Cybersecurity Compliance Checklist for State & Local Governments

Protect Infrastructure, Safeguard Public Trust, and Ensure Operational Continuity

#	Activities	✓
1	**Regulatory Compliance** • Adopt NIST Cybersecurity Framework • Meet DoD 8140 requirements andensure IT staff have required certifications • Comply with state-specific regulations • Conduct regular compliance audits	
2	**Cybersecurity Roadmap** • Define short and long-term goals • Perform regular risk assessments • Develop an incident response plan • Implement continuous monitoringusing tools like SIEM	
3	**Workforce Training & Certification** • Train staff with updated cybersecurity skills • Certify your team with CompTIA Security+ and CySA+ • Foster a culture of cybersecurity awareness for all employees	
4	**Cybersecurity Best Practices** • Implement multi-factor authentication (MFA) • Encrypt sensitive data • Regularly update software and systems • Adopt a zero trust architecture • Back up data regularly	
5	**Incident Response & Recovery** • Test your incident response plan • Establish a communication plan • Partner with law enforcement • Review and improve post-incident	
6	**Technology & Tools** • Deploy endpoint detection and response(EDR) tools • Use firewalls and intrusion detection systems (IDS) • Implement data loss prevention solutions • Adopt cloud security soutions • Monitor third-party vendors	
7	**Continuous Improvement** • Stay informed on emerging threats • Review policies annually • Invest in cybersecurity innovation - allocate budget for new tool and training • Benchmark against industry standards	