OPLIN

OHIO PUBLIC LIBRARY INFORMATION NETWORK

Security Planning from Scratch

ORC 9.64 for Public Libraries

Jessica D. Dooley

Technology Project Manager

Ohio Public Library Information Network Mission:

Ensure equity of access to digital information for all residents of Ohio *(ORC 3375.64)*.

OPLIN Staff

Don Yarman
Executive Director

Laura Solomon
Library Services Manager

Christine Morris
Digital Services Manager

Jessica Dooley
Technology Project Manager

Derek Zoladz
Software Developer

Vincent Riley
Network Support

Security Planning from Scratch

- Reviewing ORC 9.64: Defining cybersecurity terms
- Cybersecurity frameworks
- Starting a cybersecurity program from scratch
- How-to guides and resources
- Meeting the requirements of ORC 9.64 at a small organization with limited resources
- Reporting compliance guidance from Auditor of State and Ohio Homeland Security
- Free resources available to public libraries

- Reviewing ORC 9.64: Defining security terms

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

In summary:

A. Defines ‘cybersecurity incident,’ ‘political subdivision’ and ‘ransomware incident’

B. Places restrictions on political subdivisions paying or complying with ransom demands

C. Requires political subdivisions to adopt a cybersecurity program consistent with standards of best practice

D. Creates mandatory reporting requirements for cybersecurity incidents

E. Exempts cybersecurity plans and incidents from public records requirements

F. Exempts cybersecurity procurement records from public records requirements

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Adopt a cybersecurity program consistent with recognized standards of best practice:

(C) The legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program shall be consistent with generally accepted best practices for cybersecurity, such as the national institute of standards and technology cybersecurity framework, and the center for internet security cybersecurity best practices, and may include, but are not limited to, the following:

(1) Identify and address the critical functions and cybersecurity risks of the political subdivision.
(2) Identify the potential impacts of a cybersecurity breach.
(3) Specify mechanisms to detect potential threats and cybersecurity events.
(4) Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.
(5) Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.
(6) Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. Annual cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program of the Ohio cyber range institute, satisfy the requirements of this division.

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

Security Planning from Scratch

What is a cybersecurity program?

More than a policy, a cybersecurity program is a combination of a policy, an action plan, and a commitment to regularly assess your security controls and information assets, and revise your action plan and policy to best protect your organization's evolving needs.

A cybersecurity program combines

- policy
- action plan
- commitment to continuous improvement
- review, revise, repeat over time

A cybersecurity program addresses all business assets

Your cybersecurity program must cover more than just your technology resources.
It also must address all business critical information, assets, and processes.

CIA Triad

An information security model that guides strategy and policy.

CIA triad © NIST

Confidentiality: asset should only be available to those authorized.

Integrity: asset should be protected from unauthorized modification.

Availability: asset should be available to those authorized when needed.

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Defines cybersecurity incidents, which includes incidents affecting library data hosted by third-party providers:

(A.1) "Cybersecurity incident" means any of the following:

a. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
b. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
c. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
d. Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:
    i. A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
    ii. A supply chain compromise.

"Cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

- Cybersecurity Frameworks

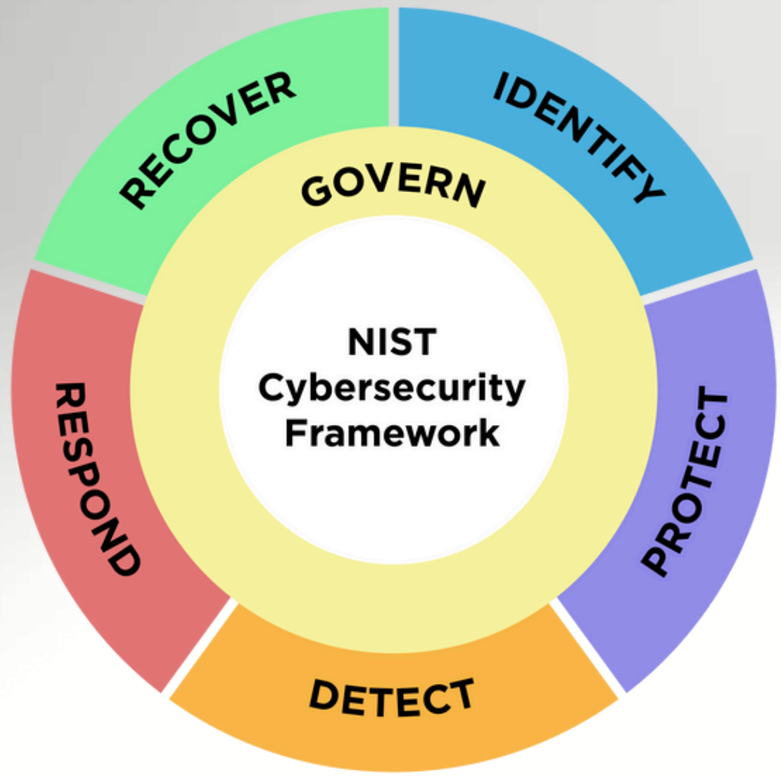
Security Planning from Scratch

Consistent with standards of best practice for cybersecurity, such as:

