关键岗位人员开展背景审查，核查无犯罪及数据安全相关违规记录，确保人员符合岗位要求；
- d) 建立人员保密管理制度，与关键岗位人员签订保密协议，明确保密范围、期限及违约责任，严禁擅自复制、提取、泄露



用户信息、产品信息、清除记录等数据；

- e) 建立人员岗位异动管理制度，关键岗位调岗、离职时，须完成工作交接，收回操作权限、证件及工具等。

7.3.4 信息安全管理体

相关内容包括：

- a) 回收经营者宜建立符合 GB/T 22080—2025 要求的信息安全管理体系；
- b) 回收经营者回收服务过程中涉及处理个人信息的，宜符合个人信息保护相关法律法规和 GB/T 35273 相关要求；
- c) 回收经营者委托第三方处理包含个人信息的电子产品、向第三方提供包含个人信息的电子产品，宜开展个人信息保护影响评估，并留存评估报告至少 3 年；
- d) 回收经营者宜对管理体系开展年度复核与监督审核，保障体系持续有效运行。大型回收经营者宜通过第三方中立机构的检测评估、认证等方式保障信息安全管理体系得到持续有效监督。

7.3.5 再销售管理

再销售的安全管理措施主要包括：

- a) **禁止条款：**未清除用户数据的电子产品、存储介质，禁止再销售和运输出境。

注：已拆除包含用户数据的存储介质的电子产品除外。



- b) **再销售前核验：**在已清除信息的电子产品上市销售前，宜抽样进行核验，抽样率不低于 5%，确保电子产品中无残留用户数据，操作系统处于初始或安全状态。
- c) **再销售记录：**记录再销售电子产品的信息（如序列号）、销售时间、销售渠道（如自营平台、合作商户）及购买方基本信息（如涉及批量采购、出境等情形），确保流通链条可追溯。
- d) **销售后追溯：**回收经营者宜建立再销售追溯制度，购买方发现数据残留反馈的需及时处置，改进管理制度和 workflows，如出现用户数据泄露的需担负相应责任。

7.4 代理回收点管理

7.4.1 概述

将代理回收点纳入回收经营者管理体系，向消费者展示代理回收点符合信息清除强制性国家标准的相关能力，是提升消费者信任使其将闲置电子产品售出，促进资源循环利用的有效措施。同时，从回收的第一步尽可能现场彻底清除用户数据，采信电子产品信息清除日志，可降低二手电子产品流转中信息泄露风险，提升电子产品信息清除工作效率，防止重复执行信息清除造成资源浪费、降低二手电子产品流通利用价值。

回收经营者与代理回收点可自行约定是否将代理回收点纳入回收经营者管理体系。如回收经营者与代理回收点双方约定将代理回收



点纳入回收经营者管理体系，宜符合7.4.2~7.4.4，如代理回收点不具备信息清除能力，则不宜将其纳入至本文件所指管理体系。

7.4.2 信息清除能力建设

相关内容包括：

- a) 代理回收点宜配备经信息清除专业培训并考核合格的作业人员，对作业人员开展岗前及年度信息安全培训，签订信息保密协议；
- b) 代理回收点作业人员宜持证上岗，并以自行佩戴工作证或集中张贴工作证方式公示作业人员信息；
- c) 严禁作业人员私自复制、留存、泄露已回收电子产品存储的用户信息，严禁擅自拆卸、更换电子产品存储介质；
- d) 代理回收点宜自行配备、或由回收经营者配备符合 GB 46864—2025 要求的信息清除的工具或设备，并明确所支持的电子产品范围；
- e) 代理回收点宜设置专门的信息清除作业区，作业区有严格的权限进出管理，并具备对标记为信息已清除、信息待清除的分区妥善保管的场所，禁止非授权人员接触已回收的电子产品；
- f) 代理回收点宜具备对电子产品信息清除后生成信息清除日志，并将信息清除日志同步给回收经营者或信息清除公共服务平台的能力；
- g) 代理回收点宜具备将电子产品进行密封包装、分类标记后进行



