The Township of Hamilton, Warren County, Ohio Board of Trustees met in regular session on April 1, 2026, at 6:00 p.m. at Hamilton Township, Warren County, Ohio, with the following Trustees present:

Mark Sousa – Trustee, *Board Chairman*
Darryl Cordrey – Trustee, *Vice Chairman*
Joe Rozzi – Trustee

Mr. Sousa presented the following Resolution and moved its adoption:

HAMILTON TOWNSHIP, WARREN COUNTY, OHIO
RESOLUTION NUMBER 26-0401C

A RESOLUTION APPROVING A CYBERSECURITY POLICY FOR HAMILTON TOWNSHIP

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

WHEREAS, a draft Cybersecurity Policy has been prepared and reviewed by Township staff and legal counsel 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 Hamilton Township, Warren County, Ohio that:

SECTION 1. The attached Cybersecurity Policy is hereby adopted as the official policy of Hamilton Township.

SECTION 2. The Board of Trustees shall distribute the adopted policy to all Township departments, employees, and relevant contractors, and ensure compliance in partnership with IT providers and legal counsel.

SECTION 3. This Resolution shall be in full force and effect upon its passage and adoption by the Hamilton Township Board of Trustees.

Mr. Cordrey seconded the Resolution and the following being called upon the question of its adoption, the vote resulted as follows:

Mark Sousa–	Aye ✓	Nay _____
Darryl Cordrey–	Aye ✓	Nay _____
Joseph P. Rozzi –	Aye ✓	Nay _____

Resolution adopted this 1st day of April, 2026.

Attest:

Leah Elliott

Leah M. Elliott, Fiscal Officer

Approved as to form:

Sarah J. Sparks

~~Benjamin Yoder,~~ *Law Director*
Sarah J. Sparks, Assistant

I, Leah M. Elliott, Fiscal Officer of Hamilton Township, Warren County, Ohio, hereby certify that this is a true and accurate copy of a Resolution duly adopted by the Board on April 1, 2026.

Date: 4/1/2026

Leah Elliott

Leah M. Elliott, Fiscal Officer

Hamilton Township Cybersecurity Program & Policy

Ohio Revised Code 9.64 (enacted via Ohio HB 96)

Draft – Editable working document (for internal review and Board adoption).

Document Control

Field	Value	Field	Value
Version	0.9	Prepared by	Titan Tech, LLC
Effective Date	TBD	Approved by	Board of Trustees
Last Review Date	TBD	Next Review	October 2026
Document Owner	Jeff Wright	Incident Response Lead	Jeff Wright

1. Purpose

This policy establishes Hamilton Township's cybersecurity program to protect the confidentiality, integrity, and availability of Township information, systems, and technology resources, and to meet the requirements of Ohio Revised Code 9.64.

2. Scope

This policy applies to all Township trustees, officials, employees, contractors, and volunteers who use or access Township technology resources.

Township technology resources include endpoints, servers, networks, cloud services, email, VPN/remote access, backups, and any systems that store or process Township data.

3. Governance and Ownership

Hamilton Township will designate program ownership, operational leadership, and technical responsibilities to ensure accountability and timely decision-making.

3.1 Ownership Matrix (Fill In)

Role	Responsibilities (Summary)	Assigned To (Name/Title)
Board of Trustees (Legislative Authority)	Adopt program; approve major exceptions; approve any ransomware payment action by resolution.	Mark Souza
Program Owner	Maintain policy; ensure annual review; ensure training; coordinate reporting	Jeff Wright

	obligations.	
Incident Response Lead	Coordinate incident response, communications, and key decisions during an incident.	Jeff Wright
Technical Owner / IT Provider (Titan Tech)	Implement and operate controls; monitor; respond; maintain evidence; support reporting.	Titan Tech – 513-400-4072
All Users	Follow policy; complete training; report suspicious activity immediately.	All Township users

4. Cybersecurity Program Structure

Hamilton Township's cybersecurity program follows generally accepted best-practice functions and is implemented through Township procedures and managed technical controls provided by its IT provider (Titan Tech).

Identify:

- Maintain an inventory of key systems/services (endpoints, servers, Microsoft 365, VPN/remote access, backups, key vendors).
- Identify mission-critical services and where sensitive data is stored.
- Provide the technology inventory to the Program Owner by the end of September each year (annually).

Protect:

- Enforce strong identity controls (Microsoft 365 SSO + MFA) and least privilege (AutoElevate for elevation; 2FA for admin access).
- Protect endpoints with SentinelOne and managed oversight via Huntress MDR.
- Harden email and remote access (SPF/DKIM/DMARC; secure VPN remote access with Microsoft 365 SSO + MFA).

Detect:

- Monitor endpoints/servers via Huntress MDR and SentinelOne alerting.
- Monitor Microsoft 365 activity and account compromise indicators via SaaS Alerts.
- Ensure staff reporting channels are clear and acted on promptly.

Respond:

- Triage/contain incidents, preserve evidence, remediate root cause, and document actions.
- Meet Ohio reporting deadlines (7-day DPS/Homeland Security; 30-day Auditor of State).

- Escalate ransomware decisions per governance requirements (Board resolution for any payment/compliance).

Recover:

- Restore from known-good backups and validate integrity before returning systems to service.
- Maintain layered recovery (M365 backups; on-site Veeam BDR not domain-joined; offsite copies; CrashPlan file-level backups secured with 2FA).
- Perform restore testing (recommended quarterly) and apply lessons learned after incidents.

