CYBERSECURITY
is everyone's job.

Leadership and Planning

It starts with policy

A guide to jump-starting your cybersecurity program

The Office of the Washington State Auditor launched the Cyber Checkup program in 2023, and one of the common results we have found is that local governments lack or need to improve their information technology (IT) documentation, including standards, procedures and most importantly, policies.

Here are what different groups need from your IT policies to #BeCyberSmart.

CYBER SECURITY

Office of the Washington State Auditor
Pat McCarthy

September 2024

IT policies are the foundation of any strong cybersecurity program. They help ensure your government implements procedures consistently, even amidst employee turnover. IT policies set expectations, rules and requirements for local government employees and vendors when it comes to using, managing and securing IT resources and data. Without these policies, key users such as employees, contractors, managed service providers, vendors and other third parties do not have clear expectations and guidelines. The lack of policies may lead to an oversight that leaves local governments at a higher risk of security breaches, data loss, and other IT-related incidents that could harm their organizations and the people they serve.

IT policies alone do not eliminate vulnerabilities, but they help establish the expectation in local government that cybersecurity is everyone's responsibility. Effective IT policies should be comprehensive, well-documented, and align with a government's goals, legal and regulatory requirements, and best practices. Additionally, government leaders should review and update these policies regularly, and communicate them often to employees and any vendors or contractors who use the organization's IT resources.

Creating effective IT policies can be a daunting task for local government leaders, especially since employees and vendors need different information from them. That is why we prepared this guide – to help leaders understand what their government's policies should cover for internal and external users. We also included a list of recommended policies and links to resources to help you create them.

Policy needs and responsibilities by role

1 Leadership

As part of their duties, local government leaders are responsible for ensuring compliance with regulatory requirements, setting cybersecurity expectations and responsibilities in their organizations, and establishing and allocating resources to achieve business goals. Government leaders may delegate policy-drafting responsibilities to someone else inside or outside the organization, but the governing body is ultimately responsible for approving them. As local government leaders develop their IT policies, they must understand how the policies should help them fulfill their obligations when it comes to data protection and privacy, resource management, compliance and security measures. Leaders should ensure their government's policies cover the following:

Data protection and privacy: IT policies should help your government safeguard employee and customer data, as well as ensure compliance with data protection regulations. They specify guidelines for handling, storing and sharing sensitive information including personal data. These policies help leaders ensure their governments can minimize data leaks, unauthorized disclosures, and data breaches, reducing the risk of legal and reputational consequences.

Resource management: IT policies should establish expectations for the appropriate use of government IT resources, including hardware, software and network resources. These policies define acceptable and prohibited activities for employees, such as downloading unauthorized software, accessing inappropriate websites or excessive personal use of government resources. Leaders should ensure policies promote efficient use of their government's IT resources and help maintain network performance and availability for critical business operations.

Compliance: Leaders should be confident their IT policies will help them ensure compliance with various contracts, data-sharing agreements, and legal and regulatory requirements relevant to their local government. The policies should address specific regulations, such as the Health Insurance Portability and Accountability Act for human resource departments, fire departments or health care organizations. Ensuring that IT policies adhere to applicable requirements – and that employees comply with them – can help local governments avoid penalties, fines and legal liabilities.

Leaders should review the policies at least annually to see if they need to update them to meet any changes in laws or regulations.

Enhanced security measures: IT policies often include security protocols and best practices to protect a local government's systems, networks and data. Local government leaders can use these policies to develop comprehensive security strategies and put in place robust controls and safeguards. When local government leaders ensure employees are aware of and follow these policies, they can help reduce vulnerabilities, mitigate risks, and maintain a secure IT environment.

2 Employees

The IT policies that local government leaders enact must define the responsibilities of each employee and department, outline the acceptable use of IT resources, and specify the consequences for policy violations. These policies should ensure employees know how to use and manage the government's IT infrastructure, applications and data consistently and securely. Here is what local government employees need from their organization's policies:

Security: IT policies should help employees understand their role in protecting sensitive information and data from unauthorized access. These policies outline security measures for employees, such as password expectations, data encryption procedures, network security protocols, and guidelines for using government-issued devices. By understanding and adhering to these policies, local government employees help maintain a secure IT environment.

Productivity and efficiency: IT policies can address issues that affect employee productivity and efficiency. They may include guidelines for software installation requirements and remote work practices, as well as how employees should use email, internet and social media. By providing clear expectations and boundaries, these policies help employees understand what is acceptable and minimize distractions or misuse of technology during work hours.

Change management: IT policies should include the local government's guidelines for managing changes to IT systems, applications or infrastructure, including how or when to communicate changes to employees. This ensures that any modifications or updates are properly planned, tested and implemented, minimizing the risk of disruptions or downtime for the local government's business operations.

Incident response and reporting: IT policies should define a local government's procedures for reporting and responding to IT incidents, including security breaches, data loss or system failures. These policies should identify whom employees should report suspicious computer activity to, who can verify and declare an emergency, and who will be the primary and backup incident command to coordinate a response to a cyberattack. With these policies, local governments can ensure their employees know the steps to take in case of an incident, facilitating a timely and coordinated response to mitigate potential damage or loss.

Streamlined processes: IT policies establish the local government's guidelines for processes such as system access, user privileges, software installations and change management. These policies can streamline the processes and ensure the local government complies with any required standards. This alignment promotes consistency, efficiency, and smoother collaboration between the local government's IT staff and service providers.

Training: Local governments should incorporate a policy review as part of their ongoing IT awareness training for employees and management. Leaders should review the policies at least annually to see if they need to update them. Additionally, requiring staff to review the IT policies at least annually reinforces the government's commitment to cybersecurity, reminds employees what the policies cover, and informs them of any changes.

3 Managed service providers

The IT policies that local government leaders adopt should also address the needs of their managed service providers. Written IT policies serve as guidelines for a government's service-level agreements and contracts with its providers; they are a foundation for the providers' operations and help build trust and confidence. When providers understand and follow their local government clients' policies, they can reduce vulnerabilities, mitigate risks and maintain a secure IT environment for their clients.

At a minimum, these policies should identify your government's security requirements, reporting requirements, and expectations for responding to cyberattacks. Documenting this information in written policies and communicating it to service providers helps local government leaders ensure the partnerships are well understood. Here is what service providers need from their local government clients' policies:

Consistency: IT policies provide a framework for consistent service delivery across different clients and environments. Service providers often work with multiple organizations, each with its own IT requirements and objectives. When governments establish IT policies that specify their standards, this can ensure service providers deliver their services consistently and in accordance with the government's goals.

Security and compliance: Service providers handle sensitive client data and have access to the client's IT infrastructure. IT policies should help governments establish security measures and protocols to protect their data from unauthorized access, breaches and cyber threats. These policies set the government's expectations, which help service providers understand the requirements and maintain their client's trust and confidence.

Service-level agreement compliance: Providers typically work under agreements that define the level of service they provide to their clients. Local government IT policies should outline the processes, procedures, and standards that providers must follow to meet the agreement's requirements. These policies help providers deliver services effectively, meet agreed-upon service levels, and maintain client satisfaction.

Efficient incident response and disaster recovery: Policies should define the procedures and protocols for responding to IT incidents and managing disaster recovery situations. Service providers need to have clear guidelines to address potential disruptions, minimize downtime, and restore services as quickly as possible. Providers can also integrate these policies into their own incident management frameworks, allowing them to respond promptly and effectively to any of their clients' IT-related issues.

Documentation and reporting: IT policies for service providers should emphasize the importance of maintaining accurate documentation of client systems, configurations and procedures. These policies ensure that providers have a comprehensive understanding of client environments, allowing them to provide effective support and troubleshooting. Documentation and reporting policies also facilitate transparent communication, allowing clients to stay informed about the status and performance of their IT systems.

