

# 客户数据 安全

策略和程序公告

## Seagate Recovery Services™

对于希捷恢复服务来说，客户媒介的数据安全具有最高优先级。策略和程序与网络和设备安全系统共同构建了一个保护环境，保护客户媒介和数据，避免任何破坏。

希捷恢复服务数据安全策略的重要组成部分如下。

### 网络安全系统

希捷采用冗余的、多级安全网络架构。所有的子网都受到状态监视防火墙的保护，并且实施细粒度存取管控，其提供的服务受到一定的限制，只能够在必要的情况下访问特定的功能应用层。希捷部署了高级的入侵检测和防护系统，由第三方安全公司提供 24×7 监控。所有的系统都安装防病毒、防垃圾邮件和防间谍程序等安全软件，避免受到恶意软件的影响。

希捷定期实施网络和应用程序脆弱性检测，鉴别和解决潜在的安全问题。第三方审计团队每年实施安全渗透测试。另外，希捷公司每年都进行 ISO 27001/2 企业安全评估。安全评估也包括安全管理能力、成熟度和 ISACA 相关技术控制目标 (COBIT 4.1) 合规性的评估。

### 设施安全系统

所有的希捷恢复服务实验室都配备了访问控制系统（包括生物指纹密码锁），24×7 安全监控系统，视频监控系统和告警系统。

另外，使用耐火的、访问受控的存储容器，进一步保护硬盘，避免未授权的访问或者环境污染。

对客户媒介的所有的访问都局限于授权的实验室工作人员，并且需要获得适当的许可。只有通过严格的安全背景检查，并接受全面的数据恢复流程培训以后，才能获得适当的许可，所有这些都是为了保护客户媒介和数据。

## ISO9001-认证恢复流程

所有的实验室都经过 ISO 认证，确保提供最高质量的服务，以及保证客户数据的安全。

ISO 流程包括：

- 在专门为数据恢复设计的数据库系统中，为客户媒介编制详细的条码和目录，从而可以追溯恢复处理流程、人员和资源。
- 开发了专门的数据恢复硬件、软件和恢复流程，将偶然的数据丢失可能性降低至最小程度。
- 在恢复完成之后，在恢复过程中使用的所有室内媒介都需要在再次使用之前被安全地清洁。

## 客户媒介安全处置

如果客户决定在恢复流程结束以后对他们的媒介进行处置，则希捷恢复服务提供一种免费的、环境友好的硬盘处置服务。

该过程使用安全的希捷设施，将客户媒介切成碎片，所产生的废料可以循环利用。在这个过程中，客户数据被安全地销毁，将来也没有任何恢复的可能。

[www.seagate.com](http://www.seagate.com)

美洲地区 希捷公司, 10200 South De Anza Boulevard, Cupertino, California 95014, United States, +1 408-658-1000  
亚太地区 希捷新加坡国际总部, 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485-3888  
欧洲、中东和非洲地区 希捷公司 SAS, 16-18, rue du Dôme, 92100 Boulogne-Billancourt, France, +33 1-41-86-10-00

© 2012 年希捷公司版权所有。保留所有权利。Seagate、Seagate Technology 和 Wave 标识是希捷公司的注册商标。Seagate 恢复服务是希捷公司的注册商标或商标，或者在美国和/或其他国家的一个附属公司。其他产品名称是各自所有者的注册商标或商标。希捷保留更改产品类别或规格的权利，届时不再另行通知。TP640.1-1206CN, 2012 年 6 月