ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31500—2015

信息安全技术
存储介质数据恢复服务要求

Information security technology—
Requirement of data recovery service for storage media

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、国家保密科学技术研究所、中国信息安全认证中心。

本标准主要起草人:叶红、王笑强、马朝斌、陈晓桦、魏连、张羽、蔡平、张翔、范晓明、邓本瑜、胡志德、张毅、陈都。

信息安全技术
存储介质数据恢复服务要求

1 范围

本标准规定了实施存储介质数据恢复服务所需的服务原则、服务条件、服务过程要求及管理要求。

本标准适用于指导提供存储介质数据恢复服务机构针对非涉及国家秘密的数据恢复服务实施和管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 50073—2001 洁净厂房设计规范

GB 50174—2008 电子信息系统机房设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子数据 digital data

基于计算机应用和通信等电子化技术手段形成的客观资料，一般用以表示文字、图形符号、多媒体等信息，包括以电子形式存储、处理或传输的静态数据和动态数据。

3.2

存储介质 storage medium

承载电子数据的各类载体或设备，包括但不限于计算机硬盘、磁带、软盘、光盘、各种形式的存储卡等。

3.3

数据恢复 data recovery

通过专门的计算机软硬件技术，修复存储介质内无法正常读取的电子数据的过程。

3.4

镜像 imaging

逐比特复制存储介质内电子数据的过程。

3.5

硬件故障 physical damage

由于存储介质硬件损坏而造成数据无法访问的故障，一般是指电路故障、机械故障、固件故障、存储介质缺陷等。

3.6

软件故障 logical damage

由于存储介质中用户数据损坏而造成数据无法访问的故障，一般是指操作系统故障、应用软件故障、用户误操作、计算机病毒破坏等。

3.7

开盘修复　interior disk repairing

打开硬盘盘体或拆取存储芯片，排除存储介质硬件故障的操作。

3.8

数据销毁　data destruction

使用覆盖、消磁等技术手段，清除存储介质上所有数据的操作。

3.9

写保护　write blocked

保证存储介质中电子数据无法被修改的防护措施。

3.10

远程数据恢复　remote data recovery

通过网络实现不同区域之间的数据恢复服务方式。

4　服务原则

存储介质数据恢复服务应在安全保密的前提下，将无法正常读取的数据从存储介质中复原，使其可正常使用。实施存储介质数据恢复服务应当遵循如下基本原则：

a）　可用性原则：恢复的数据可正常使用；

b）　保密性原则：服务过程中应按照合同对客户个人信息及用户数据严格保密；

c）　完整性原则：数据恢复过程中确保客户送修存储介质中的数据不被篡改；

d）　可核查原则：应确保数据恢复过程中对存储介质的操作可追溯。

5　服务条件要求

5.1　从业机构

从业机构应符合如下要求：

a）　应具有合法经营资格和专业的技术团队。

b）　应制定管理制度并采取防止数据泄露的技术措施保护客户数据安全。

5.2　从业人员

从事数据恢复服务的人员应该具备如下条件：

a）　遵守国家法律法规，与从业机构签署劳动合同和保密协议，承担保密义务；

b）　具有良好的计算机应用知识，熟悉计算机系统结构、数据存储原理等专业知识；

c）　实施存储介质软件故障恢复的技术人员应掌握各种应用操作系统、文件系统的基础理论知识和相关软件和设备使用方法，具有处理软件故障的能力；

d）　实施存储介质硬件故障恢复的技术人员应掌握各类电路板、硬盘结构、存储芯片的基础理论知识和相关软件和设备使用方法，具有处理硬件故障的能力。

5.3　服务场所及机房

5.3.1　服务场所

数据恢复服务机构应具有独立的、面积适宜的、配备相关设备和消防设施的服务场所；应根据不同的功能划分相互独立的客户接待区、机房和管理办公区。

5.3.2 机房

数据恢复服务机构应具备独立的机房，专门用于数据恢复的技术实施。实施硬盘开盘操作应当在不低于六级洁净等级的洁净环境中进行。洁净环境建设要求应按 GB 50073—2001，机房建设要求应按 GB 50174—2008。

5.4 设备配置

实施数据恢复服务应配备的软、硬件工具基本要求见表 1。

表 1 数据恢复服务软、硬件工具基本配置要求

序号	工具类别	配置要求	性质
1	数据恢复工作专用计算机及配套设备	a) 配置基本的正版操作系统和正版软件工作环境及必要的硬件配套设备； b) 写保护设备必须有明确的写保护方向标识	必备
2	数据镜像工具	必须具有写保护功能，或该工具的物理接口可以与写保护设备相连	必备
3	数据销毁工具	必须支持逐比特数据覆盖功能	必备
4	软件操作工具	配置正版的软件工具，包括文件系统恢复工具、数据文件恢复工具、十六进制编辑工具等	必备
5	备件	应具备可用于硬件故障恢复的，可替代存储介质故障部分的零部件等备品备件	硬件故障恢复必备
6	硬件操作工具	洁净工作台、显微镜、开盘工具、焊接设备、固件操作工具、万用表等	硬件故障恢复必备

6 服务过程要求

6.1 概述

存储介质数据恢复的实施过程可分为介质接收、介质检测、数据恢复、数据交付、数据销毁 5 个主要环节，其主要工作内容包括：

a) 介质接收：接收存储介质并记录存储介质情况；
b) 介质检测：判断存储介质故障类型，制定数据恢复方案；
c) 数据恢复：排除存储介质故障，提取可用数据；
d) 数据交付：将数据恢复结果交付给客户；
e) 数据销毁：销毁数据恢复结果和数据恢复操作过程中产生的所有相关数据信息。

