MONTRA SOLUTIONS

Back up Everything!

Ensure that your Data is Protected

CYBERSECURITY
is everyone's job.

Backup and Recovery Best Practices

Cybersecurity considerations

There are many risks to your data, including hardware failure, natural disasters, human error, theft, and attacks such as malware and ransomware. You might not be able to anticipate every data risk, but a strong backup and recovery plan will help you quickly return to operation.

This short guide to leading practices for data backup and recovery draws on the experience of the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

1 Implement a strong backup process

1. **Define your expectations and intent in a policy**

   A policy over backup and recovery communicates your expectations and the goals for protecting the government's data and assigns responsibility to ensure it happens. Are particular systems critical to your operations? If so, you might want to save multiple copies of your data in case access to your system and backup is prevented by a ransomware attack. If your data or systems were damaged, could you manually re-create all of your transactions? If not, you might want to make a backup very frequently.

2. Establish a strategy to communicate how you intend to implement the policy

   The backup strategy may be incorporated in the policy or your procedures, or may be a separate document. The strategy is generally the responsibility of management (CIO/CISO/IT manager) and contains guidance to implement the expectations and goals you set in your policy. The strategy can depend on multiple factors, including specific departmental backup needs.

   An effective backup strategy addresses:

   - Who is responsible for implementing, managing, maintaining, and verifying the system works as planned
   - What data or systems should be backed up
   - Where the backup should be located – onsite, offsite, or in the cloud
   - When and how often data or systems should be backed up. Data with no paper record must be backed up more frequently, while data that changes infrequently or is easily created can be backed up less frequently.
   - How the backup files will be protected. For example, is the backup physically protected, and do only authorized users have access?
   - How long the backup files will be kept. For critical backups, you might want an additional copy maintained offsite to protect the data in the event of a regional disaster or ransomware.

3. Establish a documented plan or procedures to ensure consistent implementation

   The backup procedures are the steps used by your IT staff to implement the backup strategy. Clearly documented steps identify the procedures to initiate, schedule, and validate each backup to ensure data has been saved. These procedures will also help you manage the process during employee absence or turnover.

   An effective backup procedure will include:

   - Backup schedules. The frequency of the backup will be defined based on your strategy. If you use an automated backup system, the schedule

may be established in the system itself. We still recommend documented procedures supporting this setup. They can be used to periodically validate the system settings and for recovery if the backup process fails.

- Tracking and monitoring. It's important to document when the backups occur. If you are using an automated backup system, a report might identify what information was backed up and when. Review of this report will help detect any failed backups.

- **Periodic verification that the backup can be** recovered. It isn't uncommon to think your backup is working well, only to find out it didn't run or cannot be recovered. A periodic test to recover the data will ensure your data will be ready when you need it. Performing routine inspections on backup equipment will also help identify issues before it's too late.

Here is a resource to consider:
Department of Homeland Security Cybersecurity and Infrastructure Security Agency Pros and cons of backup options for your data
Data Backup Option

Municipal Research and Services Center (MRSC)
Sample plans and policies available to local governments
Cyber Security Resources for State & Local Governments

National Cybersecurity Society
Guidance on developing a data backup policy
Data Backup Policy Template

2 Establish effective recovery plans

Now that your data is backed up safely, the next step is to ensure you can continue operations while you recover your data from your backup. The key to ensuring your government can rebound from a natural disaster or cyberattack is being able to quickly recover your most important data. There are two plans that address different aspects of ensuring speedy recovery of data and operations:

- A business continuity plan helps you continue all aspects of business operations during and immediately after a disaster. This can include plans for operating using manual records, establishing functionality to work remotely, defining alternate emergency office locations, and recovering data needed for critical operations during the disaster.

- A disaster recovery plan focuses on how a government responds and returns operations back to normal once the event has concluded, with a focus on information and technology. This can be included as part of a business continuity plan, or presented separately.

1. **Identify your most common significant** disaster risks

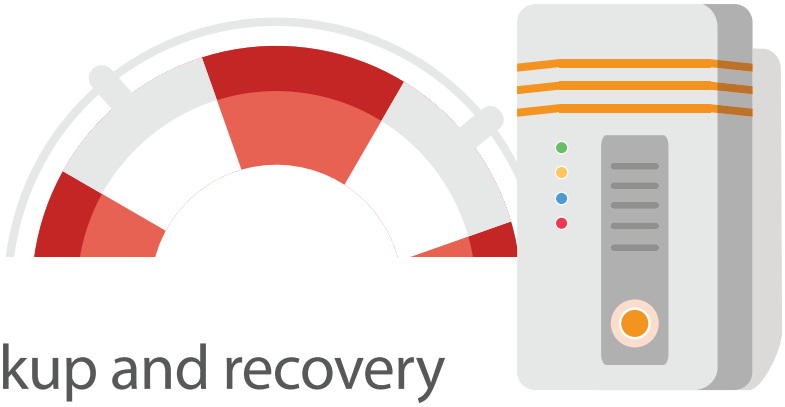
   Identify all the risks that can affect operations and carefully consider how they could affect your organization. Ransomware is a significant risk for most governments. In Western Washington, a major earthquake or flood is a significant risk. In Central and Eastern Washington, wildfires and floods can be significant risks.

2. Evaluate your backup and recovery plans **relative to your significant disaster risks**

   There is no one-size-fits-all plan. The process for recovery will vary depending on what happened and how you implemented your backups. Consider whether your backup solution(s) will support your recovery for the risks you identified.

   - Consider storage location. A backup stored locally on disks or tape is easy to quickly restore but could be destroyed by the same fire that destroyed your normal operations. A backup stored with a cloud provider or an external vendor might protect your backup from a regional event.
   - Consider where you will restore your backup. A regional event might destroy your normal operations center. Is there a secondary site that you can use?
   - Once business continuity and disaster recovery plans are established, periodic checks over the recoverability of the backed up data will help to ensure that information can be accessed when necessary.

Here are a few resources to consider:
Ready.gov
Purpose of an IT Disaster Recovery Plan and information related to data backup.
IT Disaster Recovery Plan



3 Maintain your backup and recovery best practices

1. Communicate and train employees on best practices

   Regular training on your backup practices, expectations and risks will help to ensure that data can be recovered in an emergency. This can address:

   - How employees schedule and initiate data backups and what they should do if the backup fails
   - How often and what data should be backed up
   - The importance of keeping backups and testing backup recovery on a routine basis

2. Annually review the backup, business continuity and disaster recovery plans

   As you add new systems or technology or eliminate old systems, your backup, business continuity and disaster recovery plans will need to change. An annual review will help you capture those changes in a timely fashion so you will be prepared when you need to use your backup.

You have an important role to play

As a leader, you help set the tone and cultural direction of your organization. By starting with these three steps, and ensuring the departments within your organization work together on these issues, you are on your way to improving your cybersecurity program.

Department of Homeland Security - Questions every CEO should ask about cyber risks:

https://www.us-cert.gov/ncas/tips/ST18-007

Sources:

Department of Homeland Security
National Institute of Standards and
Technology Center for Internet Security
Office of the Washington State Auditor