DATA BACKUP AND RECOVERY

BEST PRACTICES

A CHECKLIST FOR BACKUP TAPES

What does it take to **build a fail-safe backup** system? Start by setting up a comprehensive master plan that covers how to **prepare, store and quickly access** your crucial information – and then provide for regular testing and updates. ▶

IRON MOUNTAIN®

A pilot must run through a printed list of pre flight safety checks before takeoff. Likewise, you should have a go-to best practices guide for your company's data backup and recovery plans. The optimal guide removes guesswork and maintains consistency in crucial areas. It should help you:

- **Define a backup system** that lets you grab business-critical data when you need it
- **Measure your system's performance —** and plan ways to make consistent improvements
- **Identify what data to back up** and for how long, so you can eventually erase unneeded information
- **Boost your company's overall performance** by eliminating time-consuming questions or debates about your data backup strategy

With the right system in place, you can ensure that backups are handled consistently and correctly — and that business-critical data is easy to find and recover.

1. UNDERSTAND THE BACKUP TAPE LIFECYCLE

While backup tapes might seem like a slightly retro notion to the average digital consumer, enterprise data professionals know the real deal: Tape is still a vital and hugely practical form of storage and backup. When used correctly, tape is highly secure from outside tampering or hacking.

But putting offsite backup tapes to work for your organization involves much more than merely sending newly created tapes to an archive and retrieving the old ones you need. To ease your education on this topic, visualize the backup system as two cycles, one for outbound data and one for inbound.

You'll need to follow the steps of the outbound cycle carefully to ensure your records' security and integrity:

1. **Eject each backup tape when it's finished.** Verify that it has been ejected correctly. Replace all ejected tapes. Do a count to make sure you have all expected tapes and that they're ready to be transported.
2. **Create an electronic list** of all the tapes being moved. Doing this helps the recipient verify the delivery. Store your media in a container designed for safe transport.
3. Before the vendor picks up your information, **verify the materials** against your electronic list. Make sure your containers are marked as part of a system that identifies anyone making direct contact with their contents.
4. Store media being sent out in a **climate-controlled environment.** From this point on, only your designated partner should be handling these materials.

Most important, you're potentially vulnerable when data leaves your facility. Always verify that you're handing your data to a trusted representative by asking for a personal identification number and a photo ID.

You'll also need to plan for the inbound data cycle, when your backup partner returns media to you. It's crucial that physical media be handled in a structured, consistent manner:

- Receive tapes in the **same secure and climate-controlled area** where you stored your outbound data. Before unloading anything, verify receipt of all expected tapes.
- **Organize your incoming tapes** on a rack designed to store and protect them.
- **Send electronic pick lists** to your offsite storage partner when you haven't previously specified return dates.

2. GATHER YOUR TALENT

One crucial step you'll need to take in this best practices process is controlling employee access. Create an authorization list and review it regularly to make sure that the right staffers are all playing their part. Stay on top of any personnel changes, and make sure to revoke authorization for transferred or terminated staffers.

You'll also need to plan for recovery. Grant a minimum of two employees administrative rights to the backup and recovery system; designate an additional two to manage recovery in the aftermath of a disaster.

3. HEAD OFF PROBLEMS AT THE PASS

Mistakes can certainly occur. However, a solid set of best practices will minimize them, while also helping you identify and correct errors quickly.

Streamline the process by using automated technology that lets you and your information storage provider compare outbound and inbound deliveries. Your system should include bar-coded identification so that scanning devices can track media as they move from place to place. Create a system to log and track any discrepancies.

4. TEST RECOVERY PROCEDURES AGAIN (AND AGAIN)

No matter how strong and secure your system, digital information can be corrupted. The best hedge against such setbacks is a set of best practices for recovering troubled data. As part of this process, only send tapes for storage that back up data contained in your onsite servers. Also conduct regular spot checks. Make certain that data are being written to stored media correctly, that all the data needed for a full recovery is available offsite, and that you can access it on demand.

The process of creating an offsite backup and recovery system comprises many moving parts. But once you spend the time and resources to assemble them, you'll gain priceless peace of mind about your backup procedure – and most anything that can happen with it along the way.

HOW TO LEARN MORE

Do you have questions about data backup and recovery? **Read additional Knowledge Center stories** on this subject, or contact Iron Mountain's Data Backup and Recovery team at 800-899-IRON (4766). You'll be connected with a knowledgeable product and services specialist who can address your specific challenges.

RELATED ARTICLES

- **Build a Better Data and Recovery Backup Plan: The First Five Steps**
- **It's 3 a.m. Do You Know Where Your Records Are?**
- **The Costs of Downtime: What Do You Really Stand to Lose?**

IRON MOUNTAIN®

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.com for more information.