Brown Township, Franklin County Cybersecurity Policy

1. Purpose

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of Brown 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 Brown 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 (e.g., PII, financial, law enforcement, health-related, or other protected records)

3. Policy Statement

Brown 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/Manager: Oversees policy implementation, coordinates with IT providers and legal counsel.
- IT Provider (Internal or Vendor): Implements technical safeguards, monitors for threats, and reports incidents.
- Employees/Users: Follow cybersecurity protocols, complete training, and report suspicious activity.

5. Cybersecurity Controls

5.1 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.

5.2 Network and System Security

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

5.3 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.

5.4 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 the manner listed:
    (1) The executive director of the division of homeland security within 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;
    (2) 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.
    (3) 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.

5.5 Training and Awareness

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

5.6 Vendor and Third-Party Management

- Require vendors to comply with Brown 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 third-party IT providers must submit evidence of compliance to the Administrator/Manager annually.

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

10/3/2025