BOARD OF TRUSTEES
JEFFERSON TOWNSHIP, MONTGOMERY COUNTY, OHIO
RESOLUTION NO. 26-122

THE JEFFERSON TOWNSHIP BOARD OF TRUSTEES APPROVES THE CYBERSECURITY POLICY

The Board of Trustees of Jefferson Township, Montgomery County, Ohio, met in a regular meeting on September 1, 2026, at 6:00 pm at the Township Offices located at 1 Business Park Dr., Dayton, Ohio, with the following members present:

Oscar Young (Y) **Sheila Back** (Y) **Vera Powell** (Y)

Moved by: **Young** (X) **Back** ( ) **Powell** ( )
Second by **Young** ( ) **Back** ( ) **Powell** (X)

WITNESSETH

WHEREAS, Ohio Revised Code § 9.64 requires the legislative authority of each political subdivision to adopt a cybersecurity program that safeguards the subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity; and

WHEREAS, the cybersecurity program must be consistent with generally accepted cybersecurity practices and must address the Township's critical functions and risks, potential impacts of a breach, threat detection, incident communication and containment, infrastructure repair and continuing security, and employee cybersecurity training; and

WHEREAS, cybersecurity program and framework records and cybersecurity incident reports are not public records under ORC § 9.64(E), and certain cybersecurity procurement and technology records are security records under ORC § 9.64(F);

NOW, THEREFORE, BE IT RESOLVED by the Board of Trustees of Jefferson Township, Montgomery County, Ohio:

SECTION 1. The Board adopts the Jefferson Township Cybersecurity Program attached to this resolution pursuant to ORC § 9.64.

SECTION 2. The Township Administrator is authorized and directed to implement and administer the program, maintain its restricted operational provisions, require training, coordinate incident response and reporting, and make administrative updates that do not materially reduce Board-adopted controls or alter powers reserved to the Board.

SECTION 3. The Program Administrator shall ensure that the Policy and supporting program are reviewed at least annually and after a material cybersecurity incident or significant legal, operational, vendor, or technology change.

SECTION 4. No person acting on behalf of Jefferson Township may pay or otherwise comply with a ransom demand unless the Board formally approves the payment or compliance by a separate resolution that specifically states why the action is in the best interest of Jefferson Township.

BOARD OF TRUSTEES
JEFFERSON TOWNSHIP, MONTGOMERY COUNTY, OHIO
RESOLUTION NO. 26-122

SECTION 5. This resolution shall take effect immediately upon adoption.

The vote was as follows:

Oscar Young			**Sheila Back**			**Vera Powell**		
Yes	No	Abstain	Yes	No	Abstain	Yes	No	Abstain

Adopted: 1st day of September 2026

Signed by:

Oscar Young, President

Vera Powell, Trustee

Sheila Back, Vice President

Attest to Trustees Signatures:
Adrennia Kelly, Fiscal Officer

Jefferson Township

Cybersecurity Policy (HB96 Compliant & NIST-Aligned)

1. Purpose

Jefferson Township is committed to safeguarding the confidentiality, integrity, and availability of Township information systems in accordance with **Ohio House Bill 96 (HB96)** and recognized cybersecurity best practices.
This policy establishes the required controls, responsibilities, and processes that ensure the Township maintains a secure and compliant technology environment.

2. Scope

This policy applies to:

- All Township employees, contractors, volunteers, and elected officials
- All Township-owned or managed information systems, networks, and data
- All remote access mechanisms, cloud services, and connected devices

3. Governance & Framework Alignment

Jefferson Township adopts the **NIST Cybersecurity Framework (CSF)** as its guiding model. Controls and processes described in this policy map directly to the NIST CSF core functions:

1. **Identify**
2. **Protect**
3. **Detect**
4. **Respond**
5. **Recover**

4. Cybersecurity Controls (Current HB96 Compliance)

4.1 Identify (ID)

The Township will:

- Maintain an inventory of systems, applications, and network-connected devices.
- Classify Township data according to sensitivity and regulatory requirements.
- Document roles and responsibilities for cybersecurity management.

- Conduct risk assessments as required by HB96 and when environmental or operational changes occur.

4.2 Protect (PR)

4.2.1 Endpoint Protection

Jefferson Township uses a **Managed Endpoint Detection & Response (EDR)** platform to protect all Township-owned computers and servers.

- EDR provides real-time threat detection, behavioral analysis, and automated response capabilities.
- All endpoints must remain enrolled in EDR unless explicitly approved by IT.

4.2.2 Security Operations Center (SOC – 24×7 Monitoring)

The Township utilizes a **Managed SOC service** that provides:

- 24×7 monitoring of security alerts
- Event correlation and threat intelligence
- Rapid investigation of suspicious activity
- Escalation to Township IT for confirmed security issues

4.2.3 Email Security & Filtering

All Township email accounts are protected through advanced filtering solutions, including:

- Spam and phishing detection
- AI-driven malicious link and attachment scanning
- Policy enforcement for inbound and outbound messages

4.2.4 Access Control

- Users shall only have access to systems and data necessary for their job duties.
- Unique user accounts are required—password sharing is prohibited.
- Password policies shall follow NIST recommendations and HB96 expectations.

4.2.5 Acceptable Use

Employees must adhere to the Township's acceptable use guidelines, including proper handling of data, restricted installation of software, and safe browsing practices.

4.2.6 Security Awareness & Training

As required by HB96:

- All employees will complete regular cybersecurity awareness training.
- Training includes phishing awareness, password hygiene, data handling, and incident reporting.

4.3 Detect (DE)

The Township utilizes automated and monitored systems to identify anomalies and potential cybersecurity incidents.

4.3.1 Threat Detection

- Managed EDR monitors endpoint behavior for malicious activity.
- Managed SOC reviews and correlates alerts continuously.
- Email filtering detects suspicious messages and quarantines malicious content.

4.3.2 Logging & Monitoring

- Security logs from endpoints are analyzed through EDR/SOC tools.
- Unauthorized changes or access attempts are flagged for investigation.

4.4 Respond (RS)

4.4.1 Incident Response

In accordance with HB96 requirements:

- All Township employees must promptly report suspected cybersecurity incidents to IT.
- The Managed SOC will notify Township IT of verified threats and support containment actions.
- Township IT will coordinate remediation, documentation, and communication with leadership.

4.4.2 Evidence Preservation

- Logs, alerts, and investigative data will be preserved as required for analysis and potential legal review.

4.4.3 External Reporting

If an incident meets HB96 or other regulatory thresholds, appropriate authorities will be notified.

4.5 Recover (RC)

4.5.1 Restoration & Continuity

- Systems impacted by a cybersecurity event will be restored from clean backups or reinstalls.
- Township IT will ensure system integrity before returning any affected device to service.

4.5.2 Post-Incident Review

- Lessons learned will be documented.
- Policies or controls may be updated to prevent recurrence.

5. Vendor & Third-Party Requirements

All vendors accessing Township systems must:

- Comply with HB96 security expectations
- Use secure authentication mechanisms
- Only access systems when authorized
- Notify Township IT immediately of any security incidents involving Township data

6. Policy Enforcement

Violations of this policy may result in:

- Revocation of system access
- Disciplinary action
- Possible legal consequences if negligence or intentional misuse occurs

7. Review & Maintenance

- This policy shall be reviewed annually or when significant changes occur in HB96, NIST requirements, technology, or Township operations.
- Updates must be approved by Township leadership.

8. Acknowledgment

All employees, officials, and third parties must review and acknowledge this policy as a condition of system access.