# Client Data Security

Policies and Procedures Bulletin

## Seagate Recovery Services™

Data security for client media is a top priority for Seagate Recovery Services. Policies and procedures are in place along with network and facility security systems to create a system to help protect client media and data against any breach or damage.

The primary components of Seagate Recovery Services data security policy are as follows.

### Network Security System

Seagate employs redundant, multi-tiered secure network architecture. All network subnets are protected by stateful inspection firewalls with granular access controls which limit service to only those necessary for the application layer to function. Seagate deploys advance Intrusion Detection and Prevention Systems, monitored 24×7 by a third-party security firm. All systems are protected against malware using anti-virus, anti-spam and anti-spyware security software.

Seagate performs periodic network and application vulnerability testing to identify and remediate potential security issues. An annual security penetration test is conducted by a third-party audit team. In addition, each year Seagate conducts an ISO 27001/2 enterprise security assessment. The security assessment also includes evaluation of security management capability, maturity and compliance with ISACA Control Objectives for Information Technology (COBIT 4.1).

### Facility Security System

All Seagate Recovery Services labs are equipped with controlled access (including biometric locks), 24×7 security surveillance, video surveillance and alarm system.

# Client Data Security

In addition, fireproof and controlled-access storage containers are used to provide further protection against unauthorized access or environmental contamination.

All access to client media is restricted to authorized lab personnel with appropriate clearance. Appropriate clearance is granted only after rigorous background security checks and extensive training in data recovery procedures, all in order to safeguard client media and data.

## ISO9001-Certified Recovery Process

All labs are ISO certified to ensure the highest quality of service and safety of client data.

ISO Procedures include:

- A detailed inventory of client media is *barcoded* and cataloged in a proprietary database system specifically designed for data recovery services, which provides detailed tracking of procedures, personnel, and resources involved throughout the recovery process.
- Proprietary data recovery hardware, software and recovery procedures have been developed to minimize any possible inadvertent data loss.
- Following the conclusion of the recovery case, all in-house media used during the recovery is securely wiped out before reuse.

## Client Media Secure Disposal

In the event a client decides to have their media disposed of at the conclusion of the recovery process, Seagate Recovery Services provides free of charge an environmentally friendly service for the disposition of client hard disk drives.

This process utilizes a secure Seagate facility to shred the client media into small pieces, allowing the scrap material to be recycled. The client data is securely destroyed during this process, not allowing for the possibility of any future recovery.

**www.seagate.com**

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00