INFORMATICA

INFORMATION SECURITY & RISK MANAGEMENT

www.InformationSecurityCanada.com

Securing Backup Data

8 Best Practices for Executives and IT Managers

1. Once you have a reliable back-up system in place, augment its functionality with a strong, hardware-based encryption system.

2. Audit and review all access to tape storage locations and containers. Build an access control list into your existing security policy set

3. Have in-house personnel irretrievably destroy old tapes and verify/document their physical destruction.

4. Always, always, always audit third-party data storage providers for security policy enforcement, access control measures and service level agreements.

5. Always audit, preferably on a yearly basis, data (paper, media, etc) destruction companies for irretrievability of content.

6. Ensure that you have a protocol for identifying third party company representatives and only surrendering corporate data to them in sealed containers.

7. Use segregation of duties enforced by policy for all personnel handling back-up data. Document all access, testing, backup & restore cycles.

8. Considering an ‘online’ or ‘Internet-based’ backup system? Understand the security risks and always ensure that the service provider’s security is independently audited.