ORDINANCE NO. 2026-08

AN ORDINANCE ADOPTING A CYBERSECURITY PROGRAM FOR THE VILLAGE OF PERRY, OHIO, IN ACCORDANCE WITH OHIO REVISED CODE § 9.64, AND DECLARING AN EMERGENCY.

WHEREAS, the State of Ohio recently enacted Ohio Revised Code § 9.64, which mandates that political subdivisions implement and maintain a formal cybersecurity program; and

WHEREAS, the Village of Perry is committed to providing its employees, elected officials, contractors, and authorized agents with clear direction for safeguarding Village data, information technology resources, and assets; and

WHEREAS, a comprehensive organizational framework and governing document, titled the "Perry Village - Cyber Security Program," has been drafted to meet these statutory requirements and establish the Village's security controls and practices.

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF PERRY, LAKE COUNTY, OHIO:

SECTION 1. The Council of the Village of Perry hereby formally approves and adopts the "Perry Village - Cyber Security Program," a copy of which is attached hereto as **Exhibit A** and incorporated fully herein by reference.

SECTION 2. All specific details regarding incident reporting, ransomware governance, employee training, system administration by Lake County IT, and records confidentiality shall be governed by the provisions set forth in Exhibit A. The Mayor, or their designee, is hereby authorized and directed to coordinate with Lake County IT to execute and enforce the policies contained therein.

SECTION 3. It is found and determined that all formal actions of this Council concerning and relating to the passage of this Ordinance were adopted in an open meeting of this Council, and that all deliberations of this Council and of any of its committees that resulted in such formal action were in meetings open to the public, in compliance with all legal requirements including Section 121.22 of the Ohio Revised Code.

SECTION 4. This Ordinance is hereby declared to be an emergency measure necessary for the immediate preservation of the public peace, health, safety, and operational security of the Village of Perry, specifically to ensure compliance with state cybersecurity mandates. Wherefore, this Ordinance shall take effect and be in full force immediately upon its passage and approval by the Mayor, with the Program itself bearing an effective date of July 1, 2026.

ELIAS COSS, ACTING MAYOR

ADOPTED: June 18, 2026

ATTEST: _____

JOHN H. ROSKOS, FISCAL OFFICER

FIRST READING 5/14/26
SECOND READING 6/18/26
THIRD READING Rules Suspended

Perry Village - Cyber Security Program

Effective Date: July 1, 2026

1. Overview

This document constitutes the Cybersecurity Program of the Village of Perry, Ohio as required by Ohio Revised Code § 9.64 (Political Subdivision Cybersecurity). It establishes the organizational framework for safeguarding Perry Village data and information technology resources, and serves as the foundational governing document for all cybersecurity-related standards, procedures, and practices adopted by the Village.

2. Purpose

The Village of Perry is committed to providing its employees, elected officials, and contractors and other authorized agents with access to Village IT resources, data, or assets with clear direction for the safeguarding of Village information assets.

This cybersecurity program establishes the overall intent of the Village to support and promote information security across all its operations and practices. Additional standards, requirements, guidelines, and procedures created to support this program will be organized under this governing document as needed.

The Village of Perry has contracted with Lake County Information Technology (Lake County IT) to provide managed IT services, including the administration and oversight of this cybersecurity program. Lake County IT, acting as the Village's designated IT service provider, is responsible for the implementation, maintenance, and day-to-day management of the security controls and practices described herein. The Village Administrator or designee serves as the primary Village-side point of contact for cybersecurity matters and coordinates with Lake County IT on policy review, incident response, and compliance obligations under Ohio Revised Code § 9.64.

3. Scope

This program applies to all Perry Village employees, elected officials, contractors, volunteers, and any other authorized agents who access, use, or administer Perry Village IT resources, systems, or data. It covers all computer systems, network infrastructure, telecommunications systems, and data regardless of physical location or ownership used in support of Village operations.

A successful cybersecurity program depends on strong leadership support and security practices that:

- Promote public trust
- Ensure continuity of municipal services
- Comply with Ohio Revised Code § 9.64 and other applicable legal requirements

- Recognize and respond to evolving risks and threats
- Protect Village systems, data, and assets

4. Policy

The Village of Perry, as part of an overall security management strategy, shall develop and maintain cybersecurity policies, standards, requirements, and practices aligned with the **CIS Controls v8**, starting with Implementation Group 1 (IG1), as the foundational security framework for Village operations. All cybersecurity policies and practices shall ensure compliance with Ohio Revised Code § 9.64 and all other applicable federal and state security-related regulations.

Perry Village shall ensure that all personnel and partners are aware of their specific information security responsibilities in the use of Village information systems and the handling of Village data and assets.

The following minimum-security requirements provide the foundation for this program and are organized around the core principles of the CIS Controls:

4.1 Risk Management

Perry Village shall apply risk management techniques to balance the need for security measures against cost and operational impact, making informed decisions that guide the design and implementation of cybersecurity policies, standards, requirements, guidelines, and practices. Impact upon the delivery of municipal services will be considered as a key factor in this process.

4.2 Confidentiality, Integrity and Availability

Perry Village shall ensure that its IT security policies, standards, requirements, guidelines, and practices address the basic security elements of confidentiality, integrity, and availability.

4.3 Protect, Detect, and Respond

Security policies, standards, requirements, guidelines, and practices shall include methods to protect against, detect, and respond to threats and vulnerabilities to Village systems and data. These controls will be implemented with consideration of business impact and resource constraints for all Perry Village departments tasked with their implementation.

