Meeting Federal Grant Requirements for Cybersecurity Internal Controls

Current as of: 2/23/2026

The federal government has strengthened cybersecurity expectations for all recipients of federal financial assistance. As of October 1, 2024, municipalities must include cybersecurity as part of their internal control systems. This change reflects the growing risk that cyberattacks pose to public services, financial systems, and sensitive community data.

Why This Matters

Cyberattacks, especially phishing and ransomware, are increasingly targeting small towns. The updated federal rules recognize this risk and require municipalities to take reasonable steps to safeguard financial systems, grant records, and sensitive data.

Controls Municipality Can Use

Even with limited staff and tight budgets, there are practical steps every municipality can take to meet this requirement and protect its systems. The controls listed below are examples of reasonable controls a municipality could use. They are not intended to be one-size-fits-all or a compliance checklist.

Starter Steps

These low cost, low staff-time actions offer strong protection and are easy to implement.

- **Strong Passwords -** Use long, unique passwords. Encourage password managers.

- **Multi Factor Authentication (MFA) -** Turn on MFA for email, financial systems, and grant-related accounts.
- **Basic Cybersecurity Training -** Teach staff and elected officials how to spot phishing emails. Free training resources are widely available.
- **Limit System Access -** Give access only to people who need it. Remove access immediately when roles change.
- **Automatic Software Updates -** Enable automatic updates on all municipal computers and devices.

Moderate Effort Controls

These steps may require some planning or help from an IT provider.

- **Regular Data Backups -** Back up financial systems and grant files. Keep at least one backup offline or in secure cloud storage.
- **Antivirus and Firewall Protection -** Ensure devices have up-to-date security tools. Many are low-cost or included in existing IT contracts.
- **Written Cybersecurity Policies -** Create simple policies for passwords, acceptable use, remote access, and data handling.

Higher Effort or Higher Cost Controls

These tools can be phased in over time.

- **System Monitoring -** Track login attempts and unusual activity. May require IT support.
- **Vendor and Third Party Oversight -** Review IT vendor contracts to ensure they follow strong cybersecurity practices.
- **Incident Response Plan -** Create a plan for responding to a cyberattack. Conduct a simple annual tabletop exercise.

Bottom Line

You don't need a large IT department to meet the new federal requirement. Start with the low-cost steps, build gradually, and use partners for support. For example, PACIF offers grants for IT consultation services for cybersecurity risk assessments. Strong cybersecurity protects your municipality, your data, and your ability to receive federal funding.

VLCT Resources

- Cybersecurity Handouts for Employees
- Remote Work Cybersecurity
- Why & How To Protect Against Ransomware
- Technology Assessments - Learn About Your Systems
- Resources for Finding and Selecting IT Services

This document was created in part with artificial intelligence and was reviewed by a human subject matter expert.

Publication Date

02/02/2026