



Recommended Security Protocols for Data Recovery Service Providers

The National Institute of Standards and Technology now advocates proper security vetting of data recovery service providers before turning over equipment and data.*

In an independent study conducted by the Ponemon Institute among IT security and IT support practitioners, 83% reported their organization had at least one data breach in the past two years. Of the 83%, 19% said the breach occurred when a drive was in the possession of a data recovery service provider, and 43% said the breach was due to a lack of data security protocols.

*To mitigate the risk of breach, the following protocols** were recommended for all data recovery service providers:*

- Proof of internal information technology controls and data security safeguards, such as compliance with SAS 70 Type II audit reports
- Proof of certified secure network
- Proof of certified ISO 5 (Class 100) cleanroom
- Engineers trained and certified in all leading encryption software products and platforms; use of encryption for data files in transit
- Proof of chain-of-custody documentation
- Secure and permanent data destruction when required
- Vetting and background checks of its employees

Protect your critical data. Ask your data recovery service provider for proof they meet the recommended protocols.

**Download the Ponemon survey at:
www.drivesavers.com/ponemon**

*Source: NIST SP 800.34 (Rev.1), Section 5.1.3

**Source: "Security of Data Recovery Operations" — Ponemon Institute, LLC — 2009