ICS 35.240
CCS L70

T/CAICI

中 国 通 信 企 业 协 会 团 体 标 准

T/CAICI XXXX—XXXX

存储介质数据销毁安全要求和测试方法

Data security requirements and evaluation methods for Data Destruction in storage media

（征求意见稿）

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

中国通信企业协会　　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。

本文件由中国通信企业协会标准化管理委员会提出并归口。

本文件主要起草单位：中国通信企业协会、泰尔认证中心有限公司、中国联合网络通信有限公司研究院、北京通和实益电信科学技术研究所有限公司、北京椰子树信息技术有限公司、中国移动通信集团江西有限公司、联通华盛通信有限公司、中兴通讯股份有限公司、华为技术有限公司、北京华安网信科技有限公司、北京北信源软件股份有限公司、中国移动通信集团云南有限公司、长江存储科技有限责任公司、广州竞远安全技术股份有限公司、山西清众科技股份有限公司。

本文件主要起草人：范贵福、岳玲、凌大兵、陈思宇、王光全、马铮、潘波、汪志、范晓杰、朱正路、朱占东、冯国栋、尤贺、许文强、程墨、左曙光、刘宏、何刚、王程。

本文件为首次发布。

存储介质数据销毁安全要求和测试方法

1 范围

本文件规定了存储介质数据销毁安全要求和测试方法。

本文件适用于存储介质数据销毁管理和数据销毁的技术能力的设计、研发、测试、评估和验收等，包括但不限于数据销毁服务和设备的提供商、用户、测评机构和监管机构等。

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

3 术语、定义和缩略语

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1 数据和定义

3.1.1

数据 Data

任何以电子或者其他方式对信息的记录。

3.1.2

销毁 destruction

通过清除、消磁、粉碎等技术手段使电子信息载体中存储的信息不可再用，且不可恢复的过程。

[来源：TD/T 2692-2014，定义2.6]

3.1.3

数据销毁 Data Destruction

将数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何技术手段恢复的过程。

[来源：GB/T 37988-2019，5.4.1]

3.1.4

数据销毁安全 Data destruction security

通过对数据及其存储介质实施相应的操作手段，使得数据彻底消除且无法通过任何手段恢复，以防范通过对存储介质中的内容进行恢复而导致的数据或信息泄漏风险。

3.2 缩略语

下列缩略语适用于本文件。

ATA	Advanced Technology Attachment	高级技术附件规格
CD	Compact Disc	光盘

CD-ROM	Compact Disk Read Only Memory	只读光盘存储器
EEPROM	Electrically Erasable Programmable Read-Only Memory	电可擦编程只读存储器
DRAM	Dynamic Random Access Memory	动态随机存取存储器
DVD	Digital Video Disc	数字化视频光盘
NVM	Non-Volatile Memory	非易失性存储器
NVMe	Non-Volatile Memory express	非易失性内存主机控制器接口规范
PROM	Programmable Red-Only Memory	可编程只读存储器
RAM	Random Access Memory	随机存取存储器
ROM	Read-Only Memory	只读存储器
SCSI	Small Computer System Interface	小型计算机系统接口
USB	Universal Serial Bus	通用串行总线

4 概述

存储介质数据销毁安全要求和测试方法的制定是为了落实政策法规和国家标准等关于数据销毁的有关规定，本文件给出了数据销毁场景、数据销毁方式以及数据销毁原则概述，给出了数据销毁流程，并从数据销毁安全管理方面和技术要求方面提出数据销毁安全要求和测试方法。

5 数据销毁概述

5.1 数据存储介质类型

根据数据存储介质的原理和特点，数据存储介质主要有以下几种：

a) 磁盘类介质：主要包括磁盘/软磁盘、卡式或盘式磁带、硬盘（包括ATA和SCSI接口制式）等。
b) 光盘类介质：主要包括CD-ROM、DVD、CD等。
c) 闪存类介质：主要包括ATA和SCSI接口制式的固态闪存硬盘、NVMe固态闪存硬盘、USB闪存卡/条、存储卡、板卡上的内置存储芯片等。
d) RAM和ROM类介质：主要包括DRAM存储芯片/存储条、PROM存储芯片/存储条、EEPROM存储芯片/存储条等。

5.2 数据销毁启动条件

数据销毁启动条件包括以下几个场景：

a) 组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的；
b) 个人、组织依据法律规定、合同约定等请求销毁的；
c) 个人依据其合法权益请求销毁的；
d) 数据存储媒介产权发生变更时，需要销毁的；
e) 法律法规规定的其他情况。

5.3 数据销毁场景

数据销毁场景包括以下两种：

a) 存储介质中全部数据销毁场景：对存储介质中存储的所有数据进行销毁的场景。
b) 存储介质中部分数据销毁场景：对存储介质中存储的部分数据进行销毁的场景。

5.4 数据销毁方式

数据销毁方式定义如下：

a） 软销毁：又称逻辑销毁，通过数据覆盖等软件方式清除文件及数据记录的方法，此类方法应保证存储数据从其存储地址被清除，从而保证其不能通过技术手段（包括先进的实验室技术手段）进行读取或复原。

b） 硬销毁：通过采用物理、化学方法直接销毁存储介质，从而彻底销毁其中的数据，保证其不能通过技术手段（包括先进的实验室技术手段）进行读取或复原。

5.5 数据销毁原则

数据销毁应满足以下原则：

a） 合法合规原则：在法律法规规定的范围内，开展数据销毁处理活动。

b） 保密性原则：应对销毁过程中所接触的数据进行保密，不得随意向外泄漏。数据销毁设备在执行销毁作业时，除作业必须的基本数据，如设备序列号、型号和存储结构等信息外，严格禁止读取和传送任何数据信息。

c） 安全可靠性原则：应通过安全可靠的方式对存储介质中的数据或存储介质进行销毁，实现对数据及其蕴含信息的有效清除，以防范通过对存储介质中的内容进行恢复而导致的数据或信息泄漏风险。

d） 就高不就低原则：应依据存储介质载有的最高级别数据确定存储介质的销毁方式，并对应执行销毁措施。

6 数据销毁流程概述

数据销毁流程至少应包括数据销毁启动、数据销毁、数据销毁效果验证、留存销毁记录环节。整体流程如图1所示：

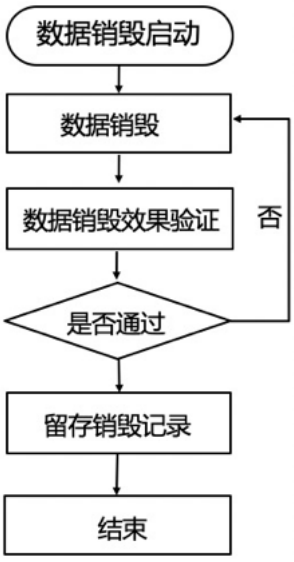

图1 数据销毁流程

数据销毁环节：针对不同存储介质和销毁场景，使用技术手段，使数据彻底删除且无法通过任何技术手段恢复的过程。

数据销毁验证环节：对数据销毁效果进行验证的过程，确认是否完成数据不可复原的数据销毁操作。

留存数据销毁记录环节：对数据销毁过程留存销毁记录，可对数据销毁过程进行溯源。

7 数据销毁安全要求

7.1 数据销毁执行方安全管理要求

7.1.1 机构人员

a) 应建立负责数据销毁的管理部门、岗位和人员，负责制定数据销毁处置规定、介质销毁管理制度，明确销毁对象和流程，配合推动相关要求的执行。
b) 应设置数据销毁监督角色，监督数据销毁过程。
c) 数据销毁相关人员应熟悉数据销毁相关合规要求，能够根据需求使用相应的数据销毁技术、介质销毁工具等。

