RECORD OF PROCEEDINGS

Minutes of Brown Township Trustees Meeting

Held September 30, 2025

The Brown Township Trustees met on this date at 2:30 PM in special emergency form with Trustees Miley and Skinner, Fiscal Officer Barrett.

Trustee Skinner called the meeting to order at 2:30 pm.

Trustee Skinner made the motion to adopt Ohio Revision Code 9.64, enacted through HB 96 to implement a Brown Township, Cyber Security policy. Trustee Miley seconded. Motion Passed.

RESOLUTION 2025-09-30-01 TO APPROVE BROWN TOWNSHIP TO ADOPT THE OHIO REVISION CODE 9.64, ENACTED THROUGH HB 96 TO IMPLEMENT A CYBER SECURITY POLICY.

Skinner Aye Miley Aye

Trustee Skinner made a motion to adjourn the meeting. Trustee Miley seconded. Motion passed. Meeting adjourned at 2:36 pm.

Heather Barrett Trustees

Heather Barrett, Fiscal Officer

Connie Skinner

Connie Skinner, Chairperson

Charles A Miley

Charles Miley, Vice Chairperson

Brown Township, Delaware County
Cybersecurity Policy

Disclaimer:
This document is provided as a cybersecurity policy to assist Ohio townships in meeting the requirements of R.C. §9.64, as provided in Ohio HB 96 (136th G.A.). It does not constitute legal advice. Townships should consult with legal counsel and IT professionals to adapt this policy to their specific environment, risks, and compliance needs.

---

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 [Entity Name]'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.**

RESOLUTION 2025- 09-30-01

RESOLUTION ADOPTING A CYBERSECURITY POLICY

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, Brown Township recognizes the importance of safeguarding sensitive and confidential information entrusted to Brown 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 [Board of Trustees of Brown Township, Delaware County, Ohio, that:

1. The attached **Cybersecurity Policy** is hereby adopted as the official policy of Brown 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 to 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 Brown Township Board of Trustees.

PASSED AND ADOPTED this 30 of September 2025.

Heather Barrett Date 9.30.25

Heather Barrett, Fiscal Officer

9.30.25

Connie Skinner, Chairperson Connie Skinner

Charles A Miley

Charles Miley, Trustee

Gary Stegner, Trustee

Cybersecurity Policy
Executive Summary

Disclaimer: This summary is provided for guidance only. It is not legal advice. Each jurisdiction should work with legal counsel and IT staff to finalize and implement cybersecurity policies.

Why This Policy Matters
Ohio Revised Code Section 9.64, enacted through HB 96, requires every jurisdiction to have a cybersecurity policy in place by **September 30, 2025**, with full implementation by **June 30, 2026**. This policy helps protect our community's data, technology, and public services from cyber threats.

Who Drafted the Policy
VC3 is the nation's largest IT firm dedicated to local government organizations, proudly serving over 1,200 counties, cities, towns, townships, and villages across the United States. In addition to providing full-service managed security solutions (MSSP) with certified security officers on staff, VC3 operates as a true 24/7/365 partner, with live in-house staff (never outsourced) ready to support clients at any hour, day or night. For more information, please visit https://www.vc3.com or contact Senior Account Executive, Randy Allen, at 800-787-1160 ext. 8205.

Our Commitment
We are committed to:

- Protecting sensitive data (financial, personal, law enforcement, and health records).
- Training staff to recognize and prevent cyber risks.
- Responding quickly to cybersecurity incidents.
- Partnering with IT providers and vendors to keep systems secure.

Key Practices

- **Strong Passwords & MFA:** Everyone uses secure passwords; remote access requires extra login security.
- **System Protection:** Firewalls, antivirus software, and regular updates are required.
- **Data Backup:** Important files are backed up and can be restored if needed.
- **Incident Response:** A process is in place to report and respond to cybersecurity events.
- **Annual Training:** All employees receive cybersecurity awareness training.
- **Vendor Oversight:** Contractors and vendors must follow our cybersecurity standards.

Who is Responsible?

- **Board of Trustees:** Approves policy and provides oversight.
- **Administrator/Manager:** Ensures implementation and coordinates with IT.
- **Employees:** Follow safe practices and report suspicious activity.
- **IT Provider:** Maintains systems, applies security controls, and responds to incidents.

Timeline

- **Policy Adoption Deadline:** September 30, 2025
- **Full Implementation Deadline:** June 30, 2026

RESOLUTION 2025-09-30-01

RESOLUTION ADOPTING A CYBERSECURITY POLICY

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, Brown Township recognizes the importance of safeguarding sensitive and confidential information entrusted to Brown 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 [Board of Trustees of Brown Township, Delaware County, Ohio, that:

1. The attached **Cybersecurity Policy** is hereby adopted as the official policy of Brown 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 to 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 Brown Township Board of Trustees.

PASSED AND ADOPTED this 30 of September 2025.

Heather Barrett Date 9.30.25

Heather Barrett, Fiscal Officer

9.30.25

Connie Skinner, Chairperson Connie Skinner

Charles A Miley

Charles Miley, Trustee

Gary Stegner, Trustee