寄送的固定渠道。

7.4.3 信息清除流程管理

相关内容包括：

- a) 宜根据 GB 46864—2025，参照回收经营者的管理体系，建立电子产品回收过程的信息清除操作流程；
- b) 宜根据电子产品类型、健康状态、信息清除工具支持范围等明确电子产品进行信息清除的方式（包括指导用户清除、使用信息清除功能或信息清除工具清除、邮寄至回收经营者统一清除等），并根据 7.2.2 b) 或 7.2.3 b) 进行信息清除。

- c) 宜向用户告知电子产品信息清除结果的查询方式、查询周期等必要信息。

注 1：用户自行完成清除的可不提供。

- d) 用户签署已自行执行信息清除的告知同意书、代理回收点作业人员使用信息清除功能或信息清除工具完成现场清除的，宜将电子产品标记为“信息已清除”，并记录信息清除日志，保证信息清除日志不被篡改；

- e) 宜通过安全路径将电子产品信息清除日志同步至回收经营者，且回收经营者将信息清除日志同步至信息清除公共服务平台的，回收经营者无需再次对相应电子产品进行信息清除；

注 2：同步的方式包括：通过网络平台上传、通过存储介质传递、通过在线通讯工具发送、生成信息清除日志码后被扫描等。

- f) 回收经营者管理体系经过第三方中立机构评估且经信息清除公共服务平台授权的，其代理回收点可在完成信息清除的电子



产品外包装或一批次电子产品的整体外包装上张贴信息清除物理标识（见附录 A.3.2）；

- g) 因信息清除工具不适配、电子产品损坏等原因无法进行现场清除的电子产品，宜使用防拆密封材料封装电子产品，加贴防拆封条与“信息待清除”相关警示标记；
- h) 代理回收点宜选用可全程追溯的寄递企业配送，交接时核验包装完整性，回收经营者收到标记为“信息已清除”电子产品的包裹后发现包装破损、封条损坏等异常时需要重新验证电子产品信息清除是否有效。

7.4.4 能力展示及监督管理

相关内容包括：

- a) 经验证具备信息清除能力的代理回收点，宜向消费者展示其具备符合 GB 46864—2025 的信息清除能力；
- b) 代理回收点展示信息清除能力时，宜展示的信息包括但不限于：
 - 1) 代理回收点纳入回收经营者管理体系后，所获得的唯一编号；

注：该编号在第三方中立机构验证代理回收点能力、信息清除公共服务平台查询等环节中作为唯一的标识予以使用。

- 2) 代理回收点所执行的管理制度和操作流程，可采取布置展板、张贴海报等形式直接展示，或采取用户扫描二维码查看等形式予以展示；
 - 3) 代理回收点使用的信息清除工具和支持的电子产品范围；



- 4) 回收经营者管理体系经过第三方中立机构验证且经信息清除公共服务平台授权的，其代理回收点可展示已获取的信息清除标识及信息清除公共服务平台查询渠道（便于用户查询该代理回收点获取的信息清除标识是否有效）；
 - 5) 用户查询电子产品信息清除日志的渠道；
 - 6) 用户向回收经营者及信息清除公共服务平台进行投诉举报的渠道。
- c) 回收经营者宜将代理回收点标记为“信息已清除”的电子产品根据 7.2.3 d) 进行清除效果验证，清除效果验证发现存在清除不彻底情形的，宜督促其对问题进行整改，连续 3 批次验证发现问题的或 1 年内 3 批次存在问题的（如信息清除日志和实际情况不符的），取消其代理回收资格，并对存在问题批次的所有电子产品重新进行信息清除；
- d) 回收经营者宜每年对代理回收点开展至少 1 次现场安全检查，发现问题的督促对问题进行整改，连续检查 3 次存在问题的，取消其代理回收资格；
- e) 回收经营者或信息清除公共服务平台接到用户投诉代理回收点存在信息清除相关问题的，宜对相应批次电子产品信息清除效果进行验证，并进行现场检查；
- f) 代理回收点因经营条件变化等原因导致不再具备信息清除能力，需向回收经营者主动说明，回收经营者需在确认相关情况



后将其从管理体系中移除，移除后的代理回收点不得再使用信息清除相应标识；

- g) 回收经营者通过用户举报、监督检查等发现未纳入回收经营者管理体系的代理回收点违规使用信息清除标识的，宜向信息清除公共服务平台进行报告，并采取法律措施进行维权。

7.5 上门回收管理

回收经营者委派工作人员上门回收的，宜在7.2的基础上，采取以下安全管理措施：

- a) **回收请求：**用户通过线上下单、电话客服等形式发起上门回收请求的，可根据 7.2.1 b) 和 c) 提醒并引导用户自行进行回收前信息清除。
- b) **收货时清除：**收货时用户自行声明已完成信息清除的，需由回收人员查验后由用户签署告知同意书，否则需根据 7.2.2 进行信息清除及管理。
- c) **收货后清除：**因上门回收时不便使用清除工具等原因，经用户同意后回收人员直接取走电子产品的，可在代理回收点或特定作业区域根据 7.2.2 进行信息清除及管理。
- d) **回收后清除：**回收经营者无法在上门收货时或收货后在代理回收点完成信息清除的，宜根据 7.2.3、7.2.4 进行信息清除及管理。

7.6 线上回收管理



线上回收也称物流回收，回收经营者提供线上下单后用户邮递或用户通过回收机投递电子产品方式回收的，宜在7.2的基础上，采取以下安全管理措施：

- a) **线上下单：**用户发起线上回收订单时，回收经营者可根据 7.2.1 b) 和 c) 提醒并引导用户自行进行回收前信息清除。
- b) **设备邮递：**回收经营者宜向用户提供安全可靠的物流合作渠道供用户选择，并根据 7.2.2 e) 和 f) 保障设备邮递过程安全。
- c) **回收机投递：**回收经营者采取部署自助回收机方式回收的，需选用符合物理安全要求的终端、通过部署视频监控、安排专人值守等方式防止用户投递的电子产品被盗。
- d) **回收后清除：**回收经营者在收到用户邮递的电子产品后，宜根据 7.2.3、7.2.4 进行信息清除及管理。





附录 A

(资料性)

信息清除标识样式和使用指引

A.1 概述

信息清除标识是用于表明电子产品信息清除功能、清除工具、回收管理体系等符合 GB 46864—2025 相关要求，或电子产品已完成信息清除的特定图案，旨在向用户、回收上下游展示信息清除能力和电子产品信息清除状态，以增进消费者信任和提升回收工作效率。

信息清除标识为推荐性标识，相关方可自行申请、使用、展示，不影响电子产品厂商、回收经营者等自行采取措施落实 GB 46864—2025 相关要求。

A.2 信息清除标识样式

相关内容包括：

- a) 信息清除标识由图形元素和文字元素组成，整体呈正方形，长宽比为 1:1。
- b) 图形元素包含两个上下重叠的“S”形图案和一个对号图案：一个“S”取自英文“Sanitization”，代表信息清除过程；第二个“S”取自英文“Security”，代表信息安全结果；对号图案位于“S”形图案的右下角，代表信息清除已完成。
- c) 文字元素为强制性国家标准编号“GB 46864”，采用黑体字，水平居中排列在图形元素下方。



- d) 标识使用时宜采用等比例缩放，确保图案和文字清晰可辨。
- e) 标识可采用彩色或黑白形式展示：
 - 1) 彩色版：整体色调为 PANTONE 2945C（深蓝色）；
注：深蓝色对应其他参数为：HEX: #004C97、RGB: 0,76,151、CMYK: C100 M50 Y0 K41。
 - 2) 黑白版：根据需要从 10% 灰度到 100% 黑色自行调节，
标识所有颜色需要统一。
- f) 信息清除标识的标准样式和禁用示例如下，不得修改标识的图形元素、文字内容、颜色比例和整体结构：



