Ordinance No. 9- 2026
1st Reading, April 13, 2026
Sponsored / Introduced by: Mayor Britton

ORDINANCE NO. 9 - 2026

AN ORDINANCE ADOPTING A CYBERSECURITY POLICY,
AND DECLARING AN EMERGENCY

WHEREAS, recently enacted § 9.64 of the Ohio Revised Code calls upon Ohio political subdivisions to enact policies and work in conjunction with the State to address cybersecurity threats; and

WHEREAS, the Council finds and determines that the purposes and of intents of § 9.64 are consistent with the public peace, health, welfare and safety of the inhabitants of this Village and accordingly it now desires to enact a cybersecurity policy, enact requirements for the reporting of cybersecurity and ransomware incidents, and enact a general prohibition on any payment or other form of compliance with a ransomware incident except upon prior legislative authorization by this Council.

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILAGE OF MADISON, COUNTY OF LAKE, STATE OF OHIO, THAT:

SECTION 1. The "Village of Madison Cybersecurity Program Policy" attached hereto as Exhibit "A" is hereby approved and adopted.

SECTION 2. The Village Administrator is hereby authorized and shall on behalf of the Council in accordance with division (D) of R.C. § 9.64 make the following notifications following each cybersecurity or ransomware incident:

(1) To 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 discovery of the incident; and

(2) To the auditor of state, in a manner prescribed by the auditor of state, as soon as possible but not later than thirty days after discovery of the incident.

SECTION 3. That in accordance with division (B) of R.C. § 9.64, no officer, employee, agent, or contractor of the Village shall in response to a ransomware incident be authorized to pay or otherwise comply with a ransom demand unless upon the prior express approval of the Council authorizing the payment or compliance with the ransom demand, which shall be in the form of a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the Village.

SECTION 4. It is found and determined that all formal actions of this Council concerning and relating to the adoption of this Ordinance were in an open meeting of this Council, and that all deliberations of this Council and any of its committees that resulted in such formal action, were in meetings open to the public, in compliance with all legal requirements including § 121.22 of the Ohio Revised Code.

SECTION 5. This Ordinance is declared to be an emergency measure necessary for the immediate preservation of the public peace, health and safety of the Village and for the further reason that time is of the essence in order to ensure compliance with State law deadlines for the adoption of a cybersecurity policy; WHEREFORE, this Ordinance shall be in full force and effect immediately upon its adoption if adopted by the affirmative vote of at least four members of Council and otherwise at the earliest time provided by Ohio law.

PASSED:

Mark V. Vest,
President of Council

1st Reading: 4-13-26

Attested:

Kristie M. Crockett,
Fiscal Officer / Clerk of Council

Approved:

Date: 4/13/26

Sam Britton, Jr.,
Mayor

VILLAGE OF MADISON

33 E. Main Street, Madison, Ohio 44057

CYBERSECURITY PROGRAM POLICY

---

1. Purpose

The purpose of this Cybersecurity Program is to safeguard the confidentiality, integrity, and availability of the Village of Madison's data, information technology systems, and information technology resources in compliance with **Ohio Revised Code § 9.64**.

This program is designed to reduce cybersecurity risk, ensure continuity of operations, and protect public resources.

---

2. Scope

This policy applies to:

- All Village employees, elected officials, and contractors
- All information systems, networks, devices, and applications
- All third-party vendors with access to Village systems or data

---

3. Cybersecurity Framework Alignment

The Village of Madison aligns its cybersecurity program with generally accepted best practices, including:

- National Institute of Standards and Technology (**NIST**) Cybersecurity Framework
- Center for Internet Security (**CIS**) Critical Security Controls

Controls implemented shall be appropriate to the Village's size, resources, and risk exposure.

---

4. Governance & Responsibilities

- The **Village Administrator and Chief of Police** shall serve as the Cybersecurity Program Coordinator and is responsible for:
  - Oversight of policy implementation
  - Coordination of incident response
  - Required external reporting
- The Village may utilize **third-party IT service providers** to assist with cybersecurity operations.
- Department heads are responsible for ensuring compliance within their respective areas.
- Village Council (legislative authority) formally adopts and approves this policy.

---

5. Risk Identification & Critical Systems

The Village shall:

- Maintain an inventory of:
  - Hardware and devices
  - Software applications
  - Critical systems (e.g., financial systems, payroll, utilities, public services)
- Identify cybersecurity risks that could impact operations
- Evaluate potential impacts of a cybersecurity incident, including:
  - Financial loss
  - Service disruption
  - Unauthorized access to sensitive data
  - Reputational harm

Risk assessments shall be conducted periodically and updated as needed.

