ORDINANCE NO. 2026-08

AN ORDINANCE TO ADOPT A CYBERSECURITY PROGRAM PURSUANT TO OHIO REVISED CODE SECTION 9.64, AND DECLARING AN EMERGENCY

WHEREAS, the Ohio Auditor of State, under the authority granted by House Bill 96 and Ohio Revised Code (ORC) Section 9.64, requires all political subdivisions to adopt a formal Cybersecurity Program to safeguard public data, information technology, and information technology resources; and

WHEREAS, the Village of Alexandria recognizes the growing importance of maintaining the confidentiality, integrity, and availability of municipal information systems and data; and

WHEREAS, the Ohio Auditor of State has provided guidance and training outlining the compliance expectations for municipalities regarding adoption of cybersecurity programs; and

WHEREAS, the Village of Alexandria, through its existing technology services and cyber risk management contracts, as well as its ongoing IT initiatives, has established strong cybersecurity practices that align with state and national standards; and

WHEREAS, this Ordinance formalizes those existing practices and demonstrates compliance with ORC Section 9.64 without incurring additional cost to the Village.

NOW, THEREFORE, BE IT ORDAINED by the Council of the Village of Alexandria, County of Licking and State of Ohio:

Section 1: The Administration is authorized and directed to adopt a cybersecurity program consistent with the requirements of ORC Section 9.64 and aligned with generally accepted best practices such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Section 2: The cybersecurity program shall comply with all requirements of ORC Section 9.64, and shall safeguard public data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.

Section 3: The Administration's designated representatives shall oversee the implementation, documentation, and annual review of the cybersecurity program to ensure continued alignment with state requirements and best practices.

Section 4: All records and documents related to the City's cybersecurity program are exempt from public records disclosure, consistent with Ohio Revised Code Section 9.64(E).

Section 5: This Council finds and determines that all formal actions of this Council

concerning and relating to the adoption of this Ordinance were taken in an open meeting of this Council and that all deliberations of the Council and of any of its Committees comprised of a majority of the members of the Council that resulted in those formal actions were in meetings open to the public, in compliance with the law.

Section 6: This Ordinance is declared to be an emergency measure necessary for the public peace, health, and safety of the Municipality, and for the further reason it is necessary for the Village to adopt a cybersecurity program to be in timely compliance with ORC Section 9.64; wherefore, this Ordinance shall be in full force and effect immediately upon its passage by Council.

PASSED: This 2nd day of June, 2026.

ATTEST:

Mayor Sean Barnes

Caroline J. Gissinger, FO
Caroline J. Gissinger, Fiscal Officer

APPROVED AS TO FORM:

David T. Ball, Esq., Solicitor

VILLAGE OF ALEXANDRIA
CYBERSECURITY POLICY

PURPOSE AND AUTHORITY

This policy establishes the official cybersecurity program for the Village of Alexandria in compliance with Ohio Revised Code Section 9.64. The purpose of this policy is to safeguard Village data, information technology (IT) systems, and IT resources against cybersecurity threats, including but not limited to ransomware, phishing, social engineering, and data breaches.

This program ensures the availability, confidentiality, and integrity of Village information systems and aligns with recognized cybersecurity best practices, including the NIST Cybersecurity Framework and Center for Internet Security (CIS) Controls.

DEFINITIONS

Cybersecurity Program – A structured set of policies, practices, and controls adopted by the Village to prevent, detect, respond to, and recover from cybersecurity incidents.

Cybersecurity Incident – Any event that results in a substantial loss of confidentiality, integrity, or availability of the Village's information systems or network, unauthorized access to sensitive information, or disruption of Village services.

Managed Service Provider (MSP) – a third-party technology vendor contracted by the Village of Alexandria to provide information technology services, including system monitoring, cybersecurity support, and incident response assistance. The MSP operates under contract and in coordination with the Village Administrator but does not independently act on behalf of the Village unless specifically authorized.

Ransomware Incident – A malicious cybersecurity incident in which software gains unauthorized access to Village systems of data, rendering them unavailable, followed by a demand for ransom.