7.1.2 制度建设

a) 应建立数据销毁制度，明确销毁场景、销毁对象、销毁规则、销毁流程和技术要求等，明确数据销毁审批机制，各类存储介质销毁处理策略和操作规程；留存销毁审批记录和销毁记录，留存时间至少满足1年。
b) 应建立对存储介质进行销毁的监管措施，确保对销毁介质登记、审批、交接、销毁等过程的监控。
c) 应建立数据销毁委托管控制度，明确数据销毁委托场景、委托管控机制等。应使用具备相关资质的服务供应商，应与数据销毁受委托方签署保密协议，明确数据保密要求。
d) 应建立数据销毁台账，包括数据（及介质）所有者信息、数据（及介质）销毁方信息、销毁数据（及介质）的信息、销毁记录、校验记录、销毁后介质使用情况等。其中数据（及介质）所有者信息宜包括所有者部门、联系人、联系人电话，数据（及介质）；销毁方信息宜包括销毁方名称、销毁方联系人、联系方式；销毁数据（及介质）的信息宜包括介质类型、生产厂家、产品型号、产品序列号（或资产号）等；销毁记录宜包括销毁人员信息、销毁开始时间、销毁结束时间、销毁方法、销毁方法/过程具体描述；校验记录至少包含校验方法等。

7.1.3 权限管理

a) 应制定数据销毁权限管理制度，明确数据销毁权限管理要求，包含但不限于账号权限分配原则、流程等，建立并定期更新企业数据销毁处理活动权限分配表。
b) 应建立合理的数据销毁处理活动账号权限开通审批流程，并记录审批流程和结果。
c) 应依照“最小化授权”原则，为用户配置合理的权限，并对所有具有数据销毁处理活动的用户进行身份接入认证和权限控制。设置账号口令的访问控制并满足复杂度要求，限制系统账号口令输入尝试次数，对口令遗忘的申请和重置流程实施严格管理。

7.1.4 销毁效果验证

a) 应建立数据销毁效果验证管理机制，明确销毁验证流程、验证方式以及应配备的技术支撑工具。
b) 数据销毁后应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前得到完全清除，不可恢复，并做好效果验证。
c) 应留存数据销毁验证记录，验证记录需包括数据销毁验证人员、销毁验证开始时间、销毁验证结束时间、销毁验证方法、销毁验证方法/过程具体描述等，数据销毁验证记录应至少留存1年。

7.1.5 安全审计

a) 应建立数据销毁记录留存管理机制，明确留存数据销毁记录、销毁监控记录，销毁记录至少包括销毁人员、销毁开始时间、销毁结束时间、销毁方法、销毁方法/过程具体描述等，销毁记录留存时间至少1年。
b) 应建立数据销毁安全审计制度，明确审计相关执行部门、审计对象、审计流程、审计内容、审计操作规程、审计结果规范和整改跟踪等内容。
c) 应至少每半年开展一次数据销毁安全审计，并形成审计报告，数据销毁安全审计的内容应包含数据销毁权限控制、数据销毁人员操作行为、数据销毁效果验证有效性等重点环节。审计报告包括审计对象、审计内容、审计时间、审计人员、审计结果，并对审计发现问题进行整改跟踪。

7.1.6 应急响应

a) 应制定数据安全事件应急预案，充分考虑企业涉及的数据安全事件场景，根据事件等级明确应急响应责任分工、工作流程、处置措施等，包括但不限于数据泄露、数据滥用、数据违规使用等场景。
b) 应制定数据安全事件应急演练计划，针对数据泄露、数据滥用、数据违规使用等场景，至少每年开展一次演练，并留存演练记录。根据演练结果优化本单位数据安全保护措施，形成演练总结报告。
c) 发生数据安全事件后，应当按照应急预案，及时开展应急处置，采取措施防止危害扩大，消除安全隐患。涉及法律法规要求需要向上级主管部门报告的安全事件，应当第一时间上报。当发生的数据安全事件涉及个人信息时，应按照相关法律、行政法规要求做好应急处置工作，并按照GB/T 35273-2020中第10.2章节要求进行告知。事件处置完成后立即开展事件调查、问题整改、责任追究，并形成数据安全事件总结报告。

7.2 数据销毁技术要求

7.2.1 磁盘类介质数据销毁技术要求

7.2.1.1 磁盘类介质软销毁技术要求

a) 磁盘类介质全部数据销毁场景

对于磁盘系统采用软销毁方法应满足如下要求，应在所有磁道中写入全“0”、全“F”或其它固定数值或随机数，可执行1次或多次覆写，并确保正确写入和读取。可以参考以下举例顺序或随机选取覆写过程。

- 覆写1：整盘写入00
- 覆写2：整盘写入FF
- 覆写3：整盘按随机数覆写
- 覆写4：整盘写入00
- 覆写5：整盘写入00
- 覆写6：整盘写入FF
- 覆写7：整盘按与覆写3不同模式的随机数覆写

b) 磁盘介质部分数据销毁场景

对于磁盘系统部分数据软销毁方法应满足如下要求：首先应取得待销毁的目标数据存储的目标地址列表，对于目标地址列表中的所有存储地址，写入全“0”、全“F”或其它固定数值或随机数，可执行1次或多次覆写，并确保正确写入和读取。可以参考以下举例顺序或随机选取覆写过程。

- 覆写1：逐地址写入00
- 覆写2：逐地址写入FF
- 覆写3：逐地址按随机数覆写
- 覆写4：逐地址写入00
- 覆写5：逐地址写入00
- 覆写6：逐地址写入FF
- 覆写7：逐地址按与覆写3不同模式的随机数覆写

7.2.1.2 磁盘类介质硬销毁技术要求

采用硬销毁方法应满足如下要求：

a) 对于磁盘、软盘和磁带系统，可采用高磁场消磁法，粉碎、焚烧等物理销毁和化学溶解等方法执行数据销毁，并采用视频等方式全程监控销毁过程，留存销毁记录。
b) 采用高磁场消除法时，应采用磁密闭箱内通过高磁场对介质进行消磁。消磁设备的基本要求为，在启动运行的状态下，其磁密闭箱内的所有任何区域内的磁场强度等于或大于30,000高斯。

c) 采用粉碎法时，粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于0.12毫米。
d) 采用焚烧法时，磁记录媒体部分燃烧至灰烬状态。
e) 采用化学溶解法时，磁记录媒体部分溶解至液体状态。

7.2.2 光盘类介质数据销毁功能要求

7.2.2.1 光盘类介质软销毁技术要求

软销毁方法仅限于可重复擦写光盘类型。对于可重复擦写光盘采用软销毁方法应满足如下要求，应在所有地址中写入全“0”、全“F”或其它固定数值或随机数，应执行至少7次覆写，并确保正确写入和读取。可以参考以下举例顺序或随机选取覆写过程。

- 覆写1: 整盘写入00
- 覆写2: 整盘写入FF
- 覆写3: 整盘按随机数覆写
- 覆写4: 整盘写入00
- 覆写5: 整盘写入00
- 覆写6: 整盘写入FF
- 覆写7: 整盘按与覆写3不同模式的随机数覆写

7.2.2.2 光盘类介质硬销毁技术要求

采用硬销毁方法应满足如下要求：

a) 光盘类介质可采用粉碎、焚烧和化学溶解等方法执行数据销毁，并采用视频等方式全程监控销毁过程，留存销毁记录。
b) 采用粉碎法时，粉碎颗粒度满足以下要求：粉碎后的颗粒任意两点间测量径不大于0.5毫米，记录面的面积不大于0.25平方毫米。
c) 采用焚烧法时，燃烧至灰烬状态。
d) 采用化学溶解法时，溶解至液体状态。

