City Council
City of Mount Vernon
Mount Vernon, OH 43050

SCHEDULED

Meeting: 09/22/25 7:30 PM
Dept: Fire, Police and Civil Defense
Mahan, Seavolt
Category: Police
Prepared By: Rob Broeren
Initiator: Zac Sherman
DOC ID: 4289

ORDINANCE 2025-28

AN ORDINANCE ADOPTING A CYBERSECURITY POLICY FOR THE CITY OF MOUNT VERNON, OHIO, IN ACCORDANCE WITH OHIO REVISED CODE § 9.64; AND DECLARING AN EMERGENCY.

WHEREAS, the State of Ohio has enacted legislation requiring local governments to adopt cybersecurity policies by September 30, 2025; and

WHEREAS, the protection of City data, systems, and critical infrastructure is essential to maintaining public trust, operational integrity, and continuity of services; and

WHEREAS, the City of Mount Vernon seeks to establish a comprehensive cybersecurity program in compliance with state law and best practices;

NOW, THEREFORE, BE IT ORDAINED by the Council of the City of Mount Vernon, Ohio:

Section 1. Adