ISSUE/TECHNICAL PAPER SUMMARY

DECEMBER 2025

CYBERSECURITY FOR MUNICIPAL GOVERNMENTS: MANAGING RISK ACROSS CRITICAL SERVICES

ISSUE PAPER OVERVIEW

Cyberattacks are now a routine threat to towns and villages of every size, affecting public services, financial systems, and sensitive community data. Even small municipalities are targeted because attackers look for easy entry points not the biggest government entity. With a few practical steps, local governments can greatly reduce their risk and protect the continuity of essential services.

SCAN TO READ THE FULL PAPER

Cybersecurity Awareness

Train Your Staff

Establish clear security practices for all employees, including requirements for strong passwords and responsible internet use. Regularly brief staff on common threats, and provide frequent reminders and short trainings to help maintain a strong security culture.

Use Strong, Unique Passwords

Passwords should be long, random, and include various character types to reduce the risk of compromise. If those are hard to remember try using a phrase or sentence that combines all of those character types. Require employees to use different passwords for each municipal system or account.

Enable Multi-Factor Authentication

Require multi-factor authentication to access areas of your network with sensitive information such as email, financial software, or clerk systems. This requires additional steps beyond logging in with a password, like a temporary code on a smartphone or a computer key.

Keep Software Up to Date

Keeping your software up to date provides critical security patches to protect against cyber threats, fixes bugs that can cause performance issues, improves efficiency, and adds new features to enhance functionality. Enable automatic updates whenever possible.

Secure Your Wi-Fi Network

Change the default network names and passwords on all municipal routers and disable remote management features that can be abused. Ensure encryption is enabled to protect information transmitted over the network. Regularly review network settings to confirm unauthorized devices are not connected.

ISSUE PAPER SUMMARY
DECEMBER 2025

CYBERSECURITY FOR MUNICIPAL GOVERNMENTS: MANAGING RISK ACROSS CRITICAL SERVICES

CYBERSECURITY REPORTING

A Simple Guide to Cybersecurity Reporting and Incident Management for Municipalities

1. DETECT THE EVENT

Recognize any unusual activity on municipal computers, networks, or accounts. A cyber security incident becomes reportable when it actually or imminently jeopardizes the confidentiality or integrity of computers and/or networks.

2. ASSESS THE INCIDENT

Determine the scope and severity:

- What systems or data are effected?
- Is the incident contained?
- Does it disrupt, degrade, or threaten municipal services?

3. REPORT TO NYS

NYS reporting rules:

Report within 72 hours:

- Any cybersecurity incident **within 72 hours**.
- Any ransomware event.

Report within 24 hours

- Any ransom payment.

Submit within 30 days

- Written justification if ransom was paid.

4. RECOVER & RESTORE

Restore critical services first such as water, 911 dispatch, and payroll systems, in order of priority. Clean and restore affected devices. Secure all accounts by resetting passwords and strengthening access controls.

How to report a cyber incident:
Call DHSES: 1-844-628-2478
Email: cyber.reporting@dhses.ny.gov
Website: www.dhses.ny.gov/cybersecurity-incident-and-ransom-payment-reporting