CYBERSECURITY
is everyone's job.

Leadership and Planning

Backup and Recovery Best Practices

Cybersecurity considerations for local government leadership

Every government faces many risks when it comes to their data, including hardware failure, natural disasters, human error, theft, and attacks such as malware and ransomware. While governments cannot anticipate every data risk, a strong backup and recovery plan will help them quickly return to operation.

Here are three things organizations can do to implement backup and recovery best practices to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

Updated June 2025

1 Implement a strong backup process

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

   The backup and recovery policy should communicate to employees and managers your expectations and the goals for protecting the government's data. In your policy, you can also assign responsibility to ensure this happens. As you update your policy, consider:

   - Do you have any systems critical to your operations? If so, you might want to save multiple copies of your data in case a cyberattack or failure prevents access to your system and backup.
   - What data should your staff back up? Know where sensitive or confidential information is stored. Knowing these locations can ensure the information is backed up and might alert the owner where information storage should be moved.
   - If an event caused damage to your data or systems, could you manually recreate all your transactions? If not, you might want to back these up more often.

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

   You may incorporate the backup strategy in your policy, or you can create a separate document on how management should implement the expectations and goals you set in your policy. The strategy can depend on multiple factors, including specific departmental backup needs. Usually, the Information Technology Manager, Chief Information Officer or Chief Information Security Officer is responsible for implementing such a strategy.

   An effective backup strategy should address:

   - Who is responsible for implementing, managing, maintaining and verifying the system works as planned?
   - Where do you plan to locate your backups – on-site, off-site or in the cloud? Consider the 3-2-1 rule of data protection, which is to maintain three copies of your data stored on two different types of media, including one copy stored off-site in case of a regional disaster or ransomware.
   - When and how often should your staff back up data or systems? (You should frequently back up data that has no paper record, whereas you might back data up less frequently when it does not often change or is easily created).
   - How will you protect the backup files? For example, do you physically protect the backup and limit access to only authorized users?
   - How long will you keep the backup files?

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

   Your information technology staff use backup procedures to implement the backup strategy. These staff follow clearly documented steps to initiate, schedule and validate each backup to ensure they save a copy of the data. Documented procedures help your employees, should absence or turnover occur.

An effective backup procedure will include:

- **Backup schedules.** Your strategy will define and determine the frequency of the backup. If you use an automated backup system, you might establish the schedule in the system itself. We still recommend documented procedures supporting this setup. That way, you can use them to periodically validate the system settings and for recovery if the backup process fails.
- **Tracking and monitoring.** Document when the backups occur. When using an automated backup system, you might review a report to verify the data and time the backups occurred. Review this report to detect any failed backups.

Here are resources to consider:

Department of Homeland Security Cybersecurity and Infrastructure Security Agency – Pros and cons of backup options for your data (PDF)

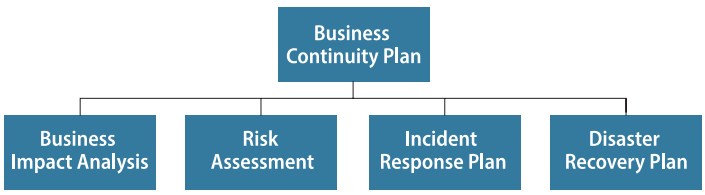
Municipal Research and Services Center (MRSC) – Cybersecurity Resources for Local Governments

National Cybersecurity Society Guidance on developing a data backup policy – Data Backup Policy Template (PDF)

Office of the Washington State Auditor Guidance on developing IT policies – A guide to jump-starting your cybersecurity program (PDF)

2 Establish effective recovery plans

Now that you have backed up your data, the next step is to ensure you can continue operations while recovering the backed-up data. The continuity plan could include workarounds that are necessary until the system is recovered. Your ability to quickly recover your most important data is key to ensuring your government can rebound from a natural disaster or cyberattack. You should consider the following two areas that address different aspects of ensuring speedy recovery of data and operations:



- **Business continuity** 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.
- **Disaster recovery** focuses on what order departments and applications return back to normal operations once the event concludes, with a focus on information and technology.

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

   Identify all risks that might affect your operations and carefully consider how they could affect your organization. Ransomware is a significant risk for most governments. Local governments in western Washington might face earthquake or flooding risks. Local governments in central and eastern Washington might face wildfire and flooding 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 your recovery site location

Some events such as flooding or fires could require evacuation of your normal operation center and you may need a secondary location to temporarily host the operation center. The secondary location will need a power source, network connectivity and air conditioning for cooling. The secondary site could be another building that your government owns but is far enough away to offer some resiliency in hosting the operation center. Your government may need an agreement with another government allowing you to temporarily use part of their datacenter during an emergency.

Test recoverability

Once business continuity and disaster recovery plans are established, regularly check the recoverability of the backup data files to ensure you can access information when necessary. Government officials might assume their backup was successful, only to later discover it did not run or that they cannot actually recover the data from the backup file. You should also regularly inspect backup equipment to identify potential issues early.

Consider storage location

You may find it convenient to store backups locally on disks, but you might not have access to those disks if a local fire destroys them. If you store your backups using a cloud provider or an external vendor, then you can better protect your backup during a regional event.

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

Washington State Office of the Chief Information Officer – IT Disaster Recovery and Business Resumption Planning Guidelines (PDF)

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 you can recover your data 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 which data employees should back up
   - The importance of keeping backups and testing backup recovery routinely

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. You should perform an annual review so that you can capture those changes in a timely fashion and prepare for using your backup.

Here are resources to consider:

National Institute of Standards and Technology In-depth guide for backup and recovery plans, policies, and strategies – Contingency Planning Guide for Federal Information Systems (Publication 800-34r1)

Department of Homeland Security – Questions Every CEO Should Ask About Cyber Risks

For assistance

This resource was developed by the Center for Government Innovation at the Office of the Washington State Auditor. Please send questions, comments, or suggestions to Center@sao.wa.gov.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.

To learn more, visit

sao.wa.gov/BeCyberSmart

Sources:

Department of Homeland Security
National Institute of Standards and Technology
Center for Internet Security

Center for Government Innovation