- National Institute of Standards and Technology Cybersecurity Framework 2.0 (**NIST CSF 2.0**)
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- Center for Internet Security 18 Critical Security Controls (**CIS Controls**)
  https://www.cisecurity.org/controls/cis-controls-list

NIST Cybersecurity Framework 2.0



NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

CIS 18 Critical Security Controls

https://www.cisecurity.org/controls/cis-controls-list

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Adopt a cybersecurity program consistent with recognized standards of best practice:

(C) The legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program shall be consistent with generally accepted best practices for cybersecurity, such as the national institute of standards and technology cybersecurity framework, and the center for internet security cybersecurity best practices, and may include, but are not limited to, the following:

(1) Identify and address the critical functions and cybersecurity risks of the political subdivision.
(2) Identify the potential impacts of a cybersecurity breach.
(3) Specify mechanisms to detect potential threats and cybersecurity events.
(4) Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.
(5) Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.
(6) Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. Annual cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program of the Ohio cyber range institute, satisfy the requirements of this division.

ALIGNS ROUGHLY WITH THE FUNCTIONS OF NIST CSF 2.0

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

- What does this mean?
- What does compliance look like?
- Where do I start?
- What goes in a security plan?
- What resources are available to help?

- Compliance Guidance

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Don’t comply with ransom demands unless the Board formally approves and specifies why it’s in the library’s best interest.

(B) A political subdivision experiencing a ransomware incident shall not pay or otherwise comply with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision.

(A.3) "Ransomware incident" means a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Notify Ohio Homeland Security and the Auditor of State of cybersecurity incidents.

(D) The legislative authority of a political subdivision, following each cybersecurity incident or ransomware incident, shall notify both of the following:

(1) The executive director of the division of homeland security within the department of public safety, in a manner prescribed by the executive director, as soon as possible but not later than seven days after the political subdivision discovers the incident;
(2) The auditor of state, in a manner prescribed by the auditor of state, as soon as possible but not later than thirty days after the political subdivision discovers the incident.

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

Mandatory Reporting Guidance

Within 7 days, report incidents to DPS/OHS Ohio Cyber Integration Center

Compliance guidance, including reporting process and definition of reportable incidents:
https://homelandsecurity.ohio.gov/ohio-cyber-integration-center/reporting-guidance

Report instruction form:
https://dam.assets.ohio.gov/image/upload/q_auto/v1756406895/cyber.ohio.gov/cyber-sop-2025-2-final.pdf

Within 30 days, report incidents to the Ohio Auditor of State

Compliance guidance, including FAQ and resources:
https://ohioauditor.gov/fraud/cybersecurity-policy.html

Report form:
https://ohioauditor.gov/fraud/docs/CybersecurityReportingForm.pdf

Ohio Revised Code Section 9.64
Political subdivision cybersecurity

Cybersecurity program documents, incident reports, and security procurement records are not public records.

(E) Any records, documents, or reports related to the cybersecurity program and framework in division (C) of this section, and the reports of a cybersecurity incident or ransomware incident under division (D) of this section, are not public records under section 149.43 of the Revised Code.

(F) A record identifying cybersecurity-related software, hardware, goods, and services, that are being considered for procurement, have been procured, or are being used by a political subdivision, including the vendor name, product name, project name, or project description, is a security record under section 149.433 of the Revised Code.

https://codes.ohio.gov/assets/laws/revised-code/authenticated/0/9/9.64/9-30-2025/9.64-9-30-2025.pdf

- Security Planning from Scratch

Security Planning from Scratch

Where do I start?

Make a list of critical business assets

Make a list of your library's critical business data, including:

- ILS provider
- cloud-hosted services, including email provider
- domain name registrar, public DNS records and authoritative name servers
- financial records and platform
- HR records
- business documents, policies and procedures
- third-party service providers and contracts
- services that accept or store patron payment information
- website hosting provider
- contact information for partner organizations, service providers and staff
- deeds and financial assets
- admin credentials for critical resources
- incident response plan and contact information

Security Planning from Scratch

Where do I start?