7.2.3 闪存类介质数据销毁功能要求

7.2.3.1 闪存类介质软销毁技术要求

对于闪存类介质采用软销毁方法应满足如下要求：

a) 采用覆写法时，在所有存储地址中写入全“0”、全“F”或其它固定数值或随机数，可执行1次或多次覆写，并确保正确写入和读取。考虑闪存类存储设备的技术特性，宜执行两次覆写。
b) 采用Block Erase方法时，应对执行Block Erase命令。NVM Express类型的闪存存储设备可执行NVM Express Format命令，执行NVM Express Format命令时应采用安全删除模式进行Format操作。

7.2.3.2 闪存类介质硬销毁技术要求

采用硬销毁方法应满足如下要求：

a) 对于USB闪存卡/条、存储卡，可采用粉碎等物理销毁方法执行数据销毁，对于板卡上的内置存储芯片，如能够具体识别存储芯片，可拆除后予以销毁；如不能完全识别存储芯片，应执行整块电路板的物理销毁。并采用视频等方式全程监控销毁过程，留存销毁记录。
b) 采用粉碎法时，应粉碎成任意两点间长度不大于0.12mm的粉末颗粒。

7.2.4 RAM 和 ROM 类介质数据销毁功能要求

7.2.4.1 RAM 和 ROM 类介质硬销毁技术要求

采用硬销毁方法应满足如下要求：

a） 对存储芯片、存储卡或整件板卡可采用粉碎等物理销毁方法执行数据销毁，对于板卡上的内置存储芯片，如能够具体识别存储芯片，可拆除后予以销毁；如不能完全识别存储芯片，应执行整块电路板的物理销毁。并采用视频等方式全程监控销毁过程，留存销毁记录。
b） 采用粉碎法时，应粉碎成任意两点间长度不大于0.12mm的粉末颗粒。

7.3 数据销毁设备安全要求

数据销毁工具/系统/平台/产品的自身安全性和具备的系统管理功能对数据销毁的实施与结果具有重大影响，具体应满足如下要求：

7.3.1 用户管理

a） 应支持用户账号创建、修改和删除等管理功能，应支持账号实名制管理，如提供姓名、手机号等用户身份信息绑定功能，并且身份标识具有唯一性。
b） 应建立合理的账号权限开通审批流程，并记录审批流程和结果。
c） 应依据“最小化授权”和“三权分立”原则，对系统管理人员、数据销毁人员、审计人员角色进行分离设置和权限设置，并可基于用户身份和用户权限，控制用户可访问和操作的数据内容和范围。
d） 应采用口令、生物鉴别方式、短信验证码、电子签名等两种或两种以上组合的鉴别技术对登录用户进行身份鉴别。
e） 应支持账号口令长度、复杂度、有效期和更换周期策略配置。
f） 应支持认证失败策略配置功能，配置内容包括限制连续的非法登录尝试次数、锁定时间、解锁方式等。
g） 应支持用户登录超时退出或锁定等功能，配置内容包括最大超时时间、超时处置方式等。

7.3.2 日志留存

a） 应具备系统操作日志记录功能，日志记录范围应覆盖所有用户访问和操作行为，留存系统运行、告警等记录。用户操作日志记录内容应至少包括操作时间、操作主体、操作对象、详细描述等内容。
b） 应留存数据销毁设备使用和销毁记录。
c） 应支持日志留存时间配置功能。

7.3.3 运维管理

a） 应能具备对数据销毁系统功能的软硬件配置情况、系统性能情况以及资源使用情况监控能力，实现对数据销毁系统的监控。
b） 如果涉及远程数据销毁场景，应支持远程数据销毁程序运行监测能力，应支持远程控制操作并反馈操作结果。
c） 远程管理设备时，应建立安全的信息传输通道。
d） 应对鉴权信息等敏感信息采用密码技术等确保数据传输机密性和完整性。
e） 应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
f） 应提供重要数据的本地数据备份与恢复功能，对重要业务信息、系统数据及软件系统等进行备份和恢复。

8 数据销毁安全测试方法

8.1 数据销毁执行方安全管理测试方法

8.1.1 机构人员

测试编号	8.1.1.1

测试要求	见本文件 7.1.1 机构人员 a）。
测试目的	验证企业数据销毁管理机构、岗位、人员的管理情况。
前置条件	1）已获取企业组织架构、数据销毁岗位、人员清单； 2）已获取企业数据销毁岗位责任说明文件； 2）已获取企业数据销毁人员工作落实文档。
测试方法	文档查验
测试步骤	1）查验企业数据销毁管理责任部门数据销毁岗位和人员名单，是否配备数据销毁管理责任部门，岗位和数据销毁人员。 2）查验企业数据销毁岗位责任说明文件，职责是否包括负责制定数据销毁处置规定、介质销毁管理制度，明确销毁对象和流程，配合推动相关要求的执行。 3）查验企业数据销毁岗位人员工作落实证明文件，核实企业数据销毁责任部门岗位人员是否根据岗位职责落实数据销毁管理要求。
预期结果	1）企业已建立数据销毁管理责任部门，设立数据销毁岗位，并配备数据销毁人员。 2)企业数据销毁岗位职责包括负责制定数据销毁处置规定、介质销毁管理制度，明确销毁对象和流程，配合推动相关要求的执行。 3）数据销毁岗位人员已根据岗位职责落实数据销毁管理要求。

测试编号	8.1.1.2
测试要求	见本文件 7.1.1 机构人员 b）。
测试目的	验证企业数据销毁监督角色设立情况。
前置条件	已获取企业数据销毁监督角色人员清单和责任说明书。
测试方法	文档查验
测试步骤	查验企业数据销毁监督角色人员清单和责任说明书，是否设立数据销毁监督人员，职责是否包括监督数据销毁过程。
预期结果	企业已设立数据销毁监督角色人员，负责监督数据销毁过程。

测试编号	8.1.1.3
测试要求	见本文件 7.1.1 机构人员 c）。
测试目的	验证企业数据销毁相关人员能力情况
前置条件	1）已获取数据销毁人员清单； 2）已获取企业数据销毁人员能力证明材料，包括但不限于能力证书、能力考核等证明材料。
测试方法	文档查验、人员访谈
测试步骤	1）从数据销毁人员清单中抽取 1-2 名，询问相关人员是否熟悉数据销毁相关合规要求，是否具备使用相应的数据销毁技术、介质销毁工具等能力。 2）查看数据销毁人员能力证明材料，是否具备数据销毁相关能力。
预期结果	1）数据销毁人员熟悉数据销毁相关合规要求，具备使用相应的数据销毁技术、介质销毁工具等能力。 2）数据销毁人员具备数据销毁相关能力证书或通过企业数据销毁相关能力考核。