Vendor management: Providers often work with various technology vendors to deliver services and support to their clients. Local government IT policies should help establish guidelines for vendor selection, management and integration. These policies must ensure that providers maintain proper relationships with vendors, evaluate their performance, and leverage their solutions effectively to meet client requirements.

Change management: IT policies for service providers should include the local government's guidelines for managing changes to client systems, applications or infrastructure. This ensures any modifications or updates are properly planned, tested and implemented, minimizing the risk of disruptions or downtime for the local government's business operations. Change management policies help providers maintain stability and reliability while introducing necessary changes to client environments.

Streamlined processes: IT policies establish the local government's guidelines for processes such as system access, user privileges, software installations and change management. Service providers can use these policies to streamline their service delivery processes and ensure compliance with the government's standards. This alignment promotes consistency, efficiency, and smoother collaboration between the government's IT staff and service provider.

Clear guidelines and expectations: IT policies outline a local government's rules and regulations for technology usage, security practices, data handling and more. When local governments have these policies in place, service providers can work within a framework that defines the government's expectations and requirements. This clarity helps providers deliver services more effectively and ensures they align with the government's goals and compliance needs.

Improved communication and collaboration: IT policies should promote clear communication and collaboration between the local government and its service provider. The policies define roles, responsibilities and expectations, ensuring that both parties have a mutual understanding of their respective obligations. This alignment fosters effective communication channels, facilitates efficient decision-making, and enhances the overall partnership between the local government and its service provider.

4 Vendors and other third parties

Written IT policies can also help other external users and organizations – such as vendors who provide cloud-based software – deliver high-quality services while adhering to a local government's guidelines and expectations. When local governments have documented IT policies, vendors and other third parties will understand any regulatory compliance requirements that they must meet, benefit from enhanced communication and collaboration, and help facilitate an efficient response to cyber incidents. Here is what other vendors and third parties need from their local government clients' policies:

Regulatory compliance: Governments that work in regulated industries must comply with specific laws and regulations. Local government IT policies can address compliance requirements related to data privacy, industry-specific regulations, and other legal obligations. Other vendors and organizations except managed service providers can use these policies as a guide to ensure their services and solutions meet the necessary compliance standards applicable to their local government clients. This helps the government adhere to regulations and avoid potential penalties or legal complications.

Improved communication and collaboration: IT policies promote clear communication and collaboration between local governments and their vendors. If local governments require external resources to respond to a cyberattack, they can list contact information along with contract numbers and service-level agreements in their IT policies. These policies also allow local governments to show their vendors what steps they took to secure their IT infrastructure.

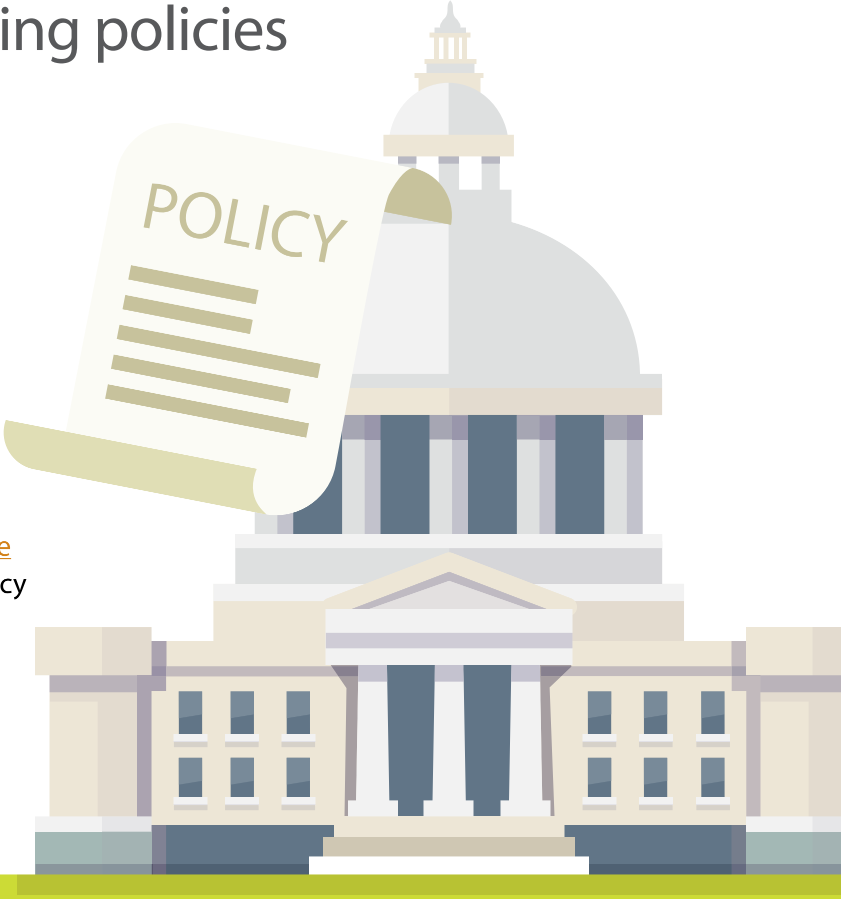
Efficient incident response and disaster recovery: IT policies often outline procedures for incident response and disaster recovery. If a local government uses a vendor to help it respond to and recover from a cyberattack, the government can use the policies to explain how it has handled the incident so far, allowing the vendor to respond promptly and effectively to any IT-related issues. This alignment facilitates better coordination between the vendor and the government during critical situations, minimizing downtime and optimizing recovery efforts.

