

**RESOLUTION NO. 2026-05-18-012**

A RESOLUTION ADOPTING A CYBER SECURITY POLICY

WHEREAS, the State of Ohio has implemented Ohio Revised Code 9.64, enacted in HB 96 (136<sup>th</sup> G.A.), requiring all local governments and jurisdictions to establish a cybersecurity policy; and

WHEREAS, the purpose of this requirement is to strengthen protections of public data, information systems, and technology resources from cybersecurity threats and risks; and

WHEREAS, the Village of Wayne Lakes recognizes the importance of safeguarding sensitive and confidential information entrusted to the Village of Wayne lakes and,

WHEREAS, A Cybersecurity Policy provides guidance on access control, system security, data protection, incident response, training, and vendor management, while requiring customization;

NOW, THEREFORE IT BE RESOLVED by the Council of the Village of Wayne Lakes, Darke County, Ohio, that:

1. The attached Cybersecurity Policy is hereby adopted as the official policy of the Village of Wayne Lakes.
2. This policy shall take effect immediately, with implementation of technical and training requirements no later than Oct 30, 2026, as provided by the Ohio Auditor of State.
3. Village of Wayne Lakes shall distribute the adopted policy to all the departments, employees, and relevant contractors, and to ensure compliance in partnership with IT providers and legal counsel.
4. This resolution shall be in full force and effect upon its passage and adoption.

Passed this 18 day of May, 2026.

President of Council

ATTEST:

Fiscal Officer

APPROVED by the Mayor this

18 day of May 2026.

Mayor

## Village of Wayne Lakes, Darke County, Cybersecurity Policy

### 1. Purpose

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of Wayne Lakes information systems, data, and technology resources in compliance with R.C. 9.64 cybersecurity requirements.

### 2. Scope

This policy applies to all elected officials, employees, contractors, vendors, and third parties who access or manage Wayne Lakes technology resources, including but not limited to : computers, servers, and mobile devices, cloud services and hosted applications networks and telecommunications systems, sensitive or confidential data (e.g. PII, financial , law enforcement, health-related, or other protected records)

### 3. Policy Statement

Village of Wayne Lakes is committed to safeguarding its information systems against cybersecurity threats and ensuring compliance with R. C. 9.64 by:

Establishing baseline cybersecurity practices

Providing ongoing cybersecurity awareness training.

Preparing for detection, response, and recovery from incidents.

Reviewing and updating cybersecurity policies annually.

### 4. Roles and Responsibilities

Village Council: Approves cybersecurity policy and ensures resources are allocated.

Fiscal Officer: Oversees policy implementation, coordinates with IT providers and legal counsel.

IT Provider (Internal or Vendor): Implement technical safeguards, monitors for threats, and reports incidents.

Employees/Users:

Follow cybersecurity protocols, complete training, and report suspicious activity.

## 5. Cybersecurity Controls

### 5.1 Access Control

Require unique user IDs and strong passwords. Enforce multi-factor authentication (MFA) for remote or administrative access. Limit access to sensitive data on a “least privilege” basis.

### 5.2 Network and System Security

Maintain up to date firewalls, antivirus, and intrusion detection/prevention. Apply software patches and updates within 30 days of release. Segregate critical systems from public networks when possible.

### 5.3 Data Protection

Encrypt sensitive data at rest and in transit. Regularly back up critical data and test restoration procedures. Retain records according to Ohio records retention schedules.

### 5.4 Incident Response

Designate an Incident Response Lead. Establish procedures for detecting, reporting, and escalating incidents. In the event of a cybersecurity incident, notify the following parties in the manner listed:

- (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.
- (3) 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.

### 5.5 Training and Awareness

Require all employees to complete cybersecurity awareness training annually. Provide role-specific training for IT administrators and staff handling sensitive data.

### 5.6 Vendor and Third-Party Management

Require vendors to comply with Wayne Lakes cybersecurity standards. Maintain contracts with cybersecurity clauses and breach notification requirements.

## 6. Compliance and Review

This policy will be reviewed annually and updated to reflect changes in technology, law, and organizational needs. Departments and third-party IT providers must submit evidence of compliance to the Fiscal Officer annually.

7. Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, as well as potential civil and criminal penalties in accordance with applicable law.

8. Effective Date

This policy takes effect immediately to meet R.C. 9.64 requirements. Implementation of technical and training requirements must be completed no later than October 30, 2026.