Business asset inventory, cont.

Conduct a risk assessment of your business data.
Store each data type in an appropriate way.
Be aware of your library's legal obligations:

- protect personally identifiable information
- don't release patron record information inappropriately
- comply with public records law and records retention policies

Ohio Revised Code, "Releasing library record or patron information," ORC 149.432
https://codes.ohio.gov/ohio-revised-code/section-149.432

Ohio Attorney General: Ohio Sunshine Laws
https://www.ohioattorneygeneral.gov/Legal/Sunshine-Laws

Ohio Library Council: "Standards for Public Library Service in Ohio"
https://olc.org/resources/publications/

Security Planning from Scratch

Where do I start?

Review these guides to become familiar with security concepts and best practices:

Cybersecurity Frontline First Aid Kit

Provided by the Ohio Cyber Range Institute, CFFAK is a self-paced online learning module that introduces key security concepts, and recommends security controls that align with best practices. Suitable for anyone. 2-3 hours, self-paced

NIST CSF 2.0 Small Business Quick-Start Guide

Specific, actionable how-to guide for small organizations starting a security program from scratch. The guide provides planning questions and action steps, with one page for each of NIST CSF 2.0's 6 security functions. 9 pages

CISA Cyber Essentials Toolkit

A series of 6 2-page PDF documents that introduce actionable tasks for administration and IT to implement security controls, starting with planning and moving through security the organization’s business and IT assets. 12 pages

Security Planning from Scratch

Where do I start?

TREAT THIS PAGE AS A TO DO LIST

Leverage existing resources for your initial cybersecurity program:

- Inventory all critical business accounts, data, providers, contact info, and credentials
- Identify data owner roles within the organization
- Review CFFAK and NIST CSF Quick-Start Guide to become familiar with concepts
- Determine who to call in an emergency, and keep all contact information in hard copy
- Enable multi-factor authentication and select long, unique passwords for each account
- Adopt a written procedure to protect the organization against payment fraud
- Create a written incident response plan identifying roles and responsibilities, procedures, and partner contact information, and mandatory reporting information. Review the plan regularly
- Work with your IT provider to make a list of your organization's existing IT assets and security controls, apply secure configurations, employ compensating controls, and limit administrative privileges
- Draft an initial security plan based on your existing resources and controls
- Make a list of goals and identify controls to implement in future years

Security Planning from Scratch

What to include in an initial cybersecurity program?

Have your initial cybersecurity plan reflect your current security controls.

Assess your current security posture, and make a list of controls to implement in the future.

Determine priorities by reviewing the minimum recommended controls listed in ORC 9.64 C.1-6:

(1) Identify and address the critical functions and cybersecurity risks of the political subdivision.

(2) Identify the potential impacts of a cybersecurity breach.

(3) Specify mechanisms to detect potential threats and cybersecurity events.

(4) Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.

(5) Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.

(6) Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. Annual cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program of the Ohio cyber range institute, satisfy the requirements of this division.

Security Planning from Scratch

What you're doing now goes in this year's plan.

Document your current capabilities in a policy document. Review the details in executive session, and have the Board adopt the policy. The policy document and the security program details are not a public record, per ORC 9.64 (E).

What you'll do next goes in next year's plan.

As you're reviewing your initial program, build a list of priorities to work toward adding capabilities. Explore existing controls, free resources and funding opportunities to expand your capacity.

Review your risks and priorities, add capabilities, and revise your plan to match.

As you implement your security goals, revise your security program to reflect your current capabilities. Designate roles and responsibilities, and meet regularly to review and revise your plan. Keep track of the dates of your revisions.

- Resources for Planning and Funding

Resources for Planning and Funding

Security framework and best practices resources:

Cybersecurity Frontline First Aid Kit (CFFAK)
Self-paced online learning module from Ohio Cyber Range Institute that introduces key concepts and security controls
https://www.ohiocyberrangeinstitute.org/cffak

NIST CSF 2.0: Resource and Overview Guide
Accessible summary of goals within each function, with links to resources (8 pages)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf

NIST NCCoE *Protecting Data from Ransomware* whitepaper
Excellent whitepaper for IT staff and MSPs on planning, scoping, and implementing a backup strategy
https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

CIS Controls Navigator
Explore what tasks are covered in each control, and compare with NIST CSF functions
https://www.cisecurity.org/controls/cis-controls-navigator

CIS Controls Self-Assessment Tool
Cloud-hosted self-assessment tool; leverage with your IT provider to assess your current controls, and identify areas for improvement
https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls

Resources for Planning and Funding

Policy building resources:

MS-ISAC NIST Cybersecurity Framework Policy Template Guide
MS-ISAC assembled example templates of cybersecurity policies as Microsoft Word documents, organized by the 6 NIST functions and linked in this PDF.
https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf

CIS Policy Templates
The Center for Internet Security offers policy template documents that align with the CIS 18 security controls. The templates focus on implementation group 1.
https://www.cisecurity.org/controls/policy-templates

State of Ohio Department of Administrative Services Information Security Governance
The State of Ohio DAS's public-facing security governance documents, although they do not apply to public libraries, may be valuable to review for comparison. Policies that are not a public record are noted but not accessible.
https://das.ohio.gov/technology-and-strategy/information-security-privacy/information-security-governance

Resources for Planning and Funding

Funding resources:

Ohio Persistent Cyber Improvement
Free cybersecurity training and assistance developing and testing a cybersecurity program for Ohio local government entities.
https://www.ohiocyberrangeinstitute.org/opci

TechCred
Reimburses Ohio employers for the cost of training leading to certification for employees.
https://techcred.ohio.gov/

E-rate Category 2
Discounts up to 85% of internal network equipment, including installation and maintenance.
https://www.oplin.ohio.gov/category2

State Library of Ohio and SEO Network Equipment Grant
Open next year, a grant to assist libraries by providing a professional assessment of the library's network equipment, and filing for E-rate Category 2 to fund replacing outdated network equipment with the library's selected equipment, vendor, and installation provider.

CyberOhio Cybersecurity Software and Services Grant
Apply for up to $20,000 toward the cost of specific security solutions, including EDR, Vulnerability Management, MFA, and more.
https://cyber.ohio.gov/priorities/assisting-local-government-entities/cyberohio-software-and-services-grant

Resources for Planning and Funding

Free Resources from OPLIN:

Cisco Umbrella DNS security filtering
https://www.oplin.ohio.gov/opendns

Security mailing list for peer information sharing (private archives)
https://lists.oplin.org/mailman/listinfo/oplinsecurity

CISA Cyber Hygiene vulnerability reports
MS-ISAC vulnerability reports
https://www.oplin.ohio.gov/security

E-rate support and training
https://www.oplin.ohio.gov/erateinfo

DMARC Report Analyzer
https://www.oplin.ohio.gov/dmarc

DDoS Mitigation

Lightning Round: Security Controls

Getting Started

- Ensure all accounts have long, unique passwords
- Enable MFA on all accounts, starting with administrator, VPN, and financial accounts
- Create a detailed inventory of data, accounts, service providers, and contact information
- Create an encrypted backup for critical credentials in a password manager
- Deploy unprivileged accounts for daily use; only use accounts with administrative privileges to make changes
- Change default equipment passwords, and ensure no administrative interfaces or unpatched VPNs face the public Internet
- Manage public computers and equipment to ensure patron data is not retained between sessions
- Deploy a DNS filtering solution, including Cisco Umbrella at the network level and uBlock Origin Lite in all browsers
- Create and practice a required procedure to help staff defend against payment fraud

Growing

- Install updates for software, operating systems and firmware promptly
- Inventory all network-connected equipment, determine availability of security patches, and schedule replacement for EOL equipment
- Segment the network to separate staff, patron, and equipment traffic, and enable client isolation on the wireless network
- Monitor all network-connected equipment with an SNMPv3 solution (LibreNMS, PRTG)
- Configure endpoints for security event logging (with free tools like sysmon)
- Deploy endpoint security software such as endpoint detection and response (EDR/MDR/XDR)
- Back up all library data, including business data, configurations and firmware, accounts and credentials, and cloud-hosted services
- Provide all staff with regular security awareness training, and participate in O-PCI

Mature

- Deploy a SIEM to gather endpoint security event data
- Monitor alerts on security events, and provision capacity to analyze, tune, and respond
- Provision enhanced authorization controls, including role-based access control and just-in-time credentials
- Deploy vulnerability monitoring and management tools
- Require service providers to meet a security standard, and audit service provider access to library infrastructure
- Develop, maintain, and practice incident response procedures with stakeholders, including tabletop exercises
- Engage penetration testing to identify areas for improved controls

Takeaway

- Be encouraged!
- Commit to realistic goals in your initial program.
- Plan to grow your program and implement additional controls over time.
- Leverage free resources and funding opportunities.
- Work with external partners and providers to enhance security controls.
- Share your successes, challenges, and experiences with peers.

OPLIN

Jessica D. Dooley
Technology Project Manager
jessica@oplin.ohio.gov

https://oplin.ohio.gov
614-728-5252
support@oplin.ohio.gov
https://support.oplin.org