5 Recommended policies

Depending on its size and available resources, a local government may have a series of IT policies. But the reality is, many organizations struggle to have any written IT policies. To start, the Office of the Washington State Auditor recommends that local government IT policy address seven areas that create a solid foundation for a cybersecurity program. By adopting policies that cover these seven areas, local governments can reduce their risk, improve efficiency and protect their assets. The following areas can be captured in either in a single policy or separate policies:

- **Acceptable use.** Set rules for what the local government considers appropriate employee use of official information and technology. Policy should also define inappropriate use and the risk it may cause.
- **Passwords.** Describe the requirements for a password, such as length and complexity. Policy should identify how often employees must change their passwords, restrictions on reusing passwords, and prohibited passwords.
- **Use of multifactor authentication (MFA).** Identify the circumstances and specific accounts (such as IT administrators versus all employees) that must use MFA.
- **Incident response.** An incident response policy should not be confused with an incident response plan. The incident response policy identifies to whom employees should report a suspected cyberattack or suspicious cyber incident, who can declare a cyber incident, who is in charge, and anyone else who should be notified. All employees should have access to the policy.
- **Email.** Describe the appropriate use of government-issued email accounts for employees, as well as address the use of personal, third-party email such as Gmail.
- **Personal device use.** Explain whether employees can use their personal devices on the government's network. If employees are allowed to use their personal devices, policy should address under what circumstances they are allowed to connect to the network, such as times of day, what network can they access and outdated operating systems restrictions.
- **Social media accounts.** If your government uses social media, such as Facebook, X or Instagram, policy should describe acceptable use for social networking, including who can access social media and post to your government's accounts. Many governments also stipulate what employees are restricted from posting on their personal social media, such as confidential information they have obtained through their employment. Policy should caution employees about making statements on social media that take a position on an issue that may be detrimental to the local government and encourage them to clarify the statements are their own opinions and not the government's.

6 Resources for creating policies



Local governments have several resources available to help them avoid reinventing the wheel when writing and adopting their own IT policies. First, managed service providers might give their local government clients IT policies they can adopt and implement. Second, local governments might consider asking other credible agencies for permission to copy and adopt their IT policies. Third, several businesses and organizations offer free IT policy templates online that local governments can download. Both the SANS Institute and the Center for Internet Security have free IT policy templates that are in Microsoft Word format and written in plain language.

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 or legal advice and might not include all information that management should consider when drafting IT policies. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.

Now offering

FREE

cyber checkups

for local governments

Learn more at

sao.wa.gov/BeCyberSmart

Center for Government
Innovation