

North Lewisburg Village Cyber Security Policy Resolution No. 3/10/2026

1. Purpose.

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and security of the Village of North Lewisburg Ohio information systems, data and technology resources in compliance with Ohio Revised Code (ORC) 9.64 cyber security requirements.

2. Scope.

This policy applies to all employees and elected officials who access or manage the Village of North Lewisburg's technology resources, including but not limited to:

- Sensitive or confidential data, personal identifiable information, financial information, and other protected records.
- Computers, servers.
- Cloud services and hosted applications.
- Networks, Telecommunications Systems, including Village owned cellular devices.

3. Policy Statement

The Village of North Lewisburg is committed to safeguarding its information systems against cyber security threats and ensuring compliance with ORC 9.64 by:

- Establishing baseline security practices.
- Providing employees with ongoing cyber security training and awareness.
- Preparing for detection, response, and recovery incidents.
- Reviewing and updating cyber security policy on an annual basis.

4. Roles and Responsibilities.

- The Village of North Lewisburg: Approves cyber security policy and ensures resources are allocated.
- The Village administrator and Fiscal Officer oversee policy implementation, manages an I.T. provider, and seeks the opinion of legal counsel on cyber security matters.
- The Village Administrator will employ or contract with an I.T. provider(s) to implement technical safeguards and to monitor, quarantine, and repair threats.
- Employees: follow cyber security protocols, complete annual training, and report any suspicious activity immediately.

5. Cybersecurity Controls

5.1 Access Controls

- Requires unique user id's and strong passwords.
- Enforced by multi factor authentication (MFA) for remote and administrative access.
- Limit access to sensitive data on a role-based basis.
- Access to personal email shall not be made on Village devices.

5.2 Network and System Security

- Maintains up to date firewalls, antivirus, intrusion detection, prevention, log in restrictions for users, and BitLocker encryption or equivalent.
- Maintains and applies daily software patches and updates.
- Maintains segregation of critical systems, including scada, from public access networks.
- Maintain user data backup system with encryption.
- Power down unused computers nightly and on the weekends, unless its operation is sensitive in nature such as Scada.

5.3 Data Protection

- Continue to encrypt all sensitive data at rest or in transit with BitLocker or equivalent.
- Continue to regularly back up data and test restoration procedures.
- Continue to retain records according to The Villages record retention schedule.

5.4 Incident Response

- The Village Administrator will be responsible for leading incident response. The Fiscal Officer will be the lead in the administrator's absence.
- In the event of a cyber security incident the affected employee will notify the Village Administrator immediately or the fiscal Officer in the Administrators absence.
- In the event of a cyber security incident the Village Administrator or The Fiscal Officer in the Administrator's absence will notify the executive director of the Department of homeland security within 7 days of the discovery of the event, and the Auditor of State within 30 days. 9.64(D)(1) and (2).

5.5 Post Response

- Following the detection and reporting of a cyber security incident the Village Administrator or Fiscal Officer in the administrator's absence shall conduct a post-incident review to establish procedures to repair the damaged infrastructure and to mitigate future cyber incidents.

6. Cybersecurity Training

- The Village of North Lewisburg requires all employees to complete a minimum of one hour of annual cyber security awareness training.

7. Ransom Policy

- It is The Policy of The Village of North Lewisburg that no ransom will be paid to release seized or stolen data from a cyber security attack.

8. Ethical Safeguards

- Village employees must only access work related trusted websites. If an email is in doubt check the sender's address. Employees should never open unverified or unexpected attachments. When in doubt call the sender or contact administration.

9. Vendor Management

- The Village requires that all vendors emailing or accessing the Villages computer or data systems comply with the State of Ohio's cyber security standards.

10. Compliance and Review

This policy will be reviewed and updated annually to reflect changes in technology, law, and Village needs.

11. Enforcement

-Violation of this cyber policy may result in disciplinary action or termination. As well as potential civil and criminal penalties in accordance with applicable law.

12. Privacy

12.1-No expectation of privacy.

-When an employee uses a Village computer, technology, or network there is no expectation of privacy in their activity or stored files.

-The Village of North Lewisburg reserves the right for the appropriate administrator to monitor all Village owned networks, computers, and equipment at any time.

-Police Files will be monitored solely by The Police Chief or Mayor in Chiefs absence.

-The remaining departments will be monitored by The Village Administrator, Fiscal Officer, and/or Mayor.

Vote 6-0 Yes 6 No 0 Abstain 0



Mayor-Ted Murphy Jr.

Date 05/12/2026



Clerk of Council-Alicia Davis

Date 5/12/2026



Council President-Matt Warner

Date 05/12/2026

Reading 1 - 3-10-26
Reading 2 4-14-26
Reading 3 5-12-26