BACKUP GUIDING PRINCIPLES

Nobody expects a system failure, data corruption, or disaster. Despite good intentions, many backup systems and procedures fail. Over twenty-five years of experience has taught us that shortcuts now can result in significant pain, disruption and expense in the future.

1 **Full Automation:** Backup systems often rely upon humans to perform critical tasks like changing media, checking job status, or transporting data off-site. But the reality is that people can forget...or they miss a few days of work...or worse, an inattentive employee may ignore the task...leaving you at risk. We recommend systems that perform all of the tasks of backup by themselves without requiring your staff to be involved.

2 **Monitored 24x7:** Backups can falsely give *"success"* messages that lead to a false sense of confidence...and undiscovered failure. Monitoring catches failures and reports on conditions that can lead to future failure, too.

3 **Regularly Tested:** Testing of backup systems can reveal failures and can also unearth configuration mistakes. If a backup job was never configured to back up a particular server (drive, directory, file, or application), finding out at the moment when you need the data is just too late. We recommend quarterly testing of backup jobs, including restores and reviews of data sets/job definitions, to ensure that recovery is possible.

Professional backup systems have all of these characteristics:

- ✓ Full Automation
- ✓ Monitored 24x7
- ✓ Regularly Tested
- ✓ Secure and Encrypted
- ✓ Automated Off-Site
- ✓ Offline Backup
- ✓ Complete and Comprehensive
- ✓ Aligned with RPO and RTO

4 **Secure and Encrypted:** Your backup jobs (and media) contain your most sensitive data, and backup media can be particularly vulnerable to security risk. If you use portable hard drives or tape, imagine the damage to your organization if the media goes missing. Will you have to inform your clients? Your vendors? Even if you use Internet-based backup services, failure to adequately secure data-in-transit (and the data in the cloud) creates enormous risk. We recommend that backup systems use a minimum of 256-bit encryption in every location where data is stored.

5 **Automated Off-Site:** Backups are critical in the event of physical damage to systems and/or backup media and damage is more common than you might imagine. Storm damage, fire, water leakage/damage, theft, or employee sabotage are just some of the risks to computer systems. Without off-site storage of backup data, these events could simply render a system unrecoverable.

SUCCESS Computer Consulting can help you choose from a variety of technologies that align with these guiding principles.

SUCCESS COMPUTER CONSULTING

info@sccnet.com
763.593.3000

BACKUP GUIDING PRINCIPLES

6 **Offline Backup:** Because hackers often hunt for and delete backups before launching ransomware attacks, having an offline copy of backup data is important to ensure data recovery from a ransomware event. *"Offline"* means not accessible via a network connection or direct attached storage, and is also referred to as *"air-gapped."* Offline backups may leverage portable media like tapes or hard drives, so they must be handled with care due to the fragility of the devices. These backups should also be encrypted so data is not easily accessible if the media is lost or stolen.

While offline backups may be stored off-site, they are not a replacement for automated off-site backups (which are typically stored in the cloud). Offline and off-site backups serve two very different purposes: off-site backups are used to recover from an environmental disaster like a fire, whereas offline backups are used for recovery from ransomware.

7 **Complete and Comprehensive:** Backing up only some data while skipping other seemingly less-important data, is a short-term cost-saving strategy that leads to the mistaken assumption that all data is “safe.” We recommend a full backup of all data, including applications and system state.

8 **Aligned with RPO and RTO:** A backup is only useful if it can return you to a desired point in time (your Recovery Point Objective, or RPO) within a reasonable amount of time (your Recovery Time Objective, or RTO).

SUCCESS Computer Consulting can help you choose from a variety of technologies that align with these guiding principles.

SUCCESS COMPUTER CONSULTING
info@sccnet.com
763.593.3000