---

6. Security Controls

A. Access Control

- Unique user accounts are required
- Access shall be limited based on job responsibilities (least privilege)
- Strong passwords are required
- Multi-Factor Authentication (MFA) shall be implemented where feasible

---

B. System Security

- Systems shall be updated and patched periodically
- Antivirus/endpoint protection shall be utilized
- Firewalls shall be maintained where applicable

C. Data Protection & Backups

- Sensitive data shall be protected and encrypted where feasible
- Data backups shall be:
  - Performed periodically
  - Stored securely (offline or offsite where feasible)
  - Tested periodically for restoration capability

---

7. Threat Detection & Monitoring

- Systems shall utilize logging and monitoring capabilities where feasible
- Suspicious activity shall be reported promptly to the Fiscal Officer or designated IT provider
- Email filtering and phishing protections should be utilized where feasible

---

8. Incident Response Plan

In the event of a cybersecurity incident, the Village shall:

1. Designate an Incident Response Lead
2. Contain and mitigate the threat with assistance from the Village's I.T. Provider
3. Assess the scope and impact
4. Notify internal leadership immediately
5. In accordance with Ohio law:
   - The Village shall notify the Director of Homeland Security through the **Ohio Cyber Integration Center (OCIC)** within **7 days** of discovering a cybersecurity incident (see Appendix A)
   - The Village shall notify the **Ohio Auditor of State** within **30 days** of discovering the incident (See Appendix A)
   - Any other parties required by law
   - Conduct a post-incident review and update policies as needed
   - Establish procedures for the repair and subsequent maintenance of infrastructure after a cybersecurity incident

---

9. Business Continuity & Recovery

The Village shall maintain the ability to restore critical operations following a cybersecurity incident.

This includes:

- Restoration of financial and payroll systems
- Restoration of public service operations
- Periodic testing of recovery procedures where feasible

---

10. Post-Incident Review & Security Improvements

Following a cybersecurity incident, the Village shall:

- Implement corrective actions to address vulnerabilities
- Update security controls as appropriate
- Document lessons learned to reduce future risk

---

11. Ransomware Policy

The Village of Madison adopts a default position of **not paying ransom demands**.

Payment of ransom shall only occur if:

- Approved by formal resolution or ordinance of Village Council
- The resolution specifically states why payment is in the best interest of the Village

---

12. Employee Cybersecurity Training

All employees shall receive cybersecurity training:

- Upon hire
- Periodically thereafter

Training shall be:

- Appropriate to the employee's job duties and level of system access

- Designed to address risks such as phishing, password security, and data handling

The Village may utilize training resources provided by:

- The Ohio Persistent Cyber Initiative (O-PCI)
- The Ohio Cyber Range Institute
- Other qualified providers

---

13. Vendor & Third-Party Security

Third-party vendors with access to Village systems or data shall:

- Maintain reasonable cybersecurity safeguards
- Notify the Village of any cybersecurity incident affecting Village data in a timely manner

Where applicable, contracts should include data protection and breach notification provisions.

---

14. Policy Review & Updates

This policy shall be reviewed **annually** and updated as necessary to address evolving cybersecurity risks and operational changes.

---

15. Public Records Exemption

Records, documents, and information related to cybersecurity systems, infrastructure, and incidents are considered security records and are exempt from disclosure under Ohio law as follows:

(1) Pursuant to R.C. § 9.64(E), any records, documents, or reports related to the Village's cybersecurity program and framework and the reports of a cybersecurity incident or ransomware incident are not public records under § 149.43 of the Revised Code.

(2) Pursuant to R.C. § 9.64(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 the Village, including the vendor name, product name, project name, or project description, is a security record under § 149.433 of the Revised Code.

APPENDIX A

Director of Homeland Security
Ohio Cyber Integration Center
1970 W. Broad St.
Columbus, OH 43223
Phone: 614-387-6171
Fax: 614-752-2419
Email: OCIC@dps.ohio.gov
Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center

The Auditor of the State of Ohio
65 E. State St.
Columbus, OH 43215
Phone: 1-800-626-2297 | 216-787-3665
Email: cyber@ohioauditor.gov
Website: https://ohioauditor.gov/fraud/cybersecurity.html

Village I.T. Provider
Newbury Technologies
11938 Mayfield Rd. Building B
Chardon, OH 44024
440-973-8379
Email: helpdesk@newburypc.com
Website: https://newburypc.com/