

# Five Best Practices for Offsite Backup

## What You Need to Know

Most people know that it's not enough to just back up your data – you need to also keep copies of it in a different location, in case something happens to your facility. For most organizations, the two main ways of getting backups offsite are through tape and cloud.

These are two different technologies with different considerations, but they serve the same purpose of ensuring data is safe and recoverable, and many of the same principles apply. Regardless of whether you use tape or cloud, here's five best practices to make sure your offsite backups are there and ready when you need them.

## 1 Send Offsite Often



**This is one of the biggest points to remember. It's one thing to make frequent backups, but if the data only goes offsite once a week, then last week's data is all you can count on getting back in a serious incident.**

The latest generation of backup tapes (LTO-6) can store up to 6TB of compressed data, while earlier generations have lower capacity. It can be tempting to let tapes fill up before sending them offsite – resist that temptation. If your “offsite” backup tape is sitting next to your server when the building burns down, you're in trouble. We strongly recommend sending your tapes offsite at least once a day.

With cloud backup, it's best to use replication to ensure changes made on your own servers are kept up to date on your backup vendor's servers as well. With your primary and backup servers synced, you'll never lose more than a few moments' data.

## 2 Ensure Fast Restoration



**Whether you're restoring a single file or an entire file system, when you need your data it should be quickly retrievable.**

This can sometime be a challenge with tape, as you're dependent on another organization to get you your data. When choosing a tape storage vendor, make sure they have a location near you, are staffed 24x7 and offer a guarantee that your tapes are back in your hands within a few hours.

If you're using cloud, make sure the vendor makes your files available to you online at any time. Also be sure to ask about any download size limits or mandatory throttling. If you need to restore an entire server or file system, you'll want to know in advance if your solution imposes limits on how quickly you'll be able to get everything back.

## 3 Use Encryption



**You know your data is valuable...and so do thieves. Any data that goes offsite should be encrypted to ensure its security.**

Encryption is an optional part of the LTO standard, so check carefully to make sure that the tape system you choose includes it. You'll also want an external key management system that works with your tape drive.

If you're using cloud, confirm with your vendor that all data is encrypted in flight and at rest to ensure that if a hacker captures the transmission or attacks the backup servers, your data will be safely unreadable.

## 4 4. Label Everything for Easy Recovery



**YOU might know what everything is and where it's kept, but there's no guarantee you'll be available in a disaster. Clear organization and labeling practices are key to a timely recovery.**

For tapes, be sure to clearly label each tape and record what it contains, and make certain other key people in the organization have access to said record document. This will also help the storage company easily locate exactly which tape you need and get it back to you in a timely manner.

With cloud, the best practice is to have your data available online in the same file format and structure as the original. This will let you or whoever at your organization is restoring the data to just browse the directory tree and find the necessary files.

## 5 5. Test and Verify



**The first time you restore your data from backups should NOT be when you need to recover from a data loss incident – if something went wrong in your configuration, that's pretty much the worst time to find out. You should regularly test your backups and restores to ensure everything is working as intended and iron out any issues before they cause problems.**

If you're using tape, the first step is to always test your tapes before sending them offsite (after all, paying to store uselessly corrupted backups is a special kind of waste). Once you've ensured your backups are in good order and sent them off to your offsite storage vendor, you should regularly pull some back out again to verify that the data can be fully restored.

If you're using cloud, make sure your vendor has an automatic system to verify the integrity of backups when they're received, and that files are regularly rechecked to be sure the data hasn't been corrupted. As with tapes, it's a good idea to personally verify your backups by downloading sample files.

Whether you get your data offsite through tape or in the cloud, you want to make sure it's secure, up-to-date and ready when you need it. By following these best practices, you can help ensure that in a real disaster, your offsite backups are one less thing to worry about.