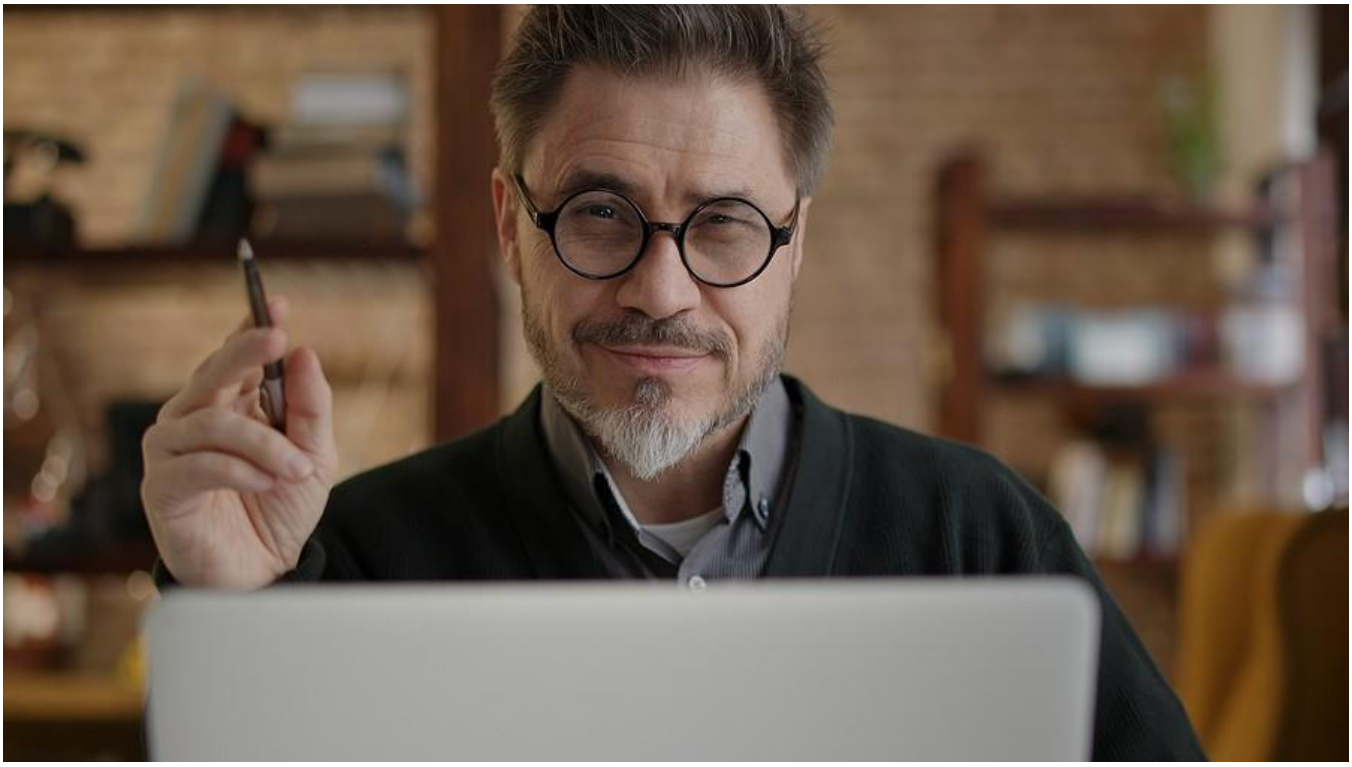
4 Best Practices for Secure Collaboration in Municipalities



Like many other industries in recent years, the public sector has witnessed a rise in hybrid work. With team members working in multiple offices, including remotely, government agencies must take a closer look at tools, policies, and processes. The following best practices for secure collaboration in municipalities will help you find the balance between productivity and security.

Challenges to Secure Collaboration in Municipalities

As employees collaborate with others both inside the agency and externally, government agencies encounter several key challenges. The rise of cloud computing has made collaborating across distance vastly easier. However, at the same time, doing so securely and in compliance with regulations requires careful planning.

For instance, employees can easily share sensitive information through email, thus putting the agency and its customers at risk. Virtual meetings, now a staple of work life, create another security risk. And with thousands of employees accessing files and programs remotely, access management proves complicated.

1. Enact Secure Sharing Policies and Tools

Government agencies work with large quantities of sensitive information, from utility customer financial data to employee information and court records. At the same time, they must adhere to numerous privacy and security regulations, such as HIPAA and other local laws.

Without proper controls, employees create risk by unintentionally sharing protected information. On the other hand, by implementing ePolicies and configuring tools wisely, agencies reduce the chance of inappropriate sharing. For instance, in SharePoint, administrators can adjust various sharing settings at both the folder and file level.

For example, they can specify whether content of a particular site can be shared only internally, or also with external guests. Additionally, sensitivity labels allow the agency to automatically restrict sharing at the file level.

2. Ensure Security of Virtual Meetings

Microsoft Teams, Zoom and other virtual meeting apps have revolutionized meetings, allowing attendees from multiple locations with ease. However, meeting organizers need to take certain steps to protect against intrusion.

- Control meeting attendance – Use protection features such as passwords and waiting rooms to ensure that only authorized attendees can join the meeting. Some meeting apps also allow organizers to disable the ability to forward a meeting invitation.
- Know who has joined the meeting – As an extra layer of protection, consider enabling entry and exit tones. This provides an alert when anyone joins or leaves the meeting.
- Restrict screen sharing – Make sure that only the meeting organizer or someone with the organizer's explicit permission can share their screens.

- Retain control over meeting recording – Ensure that only the meeting organizer can record the meeting. Once the meeting has been recorded, adjust permissions to determine which users (if any) can access and transcribe the recording.

3. Implement Authentication and Access Management Best Practices

With increased risk of cyber-attack, and with users accessing agency resources from a multitude of devices, authentication and access management take center stage. Agencies must find a balance between providing employees the access they need while protecting the agency and its digital assets.

Best practices include moving beyond basic username and password to implementing modern authentication methods such as multi-factor authentication (MFA). In addition, for agencies with large numbers of employees, simplify access management where possible. For instance, Microsoft 365 allows administrators to define access at the group level.

4. Establish Proactive Data Governance Strategy

Tools such as Microsoft Teams power collaboration, making it easy to co-author documents, conduct meetings and communicate in a variety of ways. However, agencies need to consider their approach to data governance before implementing these tools. Without a data governance strategy, information and access can quickly spiral out of control, compromising security.

For instance, before creating teams and groups, determine who can create groups and what naming conventions they will use. Carefully define policies for records management, including data retention. Know where agency data lives, who owns it and who can access it. Strategic data governance will improve both data security and regulatory compliance.

Implement Secure Collaboration in Municipalities

Begin now to improve data security with the help of the data governance and security experts at Messaging Architects. Our consultants provide security and compliance assessments, review ePolicies and help your agency implement a data governance strategy. We help to improve secure collaboration in municipalities while finding that sweet spot between control and flexibility.