

**VILLAGE OF McDONALD, OHIO**

**ORDINANCE NO. 3338-26**

**AN ORDINANCE ADOPTING A CYBERSECURITY PROGRAM IN ACCORDANCE WITH OHIO REVISED CODE SECTION 9.64.**

WHEREAS, Ohio Revised Code §9.64, which became effective on September 30, 2025, requires the Village to establish and adopt a cybersecurity program to safeguard the Village's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity; and

WHEREAS, Council for the Village of McDonald desires to establish a cybersecurity program in compliance with law to protect the Village's data, information technology, and information technology resources.

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF McDONALD, TRUMBULL COUNTY, STATE OF OHIO, that:

Section I. The Village of McDonald hereby adopts the Cybersecurity Program attached hereto as Exhibit A.

Section II. The passage of this Ordinance and all deliberations relating to the passage of this Ordinance were held in open meetings in accordance with the provisions of Ohio Revised Code Section 121.22.

Section III. This Ordinance shall take effect and be in full legal force and effect from and after the earliest period allowed by law.

Passed in Council this 20<sup>th</sup> day of May, 2026.

\_\_\_\_\_  
Mayor

Attest to:

\_\_\_\_\_  
Fiscal Officer

# **EXHIBIT A**

## **VILLAGE OF McDONALD CYBERSECURITY PROGRAM**

### **1. PURPOSE AND SCOPE**

This plan establishes the Village of McDonald (“Village”) cybersecurity program. It defines the governance, structure, roles, responsibilities, technical safeguards, and operational processes that protect the Village’s systems and data, ensuring compliance with Ohio Revised Code §9.64 while providing layers of protection against cyber threats. This program is based on NIST Cybersecurity Framework and CIS Controls, scaled according to the scope and needs of the Village. It applies to all employees, contractors, and third-party vendors with access to the Village systems.

### **2. GOVERNANCE AND RESPONSIBILITIES**

- **Village Council:** Provides oversight, formally adopts the cybersecurity program, and approves any ransom payments, if ever considered and recommended.
- **Village Administration:** Ensures executive-level support and coordinates with Council during incidents.
- **Fiscal Officer:** Oversees budgeting and ensures compliance with State of Ohio requirements.
- **IT (Team Office Technologies and Mr. PC):** Manages daily cybersecurity operations, monitoring, and incident response.
- **Department Heads:** Ensure staff compliance with cybersecurity policies.
- **Employees:** Complete training and follow secure computing practices.

### **3. CONFIDENTIALITY/PUBLIC RECORDS EXCEPTION**

In accordance with Ohio Revised Code §149.433 and Ohio Revised Code §9.64, records related to the Village cybersecurity program, security procurements, and incident response plans are classified as security records and are not subject to public disclosures. This summary version of the program may be adopted by the Village, while any detailed version will remain restricted.

### **4. RISK MANAGEMENT AND ASSET INVENTORY**

- Maintain a complete inventory of hardware, software, and cloud services.
- Perform annual risk assessments to identify vulnerabilities.
- Classify assets as critical, important, or standard to prioritize protections.

## 5. ACCESS CONTROLS AND AUTHENTICATION

- **Multi-Factor Authentication (MFA):** Multi-factor authentication is enforced for all employees.
- **Least Privilege:** No users have administrative rights. Privilege access is granted by Team Office Technologies.

## 6. ADVANCED EMAIL SECURITY AND AWARENESS TRAINING.

- Annual training required for all employees.
- Ongoing phishing simulations to test employee vigilance.

## 7. PATCH AND VULNERABILITY MANAGEMENT.

- **Automated Patching:** All workstations and servers are centrally patched for both Microsoft and third-party engineered patching service.
- **Service Levels:**
  - Critical patches are deployed immediately.
  - Regular vulnerability scans performed with remediation tracked.

## 8. ENDPOINT AND EMAIL SECURITY

- **Endpoint Detection & Response (EDR):** A comprehensive, enterprise EDR solution is deployed across all servers and workstations.
- **SOC Monitoring:** A 24/7 SOC team monitors EDR alerts and takes corrective action immediately in response to any threats.

## 9. NETWORK SECURITY

- **Firewalls:** Enterprise firewall hardware protects the edge of the network, as well as all satellite facilities.
- **Protections Enabled:** Advanced Malware Protection (AMP).
- **Segmentation:** Sensitive systems isolated where appropriate.

## 10. DATA PROTECTION AND BACKUPS

- **Backup Strategy:** Backups are conducted using an industry-standard software package, with immutable storage utilized. All back up data is encrypted end to end.

- **Testing:** Periodic backup restore tests performed.

## 11. INCIDENT RESPONSE

- **Incident Response Team:** Team Office Technologies, Designee, Department Heads, and external vendors as needed.
- **Notification Requirements:**
  - Ohio Auditor of State (AOS) must be notified within 48 hours for all confirmed breaches, even if law enforcement is already engaged.
  - Law enforcement must be notified promptly if criminal activity is suspected.
  - Impacted individuals must be notified in compliance with State of Ohio data breach laws.
  - Ohio Cyber Reserve/Department of Public Safety (OCIC/DPS) must be notified within 7 days following the discovery of a confirmed cybersecurity incident.
- **Escalation:** Team Office Technologies coordinates containment, eradication, and recovery.

## 12. TESTING AND REVIEW

- Periodic penetration testing.
- Annual tabletop exercises for incident response.
- Annual review of cybersecurity plan for alignment with State of Ohio and federal mandates.

## 13. GOVERNANCE & COMPLIANCE

- The Village must adopt this cybersecurity program by Ordinance.
- This policy will be reviewed and updated annually, or following any material change in State of Ohio or federal requirements.
- State Auditors will be provided access to the full cybersecurity program upon request.
- Village administration reserves the right to amend this plan as necessary at its discretion.