CATALIS

Cybersecurity Checklist for State & Local Government

Help every department, from IT to administration, reduce risk and respond faster when threats happen.

Cyber attacks on state and local governments are rising, often exploiting small teams and outdated systems. Most breaches start with something simple, like a missed update, a weak password, or a phishing email. Strong security doesn't require major budgets; it starts with awareness, coordination, and steady habits. This checklist highlights practical steps anyone can take to protect data and keep services running.

Strengthen Access and Authentication

- ☑ Turn on Multi-Factor Authentication (MFA) everywhere: email, payroll, accounting, and social media.
- ☑ Require strong, unique passwords (and use password managers).
- ☑ Limit admin privileges. Only give "keys to the castle" to those who truly need them.

Keep Systems Updated

- ☑ Confirm that automatic updates are enabled for all desktops, laptops, and mobile devices.
- ☑ Patch servers and applications promptly. Attackers can exploit known flaws within five days, while many organizations take more than 100 days to patch.
- ☑ If you rely on outside IT support, ask how quickly they install security updates.

Train Everyone, Often

- ☑ Run phishing simulations and short awareness refreshers at least once per quarter.
- ☑ Remind staff to never click unexpected links or share credentials. When in doubt, call the sender directly.
- ☑ Encourage a "report it, don't hide it" culture. Mistakes happen, but early reporting limits potential damage.

Cybersecurity Checklist (cont.)

Review Vendors and Third Parties

- ☑ Vet vendors before granting network access, especially remote contractors.
- ☑ Ask every vendor:
  - How fast do you patch vulnerabilities?
  - Do you use MFA for your staff?
  - How do you verify your remote workers' identities?
- ☑ Document every individual who has access to your systems and data.

Prepare for Incidents

- ☑ Have a written incident response plan. Even one page is better than none.
- ☑ Include IT, legal, communications, and leadership contacts.
- ☑ Practice a tabletop exercise at least once a year. The U.S. Cybersecurity and Infrastructure Security Agency offers free tools to help facilitate this.
- ☑ **If you suspect a Business Email Compromise (BEC), contact your bank and the FBI Internet Crime Complaint Center (FBI IC3) within 48–72 hours for the best chance of recovering any lost funds or compromised data.**

Use Trusted Federal Resources

- ☑ **CISA** (Cybersecurity and Infrastructure Security Agency): free tools, assessments, and training. https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages
- ☑ **NIST** (National Institute of Standards and Technology) Cybersecurity Framework: self-assessment and maturity model. https://www.nist.gov/cyberframework
- ☑ **FBI IC3** (Internet Crime Complaint Center): to report cybercrime. https://www.ic3.gov

Bottom Line

Cybersecurity is not just an IT issue. Leadership, finance, operations, and staff all play an important role. Following these guidelines will help ensure that every person in your organization is a defense layer, not a liability.

Catalis helps government agencies modernize securely, with cloud-based solutions built for compliance, data protection, and reliability. Our platforms make cybersecurity stronger by design, so your team can focus on serving citizens, not fighting threats.

Contact us today to learn more about how Catalis solutions can strengthen your agency's security posture.