图 A.1 电子产品信息清除标识（彩色版）



图 A.2 电子产品信息清除标识（黑色版）



图 A.3 电子产品信息清除标识（30%灰度版）

- 禁用示例 1：修改标识图形元素，如改变“S”形图案的形状或对号的位置；
- 禁用示例 2：修改标识文字内容，如将“GB 46864”改为其他编号；
- 禁用示例 3：改变标识的颜色比例，如使用红色、绿色等非标准颜色；
- 禁用示例 4：拉伸或压缩标识，改变其正方形比例；
- 禁用示例 5：在标识上添加其他文字、图案或水印。

A.3 信息清除标识展示形式

A.3.1 电子标识

信息清除电子标识相关指引包括：

- a) 电子标识宜采用矢量图格式（如 CDR、SVG 等）或高分辨率（不低于 150DPI），确保在屏幕上显示清晰。
- b) 电子标识可展示在以下数字载体上：
 - 电子产品内置信息清除功能的操作界面、完成界面等；
 - 官方信息清除服务站点的网页、移动端 APP 和微信小程序；



- 二手电子产品交易平台的商品详情页、订单页面等；
- 信息清除服务的电子凭证、电子合同和电子报告。
- c) 电子标识可设置为可点击链接，点击后直接跳转至信息清除公共服务平台的对应查询结果页面。

A.3.2 物理标识

信息清除物理标识相关指引包括：

- a) 物理标识宜采用防水、防刮、不易脱落的材质制作，如 PET 不干胶、PVC 标签等。
- b) 物理标识可粘贴或印制在以下实体载体上：
 - 电子产品机身的明显位置（如手机背面、笔记本电脑底部）；
 - 电子产品的外包装盒（包括单个或打包批量外包装盒）、保修卡或说明书；
 - 信息清除服务的纸质凭证、收据或发票；
 - 二手电子产品的标签或展示牌。

A.4 信息清除标识使用场景

A.4.1 回收经营者回收电子产品时使用标识

回收经营者使用信息清除标识的指引包括：

- a) 回收经营者可向第三方中立机构申请信息清除能力相关检测或认证，检测或认证内容包括技术工具、操作流程、管理体系、人员能力、回收点能力验证等。
- b) 回收经营者可向信息清除公共服务平台提交检测报告、代理回



收点验证报告等，申请获得标识使用授权。

- c) 获得授权后，回收经营者可在回收网络平台、自动回收机、代理回收点等展示信息清除标识，且信息清除标识在信息清除公共服务平台可查。
- d) 获得授权后，回收经营者可在完成信息清除的电子产品或批量电子产品外包装加贴信息清除物理标识。
- e) 已完成信息清除的二手电子产品流转或再销售时，如提供信息清除日志码，可将电子标识或物理标识置于信息清除日志码中央进行同步展示。

注：合理规划电子标识或物理标识的大小及位置，不得影响信息清除日志码被正常扫描访问。

- f) 回收经营者宜建立信息清除标识使用台账，记录标识的领取、使用、作废和回收情况，台账保存期限不少于 3 年。

A.4.2 其他情形使用标识

电子产品厂商、信息清除工具开发商等如需申请使用信息清除标识，相关指引包括：

- a) 可自行委托第三方中立机构验证信息清除功能、清除工具、线上/线下信息清除服务的清除效果，清除效果符合 GB 46864—2025 的，可向信息清除公共服务平台提交检测报告、产品型号清单和服务网点信息等，申请获得信息清除标识使用授权。
- b) 获得授权后，信息清除公共服务平台将公示授权信息，相关方可在信息清除功能、清除工具的相应界面、线下服务站点的显



著位置展示信息清除标识。

- c) 当信息清除功能、清除工具或服务发生变更（如功能升级、流程调整）且可能影响其符合 GB 46864—2025 要求时，电子产品厂商需重新申请检测和授权，变更期间暂停使用标识。





