HB 96 Compliance Checklist

Ohio House Bill 96 (ORC 9.64) - Cybersecurity Requirements for Public Entities

DEADLINE ALERT

Counties and Cities: Compliance deadline has passed. | All other public entities: July 1, 2026.

1. Adopt a Formal Cybersecurity Program

□ Select a recognized framework (NIST CSF or CIS Controls)

□ Document your cybersecurity program in writing

□ Include policies covering:
- Access control and identity management
- Data protection and encryption
- Network security and monitoring
- Vulnerability management and patching
- Acceptable use and remote access

□ Formally adopt the program via resolution or ordinance

□ Assign a cybersecurity program lead or coordinator

2. Conduct Risk Assessment

□ Identify critical systems, data, and assets

□ Assess current vulnerabilities and threats

□ Prioritize risks by likelihood and impact

□ Document findings and remediation plan

□ Schedule recurring assessments (at least annually)

3. Establish Incident Reporting Procedures

□ Define what constitutes a cybersecurity incident

□ Create incident response plan with roles and escalation

□ Report incidents to OCIC within 7 days of discovery

□ Report incidents to Auditor of State within 30 days

□ Document all incident details, actions taken, and outcomes

4. Ransomware Decision Process

□ Establish a ransomware response policy before an incident

□ Document the legislative path for ransomware payment decisions

□ Ensure any ransomware payment requires a public resolution or ordinance

□ Include legal counsel and leadership in decision framework

5. Staff Training & Awareness

□

Implement cybersecurity awareness training for all staff

□ Provide role-based training for IT and security personnel

□ Track training completion with dates and records

□ Conduct phishing simulations (recommended quarterly)

□ Document all training activities for audit evidence

6. Audit Evidence & Documentation

□ Compile an evidence binder with:

- Adopted cybersecurity program document
- Risk assessment reports
- Policy documents with adoption dates
- Training records with completion dates
- Incident reports and response logs
- Monitoring and testing evidence

□ Note: Cybersecurity program and incident records are EXEMPT from public records (ORC 9.64)

NEED HELP GETTING COMPLIANT?
Great Lakes Computer offers HB 96 readiness assessments, program development, and ongoing managed security services. Call (800) 966-4522 or visit greatlakescomputer.com/hb-96-compliance