上述各环节责任人应对操作及结果进行记录并签字。

6.2 介质接收

介质接收环节的实施要求如下：

a) 检查送修存储介质，记录其基本情况，包括类型、品牌、型号、序列号及外观特征；
b) 指导客户描述送修存储介质的故障现象，包括故障出现前后的操作、故障表现，并记录上述信息；

c) 指导客户描述需要恢复的数据特征，并记录上述信息；
d) 告知客户数据恢复实施的相关风险及后果、客户及数据恢复服务机构的职责；
e) 客户与数据恢复服务机构应签署服务协议，协议基本内容包括存储介质的基本情况、修复需求、修复风险及各方责任和义务。

6.3 介质检测

介质检测环节的实施要求如下：
a) 检测送修存储介质故障类型，判断本机构是否具备实施条件，若不具备实施条件，应中止数据恢复操作并返还给客户送修存储介质，并对客户说明无法实施的原因；
b) 对于具备实施条件的，应根据故障类型制定恢复方案，方案包括技术路线、使用方法、软硬件工具、人员时间安排和操作方法等。

6.4 数据恢复

数据恢复环节的实施要求如下：
a) 根据存储介质检测结果实施数据恢复操作，需要实施硬盘开盘操作应获得客户书面授权，并在符合要求的洁净环境中实施；
b) 当存储介质可正常读取后，采用写保护措施对原始存储介质实施镜像，镜像完成后，软件故障的排除需要在镜像数据上进行；
c) 恢复出的可用数据需保存在专用数据存储设备中，不得覆盖镜像数据或客户的原始数据；
d) 实施远程数据恢复时，双方均需在符合本标准机房要求的环境中进行，并由专人相互配合，共同完成数据恢复技术操作；
e) 实施远程数据恢复时，需采取保证系统安全及信息传输安全的技术措施；
f) 应对原始数据进行保护，不得更改和删除原始存储介质上的数据。

6.5 数据交付

数据交付环节的实施要求如下：
a) 数据恢复实施方案完成后，需根据客户描述确认数据的可用率，并将结果如实告知客户，由客户对恢复结果进行确认；
b) 将数据恢复结果按照客户指定方式进行数据交付；
c) 数据交付时，应完整归还客户送修的存储介质。

6.6 数据销毁

数据销毁环节实施要求数据交付完成后，应根据协议约定及时销毁数据恢复结果及操作过程中产生的所有相关数据信息。

7 服务管理要求

7.1 人员

人员管理要求：
a) 人员管理应当权责分明，对所有人员定岗定责；
b) 数据恢复服务机构有义务对员工进行职业道德教育和技能培训，每年至少两次，并对培训过程及结果进行记录。

7.2 设备

数据恢复设备管理要求：

a) 应建立设备维护和管理制度；
b) 所有设备应做到专机专用，不得安装使用与数据恢复无关的应用程序；
c) 在数据恢复过程中，除用于远程数据恢复的计算机外，其他设备不得连接互联网；
d) 未经批准，不得改变现有设备的配置。对软硬件配置的重大变更，应先形成方案文件，经讨论并获得相关负责人批准后，由具备资格的技术人员进行更改，并保留更改和操作记录；
e) 未经批准，不得在现有设备网络中加入外来移动存储介质；
f) 未经批准，不得将存储介质带出机房；
g) 通过网络传输的数据文件需要经过加密；
h) 专用设备只能由指定人员进行操作；
i) 定期检测设备运转情况，进行必要的升级维护，保障设备运转正常。

7.3 机房

机房管理要求：

a) 机房应安装门禁系统，只允许数据恢复工作人员进入，其他人员进入需要经过审批；
b) 机房应安装录像监控系统，监控范围应覆盖整个机房，且录像记录应至少保存 1 个月；
c) 机房应对不同功能区域进行物理划分，并建立访问登记制度；
d) 确定责任人定期检查机房设备设施的运转情况，查验相关日志信息，及时排查故障隐患；
e) 机房内的资料、数据、配置参数等信息应妥善保管，未经批准不得以任何形式提供给其他无关人员。

7.4 存储介质

存储介质管理要求：

a) 存储介质管理包括客户盘、工作盘、备件盘；
b) 存储介质管理应遵循易取易存原则，集中存放、分类管理，应建立专用的存储介质库并安排专人管理；
c) 应建立存储介质档案，对存储介质逐一编号，详细记录其品牌、型号、容量、序列号及性能等信息；
d) 客户存储介质应粘贴唯一性标签，同一工作单的客户存储介质应集中放置一处，并在专门防磁、防静电的存储环境中保存；
e) 存储介质管理员负责对存储介质库的维护和管理工作，应建立出入库登记制度，并定期盘点。

7.5 质量控制

7.5.1 抽查

应制定并实行质量抽查制度，按月对数据恢复进度和结果以及服务承诺进行抽查，抽样数量不低于当月总业务量的 5%，抽查结果应详细记录。

7.5.2 投诉处理

应建立良好的投诉处理机制：

a) 应在网站和服务场所显著位置公布投诉电话，为客户提供投诉渠道，包括邮件、电话、信函和面

谈等形式；

b） 接受客户投诉时，需记录并核对如下信息：投诉人的姓名、地址和联系方式、投诉的原因、目的、要求等投诉细节；

c） 受理投诉后，应核实投诉人所叙述的投诉细节是否属实，对于投诉属实的应确定相关事件责任人，并组织整改。

7.5.3 客户回访

数据恢复服务完成后，应对客户进行回访，了解数据恢复服务质量，并根据回访情况实行服务改进。