附录 B

(资料性)

信息清除日志码编码规则

B.1 二维码基本参数

- 码制：QR Code
- 纠错等级：L（7%）
- 字符集：UTF-8
- 版本：Version 5 ~ Version 10（根据数据长度自适应）
- 最小尺寸：物理标识 $\geq 15\text{mm} \times 15\text{mm}$ ；电子标识 $\geq 100\text{px} \times 100\text{px}$

B.2 编码规则

信息清除日志码宜采用结构化 JSON 或 XML 格式封装，扫描后至少可直接解析出本文件 6.2 中必选字段，无需联网即可本地展示核心信息，联网后可自动跳转至信息清除公共服务平台进行核验，具体规则包括：

- 所有字段不能为空，可选字段无内容填“-”
- 时间格式统一为：YYYY-MM-DD HH:mm:ss
- 编码后可进行 Base64 编码（可选，缩短二维码密度）
- 同一台电子产品全球唯一，不重复、不复用

B.3 解析与使用

- 扫描后优先本地解析展示全部清除信息
- 自动校验日志码哈希值防篡改



- 点击/跳转进入信息清除公共服务平台实时核验
- 解析结果与信息清除日志完全一致





附录 C

（资料性）

用户数据清除告知同意书模板

尊敬的_____客户：

为保障您的个人信息安全，根据《中华人民共和国个人信息保护法》等法律法规及**GB 46864—2025《数据安全技术 电子产品信息清除技术要求》**强制性国家标准等文件要求，在回收您的二手电子产品（以下简称“设备”）时，我们将确认您的设备中的所有用户数据是否已经进行不可恢复的清除。请您仔细阅读并确认以下内容：

一、重要提示

1.在将设备交予我们之前，请您务必自行备份并妥善保存设备中的所有用户数据（如照片、联系人、文档等）。数据清除后将无法恢复。

2.建议您先行使用设备自带的“信息清除”功能（如有，且在电子产品可正常使用的情况下）进行一次用户数据清除操作；如已选择使用符合**GB 46864—2025**的信息清除功能或信息清除工具的，为提升回收效率、降低碳排放，建议选择确认下文的“清除方式一”。

二、用户数据清除告知



1.清除内容：包括但不限于您的个人文件、账户信息、通讯录、短信、通话记录、照片、视频、应用程序及其数据、系统设置等设备内存的所有用户数据。

2.清除标准：我们将按照强制性国家标准GB 46864—2025《数据安全技术 电子产品信息清除技术要求》，采用安全可靠的技术手段对设备存储介质进行数据覆盖、块擦除或物理销毁，确保数据被彻底清除且不可通过技术手段恢复。

3.清除记录：根据GB 46864—2025要求，我们将对信息清除操作日志进行记录，包括设备信息、清除方法、操作时间、清除结果等，日志记录保存期限不少于3年。

三、 用户确认与同意（选择两种方式中的一种）

☐ 清除方式一【自行清除】：本人已阅读并完全理解上述告知内容，确认已自行备份所有需要保留的数据，确认已经使用电子产品自行提供的符合GB 46864—2025强制性国家标准的信息清除功能对用户数据进行完全清除，且已经卸载了电子产品扩展存储介质（如SIM卡、SD卡等），并同意贵方对本次回收的设备（设备信息：品牌型号/序列号_____，可选）的信息清除情况进行记录。

☐ 清除方式二【回收经营者清除】：本人已阅读并完全理解上述告知内容，确认已自行备份所有需要保留的数据，并同意贵方对本



次回收的设备（设备信息：品牌型号/序列号_____，可选）执行上述信息清除操作，并对信息清除情况进行记录。

用户签字：_____

日期：_____年____月____日

注1：回收经营者可根据回收业务特点自行调整和优化上述告知同意书内容，比如仅选择方式二。

注2：告知同意书可通过设置应用程序界面、纸质文档等形式予以展现，其中用户签字也可以用户主动点击“同意”等交互操作方式替代，经用户当面明确授权同意的可由回收人员代为操作。





