VILLAGE OF ELIDA, OHIO

ORDINANCE NO. 1255-2026

AN ORDINANCE TO ADOPT AND ADD CYBERSECURITY POLICY TO THE EMPLOYEE HANDBOOK

WHEREAS, Ohio Revised Code § 9.64, enacted through House Bill 96, requires political subdivisions to set and adopt standards for safeguarding against cybersecurity threats and ransomware attacks, and

WHEREAS, in conformity with Ohio Revised Code § 9.64 the Elida Village Council wishes to establish a policy that implements the expectations and requirements for Village employees to safeguard the Village's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity, and

WHEREAS, the Elida Village Council wishes to formally adopt a Cybersecurity Policy and add said policy to the Village Employee Handbook

BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF ELIDA, STATE OF OHIO, a majority of its members elected thereto concurring:

SECTION 1. The Village of Elida shall adopt and add to the Employee Handbook a Cybersecurity Policy which shall reads as set forth below:

A. PURPOSE

1. Ohio Revised Code § 9.64, enacted through House Bill 96, requires political subdivisions to set and adopt standards for safeguarding against cybersecurity threats and ransomware attacks. The purpose of this policy is to implement expectations and requirements for Village employees to safeguard the Village's data, information technology, and information technology resources to ensure availability, confidentiality, integrity and to maintain compliance with Ohio Revised Code § 9.64.

B. STATEMENT

1. The Village of Elida is committed to safeguarding its information systems against cybersecurity threats and maintaining compliance with Ohio Revised Code § 9.64. This policy applies to all elected officials, employees, contractors, vendors, and third parties who access or manage the Village's technology resources.

C. CYBERSECURITY PROGRAM

1. Pursuant to Ohio Revised Code § 9.64 the Village of Elida shall adopt a cybersecurity program that safeguards the Village'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:

    a. Identify and address the critical functions and cybersecurity risks of the Village;

    b. Identify the potential impacts of a cybersecurity breach;

    c. Specify mechanisms to detect potential threats and cybersecurity events;

    d. Specify procedures for the Village to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents;

    e. Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident;

    f. Establish cybersecurity training requirements for all employees of the Village; 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.

2. Any records, documents, or reports related to the cybersecurity program and framework in division (C)(1) of this section, and the reports of a cybersecurity incident or ransomware incident under division (E)(2) of this section, are not public records under Ohio Revised Code § 149.43.

3. 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 Ohio Revised Code § 149.433.

D. CYBERSECURITY TRAINING

1. REQUIRED CYBERSECURITY TRAINING

    a. Any person, as described in section (1)(B)(1) above, is required to complete cybersecurity awareness training annually. Any training provided by the State of Ohio and Ohio Persistent Cyber Initiative Program (O-PCI) of the Ohio Cyber Range Institute shall satisfy this requirement.

2. CYBERSECURITY TRAINING STANDARDS

    a. Regardless of who provides the Village employees with cybersecurity training, the curriculum shall be consistent with the O-PCI of the Ohio Cyber Range Institute. The frequency, duration, and detail of which shall correspond to the duties of each employee.

E. CYBERSECURITY INCIDENT RESPONSE

1. COORDINATION

    a. The Village, through its Fiscal Officer, or their designee, shall be responsible for coordinating a response to a cybersecurity or ransomware incident.

2. NOTIFICATION

    a. The Village, though its Fiscal Officer, or their designee, shall be responsible for notifying the following parties in compliance with Ohio Revised Code § 9.64:

        - 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 (7) days after the discovery of the incident;

        - The Auditor of the State of Ohio, in a manner prescribed by the Auditor of the State of Ohio, as soon as possible but not later than thirty (30) days after the discovery of the incident;

3. CYBERSECURITY/RANSOMWARE INCIDENT DEFINED

    a. A cybersecurity incident includes any of the following:

- A substantial loss in confidentiality, integrity, or availability of a covered entity's information system of network;

- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;

- A disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services. This may include any payment or payroll re-direct schemes.

- Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or a supply chain compromise.

- A 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.

b. A 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.

4. RANSOMWARE PAYMENT POLICY

a. In the event of a ransomware incident, the Village or any employees shall not pay or otherwise comply with a ransom demand unless the Village Council 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.

SECTION 2. The above policy shall replace any previous version of this policy and supersedes any current policy, formal or informal, written or unwritten, which may conflict with this policy.

SECTION 3. This Ordinance is hereby determined to be an emergency measure and shall take effect immediately, provided that it receives the affirmative vote of two-thirds of the members elected to the Village Council.

Date Passed: June 23, 2026

ATTEST:

Fiscal Officer, Village of Elida

APPROVED:

Mayor, Village of Elida