VILLAGE OF LOCKLAND, OHIO
RESOLUTION # 2025-R-12

A RESOLUTION ADOPTING CYBERSECURITY POLICIES AND AUTHORIZING AND DIRECTING THE VILLAGE ADMINISTRATOR TO IMPLEMENT NECESSARY TRAINING AND COMPLIANCE

WHEREAS, the State of Ohio has implemented Ohio Revised Code §9.64, enacted in HB 96 (136th 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 Lockland recognizes the importance of safeguarding sensitive and confidential information entrusted to it; and

WHEREAS, a Cybersecurity Policy has been prepared by the Village's IT staff to meet the framework for compliance with Ohio Revised Code § 9.64 and HB 96; and

WHEREAS, the policy provides guidance on access control, system security, data protection, incident response, training, and third-party management, while requiring consultation with IT professionals and legal counsel for implementation and customization; and

WHEREAS, the Policy has been reviewed by Village staff and legal counsel and is recommendations for adoption; now, therefore

BE IT RESOLVED by the Council of the Village of Lockland, State of Ohio, that:

SECTION I A Cybersecurity Policy, attached hereto as Exhibit A and incorporated by reference herein, is hereby adopted as the official cybersecurity policy of the Village; and

SECTION II: The Village Administrator shall distribute the adopted policy to all Village departments, employees, and relevant contractors, and ensure compliance in partnership with IT providers and legal counsel; and

SECTION III: The Village administrator is authorized and directed to ensure that implementation of technical and training requirements required by the state law and attendant cybersecurity policy are completed by relevant Village staff no later than June 30, 2026, as provided by the Ohio Auditor of State; and

SECTION IV: This Resolution shall take effect and be in full force from and after the earliest period allowed by law.

Passed this 8th day of December, 2025.

MAYOR, VILLAGE OF LOCKLAND

Attested:
CLERK OF COUNCIL

EXHIBIT A
to Res. # 2025 – R- 12

I. Disclaimer

This document is adopted to fulfill the requirements of Ohio Revised Code §9.64, enacted through HS 96 (136th G.A.). It serves as the official cybersecurity policy of the Village of Lockland. This policy is Intended to provide a framework for cybersecurity practices and compliance but does not constitute legal advice. The Village may consult with legal counsel and IT professionals to adapt and refine this policy, by Council resolution, as necessary.

II. Scope

This policy applies to all elected officials, employees, contractors, vendors, and third parties who access or manage the Village's technology resources, including but not limited to:

- Village-owned computers, servers, and mobile devices;
- Cloud services and hosted applications;
- Networks and telecommunications systems; and
- Sensitive or confidential data (e.g., personally identifiable information, financial records, law enforcement records, health-related information, or other protected data).
- The Village should apply best efforts to maintain contracts with cybersecurity clauses and breach notification requirements that comport with this cybersecurity policy.

III. Roles and Responsibilities

- Village Council: Approves the cybersecurity policy and ensures resources are allocated;
- Village Administrator: Oversees policy implementation, coordinates with IT providers, and consults with legal counsel as needed;
- IT Provider (Vendor): Implements technical safeguards, monitors for threats, and reports incidents;
- Employees/Users: follow cybersecurity protocols, complete training, and report suspicious activity;
- Vendors: Must comply with the Village's cybersecurity standard.

IV. Ransomware Payment Restrictions Policy

Purpose:
To ensure that ransomware payment decisions comply with Ohio HB 96 by requiring formal approval from the legislative authority, fostering transparency and accountability before any ransom payment is made.

Scope:
This policy applies to all ransomware incidents impacting the Village of Lockland, including any demand for payment to regain access to data, prevent data disclosure, or mitigate a ransomware attack.

Policy:

1. **Prohibition on Unauthorized Payments:**
    - No ransom payment or compliance with a ransom demand shall be made without the prior formal approval of the organization's legislative authority (e.g., board of education, city council, or other governing body).
2. **Legislative Approval Requirement:**
    - Approval must be obtained through a formal resolution or ordinance passed by the legislative authority.
    - The resolution or ordinance must explicitly state the specific reasons for complying with the ransom demand and explain why such compliance is in the best interest of the organization and its constituents.
3. **Emergency Meetings:**
    - In urgent cases, the legislative authority may call an emergency meeting with less than 24 hours' notice per Ohio Revised Code 121.22(F) to expedite decision-making in response to a ransomware attack.
4. **Documentation and Transparency:**
    - All decisions regarding ransomware payments, including meeting minutes and resolution texts, must be documented and retained as part of the organization's official records.
    - The rationale for the ransom payment decision should be clearly articulated to ensure accountability and transparency.
5. **Coordination with Incident Response:**
    - The organization's cybersecurity incident response team shall inform the legislative authority promptly about any ransomware incident and assist in preparing necessary information for decision-making.
6. **Compliance and Training:**
    - Relevant personnel and governing body members shall receive annual training on ransomware risks, response procedures, and compliance requirements under Ohio HB 96.

Compliance:
Non-compliance with this policy may result in legal penalties and increased organizational risk. This policy ensures adherence to Ohio HB 96 and supports prudent, transparent management of ransomware incidents.

II. Incident Reporting Policy for Cybersecurity Incidents

Purpose:
To establish clear procedures for reporting cybersecurity and ransomware incidents as required by Ohio House Bill 96, ensuring timely notification to state authorities and adherence to state law.

Scope:
This policy applies to all employees, contractors, and third parties who identify or become aware of a cybersecurity or ransomware incident affecting the Village of Lockland.

Policy:

1. **Incident Identification and Initial Response:**
    - All suspected or confirmed cybersecurity incidents must be immediately reported to the designated Incident Response Team (IRT) or IT Security Coordinator.
2. **Reporting to Ohio Cyber Integration Center (OCIC):**
    - Within **7 calendar days** of discovering the incident, the IRT must notify the Ohio Cyber Integration Center (OCIC), part of the Ohio Department of Homeland Security.
    - Notification will include completing the OCIC intake form, providing details such as organization contact information, incident date/time, incident type, mitigation steps taken, affected devices, cyber insurance status, and other relevant details.
    - Contact OCIC via phone at 614-387-1089 or email at OCIC@dps.ohio.gov.
3. **Reporting to Ohio Auditor of State:**
    - Within **30 calendar days** of discovering the incident, a full incident report must be submitted to the Ohio Auditor of State's office.
    - This report will use the standardized cybersecurity reporting form provided by the Auditor of State and be submitted via email to Cyber@ohioauditor.gov.
4. **Confidentiality and Recordkeeping:**
    - All incident reports, related documents, and communication with OCIC and the Auditor of State are confidential and exempt from public records requests as per Ohio Revised Code § 9.64.
    - The organization shall retain all incident documentation securely for auditing and compliance purposes.
5. **Coordination and Follow-Up:**
    - The IRT will coordinate with OCIC for any follow-up actions, forensics, and response activities as may be requested.

- Lessons learned and final disposition reports shared by OCIC will be reviewed for improving the organization's cybersecurity posture.

Compliance:
Failure to comply with these reporting requirements may result in legal penalties and increased cyber risk to the organization. All staff must receive annual training on cybersecurity incident reporting policies.

III. SECURITY CONTROLS POLICY

The Village incorporates by reference the publication referred to as, "CIS Critical Security Controls®," Version 8.1, dated March, 2025.