附录 D

(资料性)

用户追溯信息清除状态的方法与路径

D.1 查询渠道

相关内容包括：

a) 用户可通过回收经营者自行提供的渠道或信息清除公共服务

平台查询电子产品信息清除日志获取电子产品信息清除状态。

注：至少支持查询最近一次信息清除的日志。

b) 查询渠道宜提供以下多种便捷访问方式：

- 网页端：支持电脑浏览器访问，提供单条查询和批量查询功能；
- 移动端 APP：支持鸿蒙、Android、iOS 等常见系统，提供扫码查询、手动输入查询和拍照识别唯一识别码功能；
- 小程序：无需下载安装，提供基础查询功能。

c) 平台需保证 7×24 小时可用，可用性不低于 99.9%，查询响应时间不超过 2 秒。

d) 平台需采取必要的安全防护措施，防止恶意查询、爬虫攻击，除个人查询所必需的信息（电子产品唯一识别码）外，不收集其他个人信息。

D.2 查询操作流程

相关内容包括：

a) 扫码查询流程（如支持）：



- 用户打开平台移动端 APP 或小程序的“清除日志查询”中的扫码相关功能；
- 扫描信息清除日志码（用户自行保存的图片或电子产品张贴的二维码）；
- 平台验证日志码有效性后，实时返回对应的信息清除结果。

b) 手动输入查询流程：

- 用户进入平台的“清除日志查询”相关入口；
- 准确输入待查询电子产品的唯一识别码（IMEI 号、SN 号等）；
- 完成图形验证码验证；
- 平台验证唯一识别码有效性后，实时返回对应的信息清除结果。

c) 查询失败处理：

- 若提示“未查询到相关信息”，用户可核对唯一识别码是否输入正确，或确认该电子产品是否已完成信息清除并同步至平台；
- 若多次查询失败，用户可通过平台客服渠道寻求帮助。

D.3 查询结果内容与凭证

相关内容包括：

- a) 查询结果宜展示 6.2 中的必选信息，以及其他可选信息；
- b) 信息清除公共服务平台宜提供电子凭证功能，用户可下载包含完整查询结果的电子凭证图片（至少支持一种常见图片格式，如 PNG 格式）。
- c) 电子凭证包含但不限于以下防伪元素：



- 信息清除日志码（二维码）；
 - 查询时间戳和哈希值；
 - 平台数字水印或电子签章。
- d) 电子凭证可作为信息清除完成的有效证明，可用于二手交易等场景。

D.4 申诉处理机制

相关内容包括：

- a) 用户对查询结果有异议的，可通过平台提供的在线申诉通道提交申请，也可通过客服电话、电子邮件等方式提交。
- b) 异议申请宜包含以下内容：
 - 用户的联系方式；
 - 具体的异议内容和理由；
 - 电子产品的唯一识别码（如涉及）；
 - 相关证明材料（如购买凭证、回收凭证等）。
- c) 平台在收到异议申请后宜限期（如 15 个工作日）完成受理、核实等工作，核实完成后，平台处理结果需通过短信、平台消息或电子邮件等方式反馈给用户：
 - 经核实查询结果无误的，向用户说明理由；
 - 经核实确属信息错误的，立即更正相关信息，重新生成查询结果和电子凭证，并督促信息清除实施主体限期整改；
 - 经核实存在伪造标识、虚假清除等违法行为的，立即撤销



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

相关标识，并向监管部门上报。



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



参考文献

- [1] 《网络安全法》
- [2] 《数据安全法》
- [3] 《个人信息保护法》
- [4] 《消费者权益保护法》
- [5] 《推动大规模设备更新和消费品以旧换新行动方案》
(国发〔2024〕7号)
- [6] GB/T 35273—2020 信息安全技术 个人信息安全规范
- [7] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
- [8] GB/T 46903—2025 数据安全技术 个人信息保护合规审计要求