8.1.2 制度建设

测试编号	8.1.2.1
测试要求	见本文件 7.1.2 制度建设 a）。
测试目的	验证企业数据销毁制度建立情况。
前置条件	1）已获取企业数据销毁管理制度； 2）已获取企业数据销毁审批记录和销毁记录。
测试方法	文档查验
测试步骤	1）查验企业数据销毁管理制度，是否明确销毁场景、销毁对象、销毁规则、销毁流程和技术要求等，明确数据销毁审批机制，是否明确各类存储介质销毁处理策略和操作规程，留存销毁审批记录和销毁记录，留存时间至少满足 1 年，并细化了相关要求。 2）抽取某数据销毁记录，验证是否不存在超出数据销毁范围的销毁行为、销毁前是否按照审批流程进行审批，销毁技术方法是否符合管理制度要求。 3）查验企业数据销毁审批记录和销毁记录，确认留存时间是否满足 1 年。
预期结果	1）企业已建立数据销毁制度，明确销毁场景、销毁对象、销毁规则、销毁流程和技术要求等，明确数据销毁审批机制，明确各类存储介质销毁处理策略和操作规程，留存销毁审批记录和销毁记录，留存时间至少满足 1 年，并细化了相关要求。 2）通过抽取数据销毁记录，不存在超出数据销毁范围的销毁行为、销毁前按照审批流程进行审批，销毁技术方法符合管理制度要求。 3）企业已留存数据销毁审批记录和销毁记录，留存时间至少满足 1 年。

测试编号	8.1.2.2
测试要求	见本文件 7.1.2 制度建设 b）。
测试目的	验证企业存储介质销毁监控情况。
前置条件	1）已获取企业数据销毁监督岗位职责说明文件或人员任命书； 2）已获取存储介质销毁记录。
测试方法	文档查验
测试步骤	1）查验企业数据销毁岗位职责说明文件或人员任命书，核实企业是否设置数据销毁监督岗，岗位职责是否包括监督销毁介质登记、审批、交接、销毁等过程。 2）查验存储介质销毁记录，是否完整记录介质销毁的时间、地点、方式、原因；发起人、审批人、监销人等。
预期结果	1）企业已设立数据销毁监督岗，岗位职责包括监督销毁介质登记、审批、交接、销毁等过程。 2）存储介质销毁记录完整记录介质销毁的时间、地点、方式、原因；发起人、审批人、监销人等。

测试编号	8.1.2.3
测试要求	见本文件 7.1.2 制度建设 c）。
测试目的	验证企业数据销毁委托管理情况。
前置条件	1）已获取企业数据销毁委托管理制度；

	2）已获取企业数据销毁委托处理清单； 3）已获取企业与数据销毁委托方签署的保密协议。
测试方法	文档查验
测试步骤	1）查验企业数据销毁委托管理制度，是否明确数据销毁委托场景、委托管控机制等。 2）查看数据销毁委托处理清单，抽取 1-2 个数据销毁委托商，查验受托方是否具备数据销毁相关资质，是否与受托方签署保密协议，明确数据保密要求。
预期结果	1）企业已建立数据销毁委托管理制度，明确数据销毁委托场景、委托管控机制等。 2）数据销毁受托方具备数据销毁相关资质，并与受托方签署保密协议，明确数据保密要求。

测试编号	8.1.2.4
测试要求	见本文件 7.1.2 制度建设 d）。
测试目的	验证企业数据销毁台账建立情况。
前置条件	已获取企业数据销台账。
测试方法	文档查验
测试步骤	查验企业数据销毁台账，是否包括数据（及介质）所有者信息、数据（及介质）销毁方信息、销毁数据（及介质）的信息、销毁记录、校验记录等。
预期结果	企业已建立数据销毁台账，包括数据（及介质）所有者信息、数据（及介质）销毁方信息、销毁数据（及介质）的信息、销毁记录、校验记录等。

8.1.3 权限管理

测试编号	8.1.3.1
测试要求	见本文件 7.1.3 权限管理 a）。
测试目的	验证企业数据销毁权限管理制度建立情况。
前置条件	1）已获取企业数据销权限管理制度； 2）已获取企业数据销毁处理活动权限分配表。
测试方法	文档查验
测试步骤	1）查验企业数据销毁权限管理制度，是否明确数据销毁权限管理要求，包含但不限于账号权限分配原则、流程等； 2）查验企业是否建立并定期更新数据销毁处理活动权限分配表。
预期结果	1）企业已建立数据销毁权限管理制度，明确数据销毁权限管理要求，包含但不限于账号权限分配原则、流程等； 2）企业已建立并定期更新数据销毁处理活动权限分配表。

测试编号	8.1.3.2
测试要求	见本文件 7.1.3 权限管理 b）。
测试目的	验证企业数据销毁处理活动账号权限开通审批情况。
前置条件	1）已获取企业数据销毁处理活动权限分配表； 2）已获取企业数据销毁处理活动账号审批记录。

测试方法	文档查验
测试步骤	查验企业数据销毁处理活动账号清单，抽取 50%账号查验账号开通是否均通过审批。
预期结果	企业数据销毁处理活动账号开通均已通过审批，并留存审批记录。

测试编号	8.1.3.3
测试要求	见本文件 7.1.3 权限管理 c）。
测试目的	验证企业数据销毁处理活动账号权限分配情况和访问控制情况。
前置条件	1）已获取企业账号权限分配表； 2）已获取企业数据处理活动平台系统操作权限。
测试方法	文档查验、人工访谈、测试验证
测试步骤	1）查看企业账号权限分配表，查验是否依照“最小化授权”原则，为用户配置合理的权限，测试验证数据销毁处理设备是否不存在账号超出分配表设置权限的情况。 2）测试验证企业数据销毁处理设备，是否对所有接入的用户进行身份认证和权限控制，包括但不限于通过基于 IP 或 MAC 地址、账号口令等的方式。 3）询问企业人员企业数据销毁处理设备口令复杂度策略，并测试验证企业数据销毁处理设备口令复杂度策略是否有效。 4）询问企业人员是否对口令输入尝试错误次数进行限制，并在可控范围内测试验证企业数据销毁处理设备账号锁定策略是否有效。 5）测试验证企业数据销毁处理设备是否对口令遗忘的申请和重置流程实施严格管理，口令重置流程是否存在业务逻辑设计缺陷，是否留存申请和重置记录。
预期结果	1）企业依照“最小化授权”原则，为用户配置合理的权限，并应用与数据销毁处理设备中，不存在账号超出分配表设置权限的情况。 2）企业数据销毁处理设备具备身份接入认证和权限控制。 3）企业数据销毁处理设备账号口令复杂度满足至少 3 种 8 位要求，具备登录失败锁定机制，对口令遗忘的申请和重置流程实施严格管理。

8.1.4 销毁效果验证

测试编号	8.1.4.1
测试要求	见本文件 7.1.4 数据销毁验证 a）。
测试目的	验证企业数据销毁效果验证制度建设情况。
前置条件	已获取企业数据销毁效果验证管理制度。
测试方法	文档查验
测试步骤	查看企业数据销毁效果验证制度，查验是否明确销毁验证流程、验证方式以及应配备的技术支撑工具。
预期结果	企业已建立数据销毁效果验证制度，明确销毁验证流程、验证方式以及应配备的技术支撑工具，并细化了相关要求。

测试编号	8.1.4.2
测试要求	见本文件 7.1.4 数据销毁验证 b）。

测试目的	验证企业数据销毁效果验证执行情况。
前置条件	1）已获取企业数据销毁记录； 2）已获取企业数据销毁效果验证记录； 3）已获取数据销毁介质操作权限。
测试方法	文档查验、测试验证
测试步骤	1）查看企业数据销毁记录，抽取部分比例销毁记录查验是否对数据销毁销毁进行验证。 2）抽取部分数据销毁对象，根据销毁数据（介质）类型采用合适的技术手段测试是否对数据（介质）进行完全销毁，不可恢复。数据销毁技术测试方法见本文件 8.2 章节。
预期结果	1）企业已对数据销毁效果进行验证。 2）经技术验证，数据销毁后均可满足数据完全销毁，不可恢复要求。