4.4 Identification and Authentication

Perry Village shall implement identification and authentication requirements for information systems and services that protect the Perry Village's data and physical IT resources in the most appropriate manner.

4.5 Access Control and Authorization

Perry Village shall implement access control and authorization policies, plans, standards, and procedures required to protect Village systems, data, and information resources.

4.6 Security Audit Logging

Perry Village shall implement a security audit logging capability for information systems, including computers and network devices.

4.7 Security Management and Administration

Perry Village shall implement a Village-wide security management and administration program.

4.8 Process Management

This cybersecurity program and any supporting standards, procedures, or practices shall be reviewed at least annually by Lake County IT in coordination with the Village Administrator. Updates required by changes in law, technology, or threat environment may be made at any time. Any substantive revision to this program shall be presented to Village Council for adoption. Lake County IT shall maintain the current version of this program and make it available to Village leadership upon request.

4.9 Cybersecurity Incident Reporting

Perry Village shall report cybersecurity incidents and ransomware incidents as required by Ohio Revised Code § 9.64. Upon discovery of a qualifying incident, Perry Village shall: (a) notify the Ohio Department of Homeland Security — Ohio Cyber Integration Center (OCIC) as soon as possible, but not later than seven (7) days after discovery; and (b) notify the Ohio Auditor of State as soon as possible, but not later than thirty (30) days after discovery. Perry Village shall designate a point of contact responsible for coordinating all incident reporting obligations under this section and shall ensure that contact information for OCIC and the Auditor of State is maintained and readily accessible to responsible staff.

4.10 Employee Cybersecurity Awareness Training

Perry Village shall ensure that all employees, contractors, and authorized agents with access to Perry Village IT resources receive cybersecurity awareness training. Training shall be provided upon onboarding and on at least an annual basis thereafter. Training shall cover, at a minimum, password security, phishing awareness, acceptable use of IT resources, and incident reporting procedures. Training records, including participant names, completion dates, and topics covered, shall be maintained and made available upon request to demonstrate compliance. Annual training provided through the Ohio Persistent Cyber Improvement (O-PCI) program of the Ohio Cyber Range Institute, or other state-approved equivalent, satisfies this requirement.

4.11 Ransomware Incident Governance

Perry Village shall not pay any ransomware demand except as expressly authorized by a resolution of the Perry Village legislative authority adopted in accordance with Ohio Revised Code § 9.64. Prior to authorizing any ransomware payment, the legislative authority shall adopt a resolution documenting the justification for payment and finding that payment is in the best interest of Perry Village. Any ransomware incident shall be reported to the OCIC and the Auditor of State within the timeframes established in the Cybersecurity Incident Reporting section of this policy, regardless of whether a payment is made.

4.12 Records Confidentiality

Records, documents, and reports related to this cybersecurity program and framework, including cybersecurity incident reports and ransomware incident reports, are security records and are not public records under Ohio Revised Code § 149.43, pursuant to Ohio Revised Code § 9.64(E). Records identifying cybersecurity-related software, hardware, goods, and services that are being considered for procurement, have been procured, or are currently in use by Perry Village are security records under Ohio Revised Code § 149.433 and shall be withheld from public disclosure accordingly.

5. Policy Compliance

5.1 Compliance Measurement

Compliance with this program shall be verified through periodic review by Lake County IT in coordination with the Village Administrator, internal assessments, findings from the Ohio Auditor of State, and review of security incident reports and training records.

5.2 Exceptions

Exceptions to specific security controls within this program must be requested in writing and approved by Lake County IT in coordination with the Village Administrator. Exceptions shall be documented, time-limited, and subject to annual review. No exception may be granted that would place Perry Village out of compliance with Ohio Revised Code § 9.64.

5.3 Non-Compliance

Any employee, contractor, or authorized user found to have violated this program may be subject to disciplinary action, up to and including termination of employment or removal of system access.

6. Related Standards, Policies and Processes

Ohio Revised Code § 9.64 — Political Subdivision Cybersecurity (effective September 30, 2025); NIST Cybersecurity Framework; CIS Controls v8; Ohio Auditor of State Cybersecurity Guidance.

7. Definitions and Terms

Cybersecurity Incident: As defined in Ohio Revised Code § 9.64, an event involving a substantial loss of confidentiality, integrity, or availability of an information system or network; a serious impact on the safety or resiliency of operational systems; a disruption of normal operations or service delivery; or unauthorized access to an information system facilitated through a compromise of a third-party provider. Does not include mere threats of disruption such as extortion or events perpetrated in good faith.

Ransomware Incident: A cybersecurity incident in which malicious software encrypts, destroys, or renders inaccessible Perry Village data or systems, with a demand for payment to restore access.

OCIC: Ohio Cyber Integration Center, a division of the Ohio Department of Homeland Security. Designated primary reporting authority for cybersecurity incidents under Ohio Revised Code § 9.64.

O-PCI: Ohio Persistent Cyber Improvement program, administered by the Ohio Cyber Range Institute. Annual training completion through O-PCI satisfies the employee cybersecurity awareness training requirement of Ohio Revised Code § 9.64.

8. Revision History

Date of Change	Responsible	Summary of Change
June 2026	Lake County IT	Draft of initial Cybersecurity Program in compliance with Ohio Revised Code § 9.64.