SPRINGFIELD TOWNSHIP TRUSTEES
LUCAS COUNTY, OHIO

RESOLUTION 25-028

ADOPTING A CYBERSECURITY POLICY

The Board of Trustees of Springfield Township, Lucas County, Ohio met in Special Session on September 25, 2025, at 7617 Angola Road, Holland, Ohio, with the following members present:

Tom Anderson Jr., Andrew Glenn, and Rachel Geiger

Tom Anderson Jr. moved the adoption of the following Resolution:

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 risk; and

WHEREAS, Springfield Township recognizes the importance of safeguarding sensitive and confidential information entrusted to Springfield Township; and

WHEREAS, a draft Cybersecurity Policy has been prepared and reviewed by 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 Springfield Township Board of Trustees, Lucas County, Ohio, that:

Section 1: The attached Cybersecurity Policy is hereby adopted as the official policy of Springfield Township.

Section 2: This policy shall take effect immediately, with the 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.

Section 3: The Board of Trustees shall distribute the adopted policy to all township departments, employees, and relevant contractors, and to ensure compliance in partnership with IT providers and legal counsel.

Section 4. This resolution shall be in full force and effect upon its passage and adoption by Springfield Township Board of Trustees.

SPRINGFIELD TOWNSHIP TRUSTEES
LUCAS COUNTY, OHIO

RESOLUTION 25-028

ADOPTING A CYBERSECURITY POLICY

Andrew Glenn seconded the motion and roll resulted as follows:

Tom Anderson Jr. YES Andrew Glenn YES Rachel Geiger YES

Rachel Geiger, Trustee

Andrew Glenn, Trustee

Tom Anderson Jr., Trustee

ATTEST:

Brenna Koback, Fiscal Officer
September 25, 2025, Special Trustee Meeting

SPRINGFIELD TOWNSHP CYBER SECURITY POLICY

1. Purpose

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

2. Scope

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

- Computers, servers, and mobile devices
- Cloud services and hosted applications
- Networks and telecommunications systems
- Sensitive or confidential data (PII, financial, law enforcement, health related, or other protected records)

3. Policy Statement

Springfield 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

4. Roles and Responsibilities

- *Board of Trustees*: Approves cybersecurity policy and ensures resources are allocated.
- *Administrator*: Oversees policy implementation, coordinates with IT providers and legal counsel.
- *IT Provider*: Implements technical safeguards, monitors for threats, and reports incidents.
- *Employees/Users*: Follow cybersecurity protocols, complete training, and report suspicious activity.

5. **Cybersecurity Controls**
    a. ***Access Control***
        - Require unique user ID's and strong passwords
        - Enforce multi-factor authentication (MFA) for remote or administrative access.
        - Limit access to sensitive data on a "least privilege" basis.
    b. ***Network and System Security***
        - Maintain up-to-date firewalls, antivirus, and instruction detection/prevention.
        - Apply software patches and updates within 30 days of release.
        - Segregate critical systems from public networks when possible.
    c. ***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.
    d. ***Incident Response***
        - Designate an Incident Response Lead
        - Establish procedures for detecting, reporting, and escalating incidents.
        - In the event of a cybersecurity incident, notify the following parties in manner listed:
            - The executive director of the division of homeland security with the department of public safety, in a manner prescribed by the executive director, as soon as possible but not later than seven days after the political subdivision discovers the incident.
            - The auditor of state, in a manner prescribed by the auditor of state, as soon as possible but not later than thirty days after the political subdivision discovers the incident.
            - Any other parties as required by law.
        - Conduct a post-incident review and update policies as needed.
        - Establish procedures for the repair and subsequent maintenance of infrastructure after a cybersecurity incident.
    e. ***Training and Awareness***
        - Require all employees to complete cybersecurity awareness training annually
        - Provide role-specific training for staff handling sensitive data.
    f. ***Vendor and Third-Party Management***
        - Require vendors to comply with Springfield Township's cybersecurity standards.

- Maintain contracts with cybersecurity clauses and breach notification requirements.

6. **Compliance and Review**
   - This policy will be reviewed annually and updated to reflect changes in technology, law, and organizational needs.
   - Departments and IT providers must submit evidence of compliance to the Administrator.

7. **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.

8. **Effective Date**
   - This policy takes effect September 30, 2025, to meet R.C 9.64 requirements. Implementation of technical requirements must be completed no later than June 30, 2026.