RESOLUTION NO. 104-2025

Adopting a Cybersecurity Policy

Cuyahoga County, Ohio

Be it Resolved *by the Township Trustees of Olmsted Township, that*

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 by September 30, 2025; 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 Olmsted Township Board of Trustees recognizes the importance of safeguarding sensitive and confidential information entrusted to Olmsted Township; and

WHEREAS, a draft Cybersecurity Policy has been prepared and reviewed by Township staff and is recommended for adoption as a 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 vendor management, while requiring consultation with IT professionals and legal counsel for implementation and customization;

NOW, THEREFORE, BE IT RESOLVED by the Board of Trustees of Olmsted Township, Cuyahoga County, Ohio, that:

1. The attached Cybersecurity Policy is hereby adopted as the official cybersecurity policy of Olmsted Township.
2. This policy shall take effect immediately, with adoption required by September 30, 2025, and implementation of technical and training requirements no later than June 30, 2026, as provided by the Ohio Auditor of State.
3. The Board of Trustees shall distribute the adopted policy to all Township departments, employees, and relevant contractors, and shall ensure compliance in partnership with IT providers and legal counsel.
4. This resolution shall be in full force and effect upon its passage and adoption by the Olmsted Township Board of Trustees.

BE IT FURTHER RESOLVED; that it is hereby found and determined that all formal actions of this Board of Township Trustees concerning and relating to the adoption of this Resolution were adopted in an open meeting of this Board, and that all deliberations of this Board and any of its committees that resulted in such formal action, were in a meeting open to the public, in compliance with all legal requirements, including Section 121.22 of the Ohio Revised Code.

Adopted the 2ND *day of* OCTOBER, *2025*

Attest: _____
Township Fiscal Officer

_____
_____
_____
Township Trustees

Olmsted Township
On the Grow
EST. 1814

7900 Fitch Road, Olmsted Township, OH 44138
Phone Number: 440-235-3051 info@olmstedtownship.org

MEMORANDUM

TO: **Trustees Lisa Zver, Trustee Tom Cole, Trustee Riley Alton**
FROM: **Township Administrator, Gary Yelenosky**
DATE: **September 29th, 2025**
RE: **Cybersecurity Policy**

Disclaimer

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

Purpose

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of Olmsted Township's information systems, data, and technology resources in compliance with R.C. §9.64 cybersecurity requirements.

Scope

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

- Township-owned computers, servers, and mobile devices
- Cloud services and hosted applications
- Networks and telecommunications systems
- Sensitive or confidential data (e.g., personally identifiable information, financial records, law enforcement records, health-related information, or other protected data)

Policy Statement

Olmsted Township is committed to safeguarding its information systems against cybersecurity threats and ensuring compliance with R.C. §9.64 by:

- Establishing baseline cybersecurity practices
- Providing ongoing cybersecurity awareness training
- Preparing for detection, response, and recovery from incidents
- Reviewing and updating cybersecurity policies annually

Olmsted Township
On the Grow
EST. 1814
7900 Fitch Road, Olmsted Township, OH 44138
Phone Number: 440-235-3051 info@olmstedtownship.org

Roles and Responsibilities

- **Board of Trustees**: Approves the cybersecurity policy and ensures resources are allocated.
- **Township 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.

Cybersecurity Controls

Access Control

- Require unique user IDs and strong passwords
- Enforce multi-factor authentication (MFA) for remote or administrative access
- Limit access to sensitive data on a "least privilege" basis

Network and System Security

- Maintain up-to-date firewalls, antivirus software, and intrusion detection/prevention tools
- Apply security patches and updates within 30 days of release
- Segregate critical systems from public networks whenever possible

Data Protection

- Encrypt sensitive data at rest and in transit
- Regularly back up critical data and test restoration procedures
- Retain records according to Ohio records retention schedules

Incident Response

- Designate an Incident Response Lead
- Establish procedures for detecting, reporting, and escalating incidents
- In the event of a cybersecurity incident, Olmsted Township will notify the following parties:
    1. The executive director of the division of homeland security within the Department of Public Safety, as soon as possible but not later than seven days after discovery of the incident

2. The Auditor of State, as soon as possible but not later than thirty days after discovery of the incident
3. Any other parties as required by law

- Conduct a post-incident review and update policies as needed
- Establish procedures for repair and ongoing maintenance of infrastructure after a cybersecurity incident

Training and Awareness

- Require all employees to complete cybersecurity awareness training annually
- Provide role-specific training for IT administrators and staff handling sensitive data

Vendor and Third-Party Management

- Require vendors to comply with Olmsted Township's cybersecurity standards
- Maintain contracts with cybersecurity clauses and breach notification requirements

Compliance and Review

- This policy will be reviewed annually and updated to reflect changes in technology, law, and organizational needs
- Departments and third-party IT providers must submit evidence of compliance to the Township Administrator annually

Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, as well as potential civil and criminal penalties in accordance with applicable law.

Effective Date

This policy takes effect on September 30, 2025, to meet the requirements of R.C. §9.64. Implementation of technical and training requirements must be completed no later than June 30, 2026.