5. Implemented Controls (Current Environment)

5.1 Endpoint Protection and Threat Response

SentinelOne antivirus is deployed for endpoint protection. Huntress MDR provides managed detection and response (MDR), threat hunting, and escalation of suspicious activity.

5.2 Identity, Authentication, and Privileged Access

Multi-factor authentication (MFA) is required for all Microsoft 365 accounts. SaaS Alerts is used to detect and alert on suspicious Microsoft 365 activity and potential unauthorized access. AutoElevate is used for privileged access management and requires 2FA for administrative login.

5.3 Secure Remote Access

A secure VPN solution is used for remote access. The VPN service is self-hosted on a cloud server hosted and maintained by Titan Tech and authenticates via Microsoft 365 single sign-on (SSO) with multi-factor authentication (MFA).

5.4 Email Domain Protection

SPF, DKIM, and DMARC are implemented for Township email domains to reduce spoofing and improve delivery integrity.

5.5 Backup, Disaster Recovery, and Ransomware Resilience

Nightly backups are stored to a server secured at Titan Tech's office and not directly accessible from the internet.

A Backup and Disaster Recovery (BDR) server runs Veeam Backup & Replication. The BDR server is not joined to the domain and uses unique credentials. Backups and replicas are written to local drives and copied offsite to Titan Tech's secured data center.

5.6 Security Awareness and Phishing Simulation

All Township staff receive security awareness training. Monthly managed phishing simulations are conducted and tracked for follow-up training where needed.

6. Minimum Control Standard

Hamilton Township will maintain, at minimum, the following baseline controls unless documented exceptions are approved with compensating safeguards:

MFA for email/cloud access, remote access, and administrative functions.

Endpoint protection and MDR monitoring on supported systems.

Patch management and vulnerability remediation processes.

Backups with restricted access and offsite copies; restore testing at an established cadence.

Email anti-spoofing controls (SPF/DKIM/DMARC).

Security awareness training and phishing simulations.

Least privilege access controls and vendor access governance.

7. Incident Response and Mandatory Reporting (R.C. 9.64)

7.1 Internal Reporting

All users must report suspected cybersecurity incidents immediately to the Incident Response Lead and/or Program Owner, and to the Technical Owner (IT provider).

7.2 Minimum Incident Handling Steps

Triage and classify severity.

Contain (isolate systems, disable accounts, block indicators).

Preserve evidence (logs, timelines, affected systems/users).

Eradicate and remediate (remove persistence, patch, credential resets).

Recover (restore from known-good backups; validate).

Post-incident review with corrective actions.

7.3 External Reporting Deadlines

Upon discovery of a cybersecurity incident or ransomware incident, Hamilton Township will notify:

Ohio Department of Public Safety / Division of Homeland Security: as soon as possible, but no later than 7 days after discovery.

Ohio Auditor of State: as soon as possible, but no later than 30 days after discovery.

Any additional parties required by law, contract, or cyber insurance.

7.4 Ransomware Payment Restriction

Hamilton Township will not pay a ransom or comply with a ransomware demand unless the Board of Trustees approves such action by resolution stating why payment/compliance is in the Township's best interest. In the event of a ransomware incident (or any incident reasonably suspected to involve extortion), the Township will promptly notify and engage its cyber insurance carrier, and will follow the carrier's required incident response procedures, including any insurer-led or insurer-approved forensic investigation and claims workflow, in coordination with the Township's Incident Response Lead, IT provider, and legal counsel as appropriate.

8. Training and Awareness

All staff will complete cybersecurity awareness training at least annually. Role-based training will be provided where appropriate (e.g., finance, administrators, privileged users). Monthly managed phishing simulations will be conducted and tracked.

9. Third-Party and Vendor Security

Vendors with access to Township systems or data should be required to use MFA where feasible, use least privilege access, and notify the Township of cybersecurity incidents affecting Township data or services.

10. Policy Maintenance, Exceptions, and Review

This policy will be reviewed at least annually and updated as required. Exceptions must be documented, time-bounded where feasible, and include compensating controls.

11. Enforcement

Violations of this policy may result in disciplinary action and/or contract remedies, and may carry civil or criminal consequences.

Appendix A – Incident Reporting Checklist (Fill In)

Use this checklist during an incident. Keep specific reporting methods (emails/URLs/forms) current in this appendix.

[ ] Record discovery date/time and who discovered the incident.

[ ] Identify impacted systems, accounts, and locations.

[ ] Preserve evidence (screenshots, ransom note, logs, affected user list).

[ ] Contain (isolate systems, disable accounts, block indicators).

[ ] Notify Incident Response Lead / Program Owner / IT Provider.

[ ] Start the 7-day and 30-day external reporting clocks.

[ ] Document recovery steps and restore validation.

[ ] Complete post-incident review and corrective actions.

Appendix B – Board Resolution Template (Ransomware Payment)

NOTE: The Township should consult legal counsel before adopting any resolution related to ransomware payment.

Resolution No. _____

A RESOLUTION AUTHORIZING PAYMENT OR COMPLIANCE WITH A RANSOMWARE DEMAND

WHEREAS, Hamilton Township experienced a ransomware incident on _____; and

WHEREAS, the Board of Trustees finds that payment/compliance is in the Township's best interest for the following reasons:

- _____
- _____

NOW, THEREFORE, BE IT RESOLVED that the Board of Trustees authorizes the following action:

_____

Adopted this ____ day of _____, 20___.

_____ (Chair)

_____ (Trustee)

_____ (Trustee)

Attest: _____ (Fiscal Officer)