Political Subdivision – As defined in R.C. 9.64, including counties, townships, and municipalities.

CYBERSECURITY PROGRAM STANDARDS

The Village of Alexandria shall maintain a cybersecurity program that includes:

Adopted 6-2-2026
Ordinance 2026-08

Risk Identification – Identifies critical functions, IT assets, and cybersecurity risks to Village operations.

Impact Assessment – Evaluates the potential impacts of a cybersecurity breach on Village operations and public safety.

Threat Detection – Implements monitoring tools, alerts, and procedures to detect potential cybersecurity threats or incidents.

Incident Response Procedures – Establishes communication channels and processes to analyze, contain, and recover from cybersecurity incidents.

Recovery and Maintenance – Provides procedures for restoring affected systems, securing infrastructure post-incident, and maintaining ongoing resilience.

EMPLOYEE CYBERSECURITY TRAINING

Mandatory Training is required for all Village employees; employees shall complete annual cybersecurity training as follows:

Approved Training Program – Training provided by the Ohio Persistent Cyber Initiative (O-PCI) or equivalent programs satisfies this requirement.

Role-Based Training – Additional training may be required for employees with elevated IT access or responsibilities.

Tracking Compliance – The Village Administrator shall track and report training completion annually to the Mayor

INCIDENT REPORTING REQUIREMENTS

In the event of a cybersecurity or ransomware incident, the Village of Alexandria shall:

Notify the Ohio Department of Public Safety – Ohio Homeland Security (OCIC) within 7 days of discovery.

OCIC Contact – https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
Email – OCIC@dps.ohio.gov
Phone – (614) 387-1089

Notify the Ohio Auditor of State within 30 days of discovery.

Email – cyber@ohioauditor.gov
Reporting Form – https://ohioauditor.gov/fraud/cybersecurity.html

Internally, incidents shall be reported immediately to the Village Administrator, who will notify the Mayor. The Mayor will then make notification to Village Council.

If Personally Identifiable Information (PII) is breached, notification of affected residents must follow the requirements of R.C. 1349.19.

Managed Service Provider (MSP) Notification and Coordination (if under contract)

MSP Notification Requirement - Upon discovery or suspicion of a cybersecurity or ransomware incident, the Village Administrator shall immediately notify the Village's contracted Managed Service Provider (MSP). If the Village Administrator is unavailable, Village personnel discovering the incident shall notify both the MSP and the Mayor directly.

MSP Role in Incident Response - The MSP shall assist in investigating, containing, and remediating the incident in coordination with the Village Administrator. The MSP shall provide technical documentation, logs, and analysis to support required state reporting.

Coordination with State Reporting - The MSP shall not directly report to state authorities unless specifically authorized by the Village Administrator or Mayor. The MSP's role is to provide timely information and technical support to ensure that required reports to Ohio Homeland Security and the Ohio Auditor of State are accurate and complete.

RANSOMWARE RESPONSE

Prohibition on Payment – The Village shall not pay or comply with ransom demands unless authorized by a formal vote of Village Council

Council Resolution Requirement – Any authorization must be in the form of a resolution or ordinance stating why payment or compliance is in the Village's best interest.

Documentation – All actions taken in response to ransomware incidents must be documented and retained by the Village Administrator.

RECORDS AND PUBLIC RECORDS EXEMPTIONS

Cybersecurity programs, incident reports, and related records are exempt from disclosure under R.C. 9.64.

Procurement records identifying cybersecurity-related software, hardware, vendors, or services are designated as security records and are not public records.

OVERSIGHT AND COMPLIANCE

The Village Administrator shall be responsible for implementing and maintaining the cybersecurity program.

Adopted June 2, 2026
Ordinance 2026-08

The cybersecurity program will be reviewed annually and updated as necessary.

Compliance procedures will align with the Ohio Compliance Supplement as developed by the Auditor of State.

EFFECTIVE DATE

This policy shall become effective upon adoption by the Village of Alexandria Council.

Adopted June 2, 2026
Ordinance 2026-08