测试编号	8.1.4.3
测试要求	见本文件 7.1.4 数据销毁验证 c）。
测试目的	验证企业数据销毁效果验证记录留存情况。
前置条件	已获取企业数据销毁效果验证记录。
测试方法	文档查验
测试步骤	1）查验数据销毁验证记录，是否包括数据销毁验证人员、销毁验证开始时间、销毁验证结束时间、销毁验证方法、销毁验证方法/过程具体描述等。 2）查验数据销毁验证记录，确认留存时间是否满足 1 年。
预期结果	1）数据销毁验证记录包括数据销毁验证人员、销毁验证开始时间、销毁验证结束时间、销毁验证方法、销毁验证方法/过程具体描述等。 2）数据销毁验证记录留存时间满足 1 年。

8.1.5 安全审计

测试编号	8.1.5.1
测试要求	见本文件 7.1.5 安全审计 a）。
测试目的	验证企业数据销毁记录留存管理情况。
前置条件	1）已获取企业数据销毁记录留存制度； 2）已获取企业数据销毁记录。
测试方法	文档查验
测试步骤	1）查验数据销毁记录管理制度，是否明确留存数据销毁记录、销毁监控记录，销毁记录至少包括销毁人员、销毁开始时间、销毁结束时间、销毁方法、销毁方法/过程具体描述等，销毁记录留存时间不少于 1 年。 2）查验数据销毁记录，确认留存时间是否满足 1 年。
预期结果	1）企业已建立数据销毁记录管理制度，明确留存数据销毁记录、销毁监控记录，销毁记录至少包括销毁人员、销毁开始时间、销毁结束时间、销毁方法、销毁方法/过程具体描述等，销毁记录留存时间不少于 1 年。 2）数据销毁验证记录留存时间满足 1 年。

测试编号	8.1.5.2
测试要求	见本文件 7.1.5 安全审计 b）。
测试目的	验证企业数据销毁审计管理情况。
前置条件	已获取企业数据销毁审计制度。
测试方法	文档查验
测试步骤	查验企业数据销毁审计制度，是否明确审计相关执行部门、审计对象、审计流程、审计内容、审计操作规程、审计结果规范和整改跟踪等内容。
预期结果	企业已建立数据销毁审计制度，明确审计相关执行部门、审计对象、审计流程、审计内容、审计操作规程、审计结果规范和整改跟踪等内容。

测试编号	8.1.5.3
测试要求	见本文件 7.1.5 安全审计 c）。
测试目的	验证企业数据销毁安全审计落实情况。
前置条件	1）已获取企业数据销毁审计报告； 2）已获取企业数据销毁审计问题整改跟踪材料。
测试方法	文档查验
测试步骤	1）查验企业数据销毁审计报告，至少每半年开展一次数据销毁安全审计，数据销毁安全审计的内容应包含数据销毁权限控制、数据销毁人员操作行为、数据销毁效果验证有效性等重点环节，审计报告是否包括审计对象、审计内容、审计时间、审计人员、审计结果。 2）查验企业数据销毁审计问题整改跟踪材料，是否对审计发现问题进行整改跟踪。
预期结果	1）企业至少每半年开展一次数据销毁安全审计，并形成审计报告，审计的内容包含数据销毁权限控制、数据销毁人员操作行为、数据销毁效果验证有效性等重点环节，审计报告包括审计对象、审计内容、审计时间、审计人员、审计结果。 2）企业对数据销毁审计发现问题进行整改跟踪。

8.1.6 应急响应

测试编号	8.1.6.1
测试要求	见本文件 7.1.6 应急响应 a）。
测试目的	验证企业数据安全应急预案制定情况。
前置条件	已获取企业数据安全应急预案。
测试方法	文档查验
测试步骤	查验企业数据安全应急预案，是否充分考虑企业涉及的数据安全事件场景，根据事件等级明确应急响应责任分工、工作流程、处置措施等，并细化相关要求，应急场景是否包括但不限于数据泄露、数据滥用、数据违规使用等场景。
预期结果	企业已制定数据安全事件应急预案，充分考虑企业涉及的数据安全事件场景，根据事件等级明确应急响应责任分工、工作流程、处置措施等，并细化相关要求，应急场景包括但不限于数据泄露、数据滥用、数据违规使用等场景

测试编号	8.1.6.2
测试要求	见本文件 7.1.6 应急响应 b）。
测试目的	验证企业数据安全应急演练情况。
前置条件	1）已获取企业应急演练计划； 2）已获取企业数据安全应急响应演练记录。
测试方法	文档查验
测试步骤	1）查验企业是否根据数据安全事件应急响应预案制定演练计划并定期组织演练，保存演练记录。 2）查验企业数据安全应急响应演练记录，确认企业是否针对数据泄露、数据滥用、数据违规使用等场景，至少每年开展一次演练。 3）查验企业是否根据演练结果优化本单位数据安全保护措施，形成演练总结报告。
预期结果	1）企业根据数据安全事件应急响应预案制定演练计划并定期组织演练，保存演练记录 2）企业针对数据泄露、数据滥用、数据违规使用等场景，至少每年开展一次演练。 3）企业已根据演练结果优化本单位数据安全保护措施，形成演练总结报告。

测试编号	8.1.6.3
测试要求	见本文件 7.1.6 应急响应 c）。
测试目的	验证企业数据安全事件处置情况。
前置条件	1）已获取企业数据安全事件处置记录； 2）已获取企业数据安全事件上报记录； 3）已获取企业个人信息安全事件处理记录； 4）已获取企业个人信息安全事件告知记录； 5）已获取企业数据安全事件总结报告。
测试方法	文档查验
测试步骤	1）查验企业数据安全事件处置记录，是否在发生数据安全事件时及时按照数据安全事件应急预案进行处置，是否未遗漏应急响应流程，是否采取措施防止危害扩大，消除安全隐患。 2）查验数据安全事件上报记录，是否按法律法规要求向上级主管部门进行报告。 3）查验企业个人信息安全事件处置记录，是否在发生用户数据泄露、数据滥用等个人信息安全事件时，当按照相关法律、行政法规要求做好应急处置工作，是否及时将个人信息安全事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体，难以逐一告知个人信息主体时，采取合理、有效的方式发布与公众有关的警示信息。企业告知内容是否包括但不限于安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范或降低风险的建议、针对个人信息主体提供的补救措施、个人信息保护负责人及个人信息保护工作机构的联系方式。 4）查验企业数据安全事件总结报告，企业是否在事件处置完成后立即开展事件调查、问题整改、责任追究，形成数据安全事件总结报告。
预期结果	1）企业在发生数据安全事件时及时按照数据安全事件应急预案进行处置，并采取措施防止危害扩大，消除安全隐患。

	2）涉及法律法规要求需要向上级主管部门报告的安全事件，企业在第一时间向上级主管部门进行报告。 3）当发生的数据安全事件涉及个人信息时，企业已按照相关法律、行政法规要求做好应急处置工作，并及时将个人信息安全事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体，难以逐一告知个人信息主体时，采取合理、有效的方式发布与公众有关的警示信息。企业告知内容包括但不限于安全事件的内容和影响、已采取或将要采取的处置措施、个人信息主体自主防范或降低风险的建议、针对个人信息主体提供的补救措施、个人信息保护负责人及个人信息保护工作机构的联系方式。 4）企业在事件处置完成后立即开展事件调查、问题整改、责任追究，并形成数据安全事件总结报告。

8.2 数据销毁技术测试方法

8.2.1 磁盘类介质数据销毁测试方法

8.2.1.1 磁盘类介质软销毁测试方法

测试编号	8.2.1.1.1
测试要求	见本文件 7.2.1.1 磁盘类介质软销毁技术要求 a）。
测试目的	验证磁盘系统介质，在存储介质全部数据销毁场景下通过覆写方式进行数据销毁的情况。
前置条件	1）已获取数据销毁时所采用的覆写模式（最后一次覆写写入的内容，即全“0”、全“F”或其它固定数值或随机数）； 2）已获取执行数据销毁后的磁盘系统介质。
测试方法	测试验证
测试步骤	采用抽样方式检测对存储单元进行读出检测： 选取相当比例的存储单元进行读取，验证是否与预期的效果一致（如全“0”、全“F”或其它固定数值或随机数）。选取存储单元的原则如下： （1）包含第一个和最后一个对于存储单元；其它验证地址应随机选取； （2）随机选取的地址应包括可访问区域和预留区域； （3）随机选取的地址应以相近的概率覆盖存储介质的各个存储区域。例如，对于多层硬盘，应覆盖所有盘片的两面。
预期结果	对所有抽样检测的存储单元，读出的数据均与验证数据（即最后一次覆写预定写入的内容）完全一致。

测试编号	8.2.1.1.2
测试要求	见本文件 7.2.1.1 磁盘类介质软销毁技术要求 b）。
测试目的	验证磁盘系统介质，在存储介质部分数据销毁场景下通过覆写方式进行数据销毁的情况。
前置条件	1）已获取数据销毁的所有目标存储地址。 2）已获取数据销毁时所采用的覆写模式（最后一次覆写写入的内容，即全“0”、全“F”或其它固定数值或随机数） 3）已获取执行数据销毁后的硬盘系统介质；
测试方法	测试验证
测试步骤	采用抽样方式检测在已获取的目标存储地址列表中进行随机读出检测：

	选取相当比例的存储单元进行读取，验证是否与预期的效果一致（如全“0”、全“F”或其它固定数值或随机数）。选取存储单元的原则如下： （1）包含第一个和最后一个对于存储单元；其它验证地址应随机选取； （2）如目标存储地址列表包含多个物理介质，随机选取的地址应以相近的概率覆盖各个存储存储。例如，对于文件或文件夹存储于多个硬盘，应覆盖所有硬盘。
预期结果	对所有抽样检测的存储单元，读出的数据均与验证数据（即最后一次覆写预定写入的内容）完全一致。

8.2.1.2 磁盘类介质硬销毁测试方法

测试编号	8.2.1.2.1
测试要求	见本文件 7.2.1.2 磁盘类介质硬销毁技术要求 a）。
测试目的	验证磁盘系统介质通过硬销毁方式进行数据销毁的情况。
前置条件	1）已获取磁盘、软盘和磁带系统销毁监控记录。
测试方法	文档查验、测试验证
测试步骤	对于磁盘、软盘和磁带系统，如采用高磁场消磁法，粉碎、焚烧等物理销毁和化学溶解等方法执行数据销毁，查验是否采用视频等方式全程监控销毁过程，留存磁盘、软盘和磁带系统销毁监控记录。
预期结果	1）对于磁盘、软盘和磁带系统，采用高磁场消磁法，粉碎、焚烧等物理销毁和化学溶解等方法执行数据销毁时，已采用视频等方式全程监控销毁过程，留存销毁记录。

测试编号	8.2.1.2.2
测试要求	见本文件 7.2.1.2 磁盘类介质硬销毁技术要求 b）。
测试目的	采用高磁场消除法数据销毁情况，检测磁盘类盘存储介质是否存在可读出的数据。
前置条件	1）已获取执行数据销毁后的硬盘系统介质。
测试方法	测试验证
测试步骤	1）测试方法一：使用数据恢复软件或数据恢复设备对磁存储介质（软盘、硬盘或磁带）进行读出测试，如果无法找到任何数据，那么可以证明存储已经被完全破坏。 2）测试方法二：采用抽样法对磁记录表面进行观察。利用磁力显微镜观察磁表面磁性材料的磁畴结构，如果硬盘已经被完全破坏，那么磁力显微镜可以观察到硬盘表面的磁畴结构已经消失或者变得非常微弱，由此证明存储已经被完全破坏。 抽样原则如下：抽样点位置应近似均匀分布于有效磁记录表面。在检测多层硬盘时，应覆盖每一个盘片的两面，且抽样必须覆盖每个磁记录表面的部分内侧记录介质表面（即靠近硬盘转轴部分的记录点）。
预期结果	1）使用数据恢复软件或数据恢复设备进行读出测试，无法读出任何数据。 2）利用磁力显微镜观察磁表面磁性材料的磁畴结构，应在所有抽样点上观察到硬盘表面的磁畴结构已经消失或者变得非常微弱，由此证明存储已经被完全破坏。

测试编号	8.2.1.2.3
测试要求	见本文件 7.2.1.2 磁盘类介质硬销毁技术要求 c）。
测试目的	验证磁盘系统介质采用粉碎法销毁数据情况。
前置条件	1）已获取硬盘系统介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。

测试编号	8.2.1.2.4
测试要求	见本文件 7.2.1.2 磁盘类介质硬销毁技术要求 d）。
测试目的	验证磁盘系统介质采用焚烧法销毁数据情况。
前置条件	1）已获取硬盘系统介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验及抽样查验
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。焚烧后的磁记录媒体部分燃烧至灰烬状态。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态，磁记录媒体部分燃烧至灰烬状态。

测试编号	8.2.1.2.5
测试要求	见本文件 7.2.1.2 磁盘类介质硬销毁技术要求 e）。
测试目的	验证磁盘系统介质采用化学溶解法销毁数据情况
前置条件	1）已获取硬盘系统介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。磁记录媒体部分溶解至液体状态，无颗粒状残留。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态，磁记录媒体部分溶解至液体状态，无颗粒状残留。

8.2.2 光盘类介质数据销毁测试方法

8.2.2.1 光盘类介质软销毁测试方法

测试编号	8.2.2.1.1
测试要求	见本文件 7.2.2.1 光盘类介质软销毁技术要求 。
测试目的	验证光盘类介质通过擦写方式进行数据销毁的情况。
前置条件	1）仅对可擦写光盘适用； 2）已获取数据销毁时所采用的覆写模式（最后一次覆写写入的内容，即全“0”、全“F”或其它固定数值或随机数）； 3）已获取执行数据销毁后的磁盘系统介质。
测试方法	测试验证、测试验证
测试步骤	采用抽样方式检测对存储单元进行读出检测： 1）根据数据类型选取相当比例的存储单元进行读取，验证是否与预期的效果一致（如全“0”、全“F”或其它固定数值或随机数）。选取存储单元的原则如下： （a）包含第一个和最后一个存储单元；其它验证地址应随机选取； （b）随机选取的地址应包括可访问区域和预留区域；
预期结果	对所有抽样检测的存储单元，读出的数据均与验证数据（即最后一次覆写预定写入的内容）完全一致。

8.2.2.2 光盘类介质硬销毁测试方法

测试编号	8.2.2.2.1
测试要求	见本文件 7.2.2.2 光盘类介质硬销毁技术要求 a）。
测试目的	验证光盘类介质通过硬销毁方式进行数据销毁的情况。
前置条件	1）已获取光盘类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	对于光盘类介质，如采用粉碎、焚烧等物理销毁和化学溶解等方法执行数据销毁，查验是否采用视频等方式全程监控销毁过程，留存销毁监控记录。
预期结果	对于光盘类介质采用粉碎、焚烧等物理销毁和化学溶解等方法执行数据销毁时，已采用视频等方式全程监控销毁过程，留存销毁记录。

测试编号	8.2.2.2.2
测试要求	见本文件 7.2.2.2 光盘类介质硬销毁技术要求 b）。
测试目的	验证光盘类介质采用粉碎法销毁数据情况。
前置条件	1）已获取光盘类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。粉碎颗粒度满足以下要求：颗粒任意两点间测量径不大于 0.5 毫米，任意平面的面积不超过 0.25 平方毫米。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态。粉碎颗粒度满足以下要求：颗粒任意两点间测量径不大于 0.5 毫米，任意平面的面积不超过 0.25 平方毫米。

测试编号	8.2.2.2.3
测试要求	见本文件 7.2.2.2 光盘类介质硬销毁技术要求 c）。
测试目的	验证光盘类介质采用焚烧法销毁数据情况。
前置条件	1）已获取光盘类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。焚烧后的介质燃烧至灰烬状态。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态，光盘类介质燃烧至灰烬状态。

测试编号	8.2.2.2.4
测试要求	见本文件 7.2.2.2 光盘类介质硬销毁技术要求 d）。
测试目的	验证光盘类介质采用化学溶解法销毁数据情况
前置条件	1）已获取光盘类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。磁记录媒体部分溶解至液体状态，无颗粒状残留。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态，磁记录媒体部分溶解至液体状态，无颗粒状残留。

8.2.3 闪存类介质数据销毁测试方法

8.2.3.1 闪存类介质软销毁测试方法

测试编号	8.2.3.1.1
测试要求	见本文件 7.2.3.1 闪存类介质软销毁技术要求 a） 。
测试目的	验证闪存类介质通过覆写方式进行数据销毁的情况。
前置条件	1）已获取数据销毁时所采用的覆写模式（最后一次覆写写入的内容，即全“0”、全“F”或其它固定数值或随机数）； 2）已获取执行数据销毁后的存储系统介质。
测试方法	测试验证、测试验证
测试步骤	采用抽样方式检测对存储单元进行读出检测，根据数据类型选取相当比例的存储单元进行读取，验证是否与预期的效果一致（如全“0”、全“F”或其它固定数值或随机数）。选取存储单元的原则如下： 1）包含第一个和最后一个存储单元，其它验证地址应随机选取； 2）随机选取的地址应包括可访问区域和预留区域。
预期结果	对所有抽样检测的存储单元，读出的数据均与验证数据（即最后一次覆写预定写入的内容）完全一致。

测试编号	8.2.3.1.2
测试要求	见本文件 7.2.3.1 闪存类介质软销毁技术要求 b） 。
测试目的	验证闪存类介质通过 Block Erase 方法进行数据销毁的情况。
前置条件	1）已获取执行数据销毁后的存储系统介质。
测试方法	测试验证、测试验证
测试步骤	采用抽样方式检测对存储单元进行读出检测，根据数据类型选取相当比例的存储单元进行读取，验证是否与预期的效果一致（即所有读取单元的内容均为全“0”）。选取存储单元的原则如下： 1）包含第一个和最后一个存储单元，其它验证地址应随机选取； 2）随机选取的地址应包括可访问区域和预留区域。
预期结果	对所有抽样检测的存储单元，所有读取单元的内容均为全“0”。

8.2.3.2 闪存类介质硬销毁测试方法

测试编号	8.2.3.2.1
测试要求	见本文件 7.2.3.2 闪存类介质硬销毁技术要求 a）。
测试目的	验证闪存类介质通过硬销毁方式进行数据销毁的情况。
前置条件	1）已获取闪存类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	对于 USB 闪存卡/条、存储卡，如采用粉碎等物理销毁等方法执行数据销毁，查验是否识别存储芯片并执行销毁，是否采用视频等方式全程监控销毁过程，留存销毁监控记录。
预期结果	1）对于 USB 闪存卡/条、存储卡等介质采用粉碎等物理销毁等方法执行数据销毁时，对于板卡上的内置存储芯片，如能够具体识别存储芯片，拆除后予以销毁；如不能完全识别存储芯片，执行整块电路板的物理销毁。 2）已采用视频等方式全程监控销毁过程，留存销毁记录。

测试编号	8.2.3.2.3
测试要求	见本文件 7.2.3.2 闪存类介质硬销毁技术要求 b）。
测试目的	验证闪存类介质采用粉碎法销毁数据情况。
前置条件	1）已获取闪存类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。

	2）检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。

8.2.4 RAM 和 ROM 类介质数据销毁测试方法

8.2.4.1 RAM 和 ROM 类介质硬销毁测试方法

测试编号	8.2.2.4.1
测试要求	见本文件 7.2.4.1RAM 和 ROM 类介质硬销毁技术要求 a）。
测试目的	验证 RAM 和 ROM 类介质通过硬销毁方式进行数据销毁的情况。
前置条件	1）已获取 RAM 和 ROM 类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	对于存储芯片、存储卡或整件板卡，如采用粉碎、焚烧等物理销毁等方法执行数据销毁，查验是否识别存储芯片并执行销毁，是否采用视频等方式全程监控销毁过程，留存销毁监控记录。
预期结果	1）对于对存储芯片、存储卡或整件板卡等介质采用粉碎等物理销毁等方法执行数据销毁时，对于板卡上的内置存储芯片，如能够具体识别存储芯片，拆除后予以销毁；如不能完全识别存储芯片，执行整块电路板的物理销毁。 2）已采用视频等方式全程监控销毁过程，留存销毁记录。

测试编号	8.2.2.4.2
测试要求	见本文件 7.2.1.2 RAM 和 ROM 类介质硬销毁技术要求 b）。
测试目的	验证 RAM 和 ROM 类介质采用粉碎法销毁数据情况。
前置条件	1）已获取 RAM 和 ROM 类介质销毁监控记录； 2）已获取数据销毁记录。
测试方法	文档查验、测试验证
测试步骤	1）查看监控记录。 2）抽样检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。
预期结果	1）监控记录应完整记录销毁全过程，包括对介质信息的记录和销毁过程，无跳跃，且无明显视场遮蔽。监控记录的时间标记清晰、连续且无中断。 2）检查销毁后介质形态。粉碎颗粒度满足以下要求：有效磁记录材料颗粒任意两点间测量径不大于 0.12 毫米。

8.3 数据销毁设备安全测试方法

8.3.1 用户管理

测试编号	8.3.1.1
测试要求	见本文件 7.3.1 用户管理 a）。
测试目的	验证数据销毁设备的用户账号管理功能、账号身份唯一性功能。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。

测试方法	测试验证、测试验证
测试步骤	1）创建新的用户，编辑用户信息。 2）绑定用户身份信息。
预期结果	1）可成功创建用户，可对用户信息进行编辑和删除。 2）账号需与用户身份进行绑定，且用户身份标识唯一。

测试编号	8.3.2.1
测试要求	见本文件 7.3.1 用户管理 b）。
测试目的	验证数据销毁设备账号权限审批管理情况。
前置条件	1）已获取企业账号权限开通流程制度。 2）已获取数据销毁设备账号权限清单； 3）已获取账号审批记录。
测试方法	文档查验、测试验证
测试步骤	1）查验企业账号权限开通流程制度，是否明确账号开通审批流程。 2）查验企业数据销毁设备账号权限清单和审批记录，查看账号权限开通是否通过审批。
预期结果	1）企业已建立账号权限开通流程制度，明确账号开通审批流程。 2）企业账号权限开通均按照企业要求进行审批，并留存审批记录。

测试编号	8.3.2.3
测试要求	见本文件 7.3.1 用户管理 c）。
测试目的	验证数据销毁设备权限管理情况。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证、测试验证
测试步骤	1）检查数据销毁设备的权限管理逻辑； 2）检查数据销毁设备能否基于角色配置不同粒度的权限。
预期结果	1）数据销毁设备依据“最小化授权”和“三权分立”原则，对系统管理人员、数据销毁人员、审计人员角色进行分离设置和权限设置； 2）数据销毁设备可基于角色进行权限配置，设置不同粒度的权限。

测试编号	8.3.2.3
测试要求	见本文件 7.3.1 用户管理 d）。
测试目的	验证数据销毁设备身份鉴别能力。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证、测试验证
测试步骤	检查数据销毁设备是否采用口令、生物鉴别方式、短信验证码、电子签名等两种或两种以上组合的鉴别技术对登录用户进行身份鉴别。

预期结果	数据销毁设备采用口令、生物鉴别方式、短信验证码、电子签名等两种或两种以上组合的鉴别技术对登录服务端的用户进行身份鉴别。

测试编号	8.3.1.2
测试要求	见本文件 7.3.1 用户管理 e）。
测试目的	验证数据销毁设备的用户账号口令策略配置功能。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证
测试步骤	创建新的用户，对用户账号口令长度、复杂度、有效期和更换周期策略进行配置。
预期结果	可成功对用户账号口令长度、复杂度、有效期和更换周期策略进行配置。

测试编号	8.3.2.2
测试要求	见本文件 7.3.1 用户管理 f）。
测试目的	验证数据销毁设备账号登录失败策略。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证、人员访谈
测试步骤	1）检查数据销毁设备能否对认证失败策略进行配置，配置内容包括限制连续的非法登录尝试次数、锁定时间、解锁方式等。 2）询问相关人员数据销毁设备是否设置账号登录失败锁定策略。 3）登录测试账号，验证登录失败策略配置是否生效。
预期结果	1）数据销毁设备可对认证失败策略进行配置，配置内容包括限制连续的非法登录尝试次数、锁定时间、解锁方式等。 2）数据销毁设备已设置账号登录失败锁定策略。 3）登录测试账号，登录失败策略配置生效。

测试编号	8.3.2.3
测试要求	见本文件 7.3.1 用户管理 g）。
测试目的	验证数据销毁设备账号超时登出策略。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证、人员访谈
测试步骤	1）检查数据销毁设备能否对用户登录超时退出或锁定进行配置，配置内容包括最大超时时间、超时处置方式等。 2）询问相关人员数据销毁设备是否设置用户登录超时退出或锁定策略。 3）登录测试账号，验证用户登录超时退出或锁定是否生效。
预期结果	1）数据销毁设备可对用户登录超时退出或锁定进行配置，配置内容包括最大超时时间、超时处置方式等。

	2）数据销毁设备已设置用户登录超时退出或锁定策略。 3）登录测试账号，用户登录超时退出或锁定策略配置生效。

8.3.2 日志留存

测试编号	8.3.2.1
测试要求	见本文件 7.3.2 日志留存 a）。
测试目的	验证数据销毁设备日志留存策略。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证
测试步骤	1）登录数据销毁设备，进行数据操作，检查数据销毁设备是否生成用户访问和操作日志，是否留存系统运行、告警记录。 2）用户操作日志是否至少包括操作时间、操作主体、操作对象、详细描述等内容。
预期结果	1）数据销毁设备可对用户访问和操作行为生成用户访问和操作日志，留存系统运行、告警记录。 2）用户操作日志包括操作时间、操作主体、操作对象、详细描述等内容。

测试编号	8.3.2.2
测试要求	见本文件 7.3.2 日志留存 b）。
测试目的	验证数据销毁设备日志时间配置策略。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证
测试步骤	登录数据销毁设备，检查是否支持日志留存时间配置功能。
预期结果	数据销毁设备支持日志留存时间配置功能。

8.3.3 运维管理

测试编号	8.3.3.1
测试要求	见本文件 7.3.3 运维管理 a）。
测试目的	验证数据销毁设备资源监控能力。
前置条件	1）已获取数据销毁设备操作权限； 2）数据销毁设备运行正常。
测试方法	测试验证
测试步骤	检查是否具备系统运行监测功能，查看其监测内容，是否可对数据销毁系统功能的软硬件配置情况、系统性能情况以及资源使用情况进行监控。
预期结果	数据销毁设备具备系统运行监测功能，可查看和监控数据销毁设备各功能模块的软硬件配置情况、系统性能情况及资源使用情况。

测试编号	8.3.3.2
测试要求	见本文件 7.3.3 运维管理 b）。
测试目的	验证远程数据销毁控制端数据销毁程序运行监测能力。
前置条件	1）已获取远程数据销毁控制端设备操作权限； 2）远程数据销毁控制端运行正常。
测试方法	测试验证
测试步骤	1）登陆远程数据销毁控制端，查看是否具备远程数据销毁程序运行监测能力； 2）查看是否具备远程开启、关停数据销毁程序功能。 3）开启或关停远程销毁程序，查看是否能够反馈操作结果。
预期结果	远程数据销毁控制端具备远程数据销毁程序运行监测能力，应支持远程控制操作并反馈操作结果。

测试编号	8.3.3.3
测试要求	见本文件 7.3.3 运维管理 c）。
测试目的	验证远程管理设备时，是否建立安全的信息传输通道。
前置条件	1）已获取信息传输通道说明相关文档； 2）已获取远程数据销毁控制端设备操作权限； 3）远程数据销毁控制端运行正常。
测试方法	文档审查、测试验证
测试步骤	查看产品说明文档有关信息传输通道的相关描述，验证远程管理时是否建立安全的信息传输通道。
预期结果	远程管理时，建立安全的信息传输通道。

测试编号	8.3.3.4
测试要求	见本文件 7.3.3 运维管理 d）。
测试目的	验证数据传输机密性和完整性保护能力。
前置条件	1）已获取数据完整性和机密性保护相关文档； 2）已获取远程数据销毁控制端设备操作权限； 3）远程数据销毁控制端运行正常。
测试方法	文档审查、测试验证
测试步骤	查看产品说明文档有关信息机密性和完整性的相关描述，验证相关保护措施是否有效。
预期结果	具备数据传输机密性和完整性保护机制。

测试编号	8.3.3.5
测试要求	见本文件 7.3.3 运维管理 e）。
测试目的	验证数据销毁系统恶意代码防范管理。

前置条件	1）已获取恶意代码库升级记录； 2）已获取远程数据销毁控制端设备操作权限； 3）远程数据销毁控制端运行正常。
测试方法	文档审查、测试验证
测试步骤	1) 核查是否安装了防恶意代码软件或相应功能的软件。 2) 核查是否定期进行升级和更新防恶意代码库。
预期结果	数据销毁系统安装了防恶意代码软件或相应功能的软件并定期进行升级和更新防恶意代码库。

测试编号	8.3.3.6
测试要求	见本文件 7.3.3 运维管理 f）。
测试目的	验证数据销毁系统备份与恢复管理。
前置条件	1）已获取数据销毁系统备份和恢复策略文档； 2）已获取数据备份记录和恢复记录。
测试方法	文档审查、系统查验
测试步骤	1) 核查备份与恢复管理制度是否明确备份方式、频度、保存期等内容。 2）核查是否按照备份策略进行本地备份。 3)核查备份结果是否与备份策略一致，是否对重要业务信息、系统数据及软件系统等进行备份。 4)核查近期恢复测试记录是否能够进行正常的数据恢复。
预期结果	具备重要数据的本地数据备份与恢复功能，对重要业务信息、系统数据及软件系统等进行备份和恢复。

参 考 文 献

[1] NIST Special Publication 800-88r1。