

Offsite Tape Vaulting**GUIDE TO IMPROVING YOUR
TAPE STORAGE PRACTICES****DATA SECURITY: IT'S NOW STRATEGIC**

Now, more than ever, it is critical that organizations implement solid media management practices across all business units. And these practices should build to a comprehensive and consistently applied media management master plan.

Organizations that follow a planned, well-structured model have the opportunity to strengthen their brand by reducing the risk of information loss, inadvertent disclosures, and downtime during unplanned outages. Collectively, that improves efficiencies and increases competitive advantage.

For decades, Iron Mountain has worked with many of the world's largest organizations to design, plan, and implement secure end-to-end data-protection strategies. The following white paper highlights many of the best practices and proven techniques for strengthening all phases and milestones of the data backup continuum.

PERFORM A RISK ANALYSIS

To start, it's a good idea to conduct a tactical audit of each step of your backup process to identify security vulnerabilities. For instance, are boxes of tapes left in the open? Is there a tight, end-to-end chain of custody for your backup tapes?

Is data backed up and transported in clear, unencrypted formats? Do you geographically separate your tapes from the data center in case of a disaster?

Vulnerabilities like these should be easy to detect and eliminate. Ideally, this tactical analysis should be conducted by an internal audit team or external third party. You can even align this with your regulatory practices to evaluate how the data center is configured to accurately execute backup processes.

IDENTIFY SENSITIVE DATA

Privacy laws are constantly increasing the scrutiny on organizations that maintain personal data and are continuing to introduce disclosure requirements around nonpublic or private information. It is important to identify and separate these files, databases, and formats that are sufficiently sensitive to warrant encryption. Additionally, know where that data resides. In many instances, data is duplicated throughout the organization. Design your policies and procedures to identify where data lives at any point in time. For example, companies have information on laptops that may also exist in duplicate on a network drive or in a backup repository used by the PC.

ENCRYPT YOUR DATA

The fact is, virtually every backup tape will almost certainly contain vital, sensitive, or confidential information. While it can slightly increase the cost and time required for recording the backup, today's best practices call for companies to encrypt all data that is backed up. In the end, when one compares the cost of encryption with the potential risks and the likelihood of a data breach, it quickly makes economic sense to implement encryption broadly.

ADOPT A MULTILAYERED SECURITY APPROACH

Just as companies are careful to ensure that sensitive financial processes have the inherent checks and balances of multiple authorizations, it's prudent to enact similar measures for data backups. Ensure that the person creating the backup tape is not the one who confirms that the backup was placed into the proper container for offsite storage. If one person makes the backup, another should test or verify it. This prevents a single point of failure.

- **Authentication.** Apply multilevel authentication and anti-spoofing techniques.
- **Authorization.** Enforce privileges based on roles and responsibilities rather than full administrative access. Where possible, leverage role-based administrative capabilities of storage-management applications – especially backup.
- **Auditing.** Logs of administrative operation by any user should be maintained to ensure traceability and accountability.

COPY YOUR BACKUP TAPES

It's no longer acceptable for organizations to simply depend on a single backup copy of its data. While tape media can have a long life, it remains susceptible to environmental and physical damage and other anomalies. The recommended best practice is to copy the backup tapes and then send the copy offsite so that you have at least two distinct, physically separate options for restoring data. This exponentially increases your reliability.

MOVE BACKUPS OFFSITE

Onsite storage is a poor practice for data backups. While you've made copies, those copies are vulnerable to any number of events and threats, ranging from natural disasters to thefts or malicious destruction. However, that doesn't mean an IT manager can simply drop a tape into his briefcase and take it to his basement or garage. Offsite data protection requires thoughtful procedures, facilities, and skilled partners to create a streamlined end-to-end process that eliminates risks and vulnerabilities to data backups. Some of the key considerations include:

- **Bar Coding.** Comprehensive bar coding of media ensures proper tracking every time a tape is moved to an offsite location. Tracking each individual piece of media and the container it is transported or stored in is the control mechanism that auditors prefer.
- **Background Checks.** Be certain that your offsite partner conducts thorough background checks on every one of its employees.
- **Location Security.** Offsite facilities must be appropriately secured. No unauthorized person should be able to gain access to the vaults.
- **Environmental Controls.** Sensitive tape media require transit and storage locations that control temperature and humidity and constantly monitor changes in both. Tapes should be shipped in proper containers and stored in climate-controlled vaults.

DESIGN AND FOLLOW A RIGOROUS CHAIN OF CUSTODY

A tight, end-to-end chain of custody is essential to preserving the safety and integrity of data backups. The following are key considerations:

- **Use Secured Containers.** Open boxes and bins invite opportunistic thefts. Make sure your tapes are enclosed in locked containers before they even leave the data center. Ensure pickups follow standard operating procedures where a designated, accountable IT person hands over and receives a signature from a known, ID-carrying vendor representative.
- **Perform Daily Reconciliations.** The sooner you find a problem, the more information you have to fix it. A daily reconciliation of your media stored offsite with tapes kept in house is an extra step to ensure tapes end up where they are supposed to be. If any tapes are not accounted for, you can take appropriate steps to close those gaps immediately.
- **Destroy Obsolete Media and Data.** Once media reach obsolescence, confidentially and completely destroy that media by either scrambling the data on the tape or destroying the tape altogether. Data destruction can be performed onsite or by a third-party service with proper certification of destruction.

CONSIDER ELECTRONIC VAULTING

Encrypting and electronically sending your backup data over the Internet to a secure remote facility bypasses the need to physically transport media in a vehicle. This strategy may not be practical for all company data, but is suitable for data that is most critical to the business.

Ensure the vendor offering these services encrypts data while it's transmitted and when it is in storage. Also ensure that the vendor's disaster recovery and replication practices meet rigorous standards.

USE TRAINING TO IDENTIFY AND ELIMINATE PROCESS RISKS AND GAPS

It is important to ensure that the people responsible for carrying out your data backups are informed and trained. Security policies are essential for assigning accountability, responsibility, and authority. Since data loss is a business issue, not just an IT issue, business executives must be educated about the risks, threats, and potential losses from security breaches, as well as the costs of various countermeasures. This enables corporate officers to make informed decisions on the cost/benefit profile of data security investments. Organizations that assess risks and train staff are more likely to implement security policies, procedures, and technologies that protect these vital assets. On the other hand, vulnerable infrastructure and unskilled staff are a problem waiting to happen.

EXECUTE AND TEST YOUR PLAN

Secure data protection is not just about technology. It also involves process, which is essential to test. As a company evolves and changes, information security practices must change as well. Once the end-to-end plan has been developed, defined, and communicated to all participants, test your plan with various simulations. Remember, the test must include both backup and restore operations. Inject any conceivable threat into the process including server and tape loss, network issues, device issues, data classification issues, and other scenarios that might affect the business. Test with staff who may be less familiar with the process. This testing can help ensure that the process is easy to follow and can be executed if the usual person is unavailable due to illness, vacation, or termination.

CONCLUSION

Proper security of data backups doesn't just happen. It requires thoughtful planning and careful controls. Given the implications of failure – reputational damage, direct costs, compliance issues, and suboptimal business operations – companies must allocate proper resources to implementing and maintaining rigorous processes for securing data backups.

For more information, visit www.ironmountain.ca.



ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.ca for more information.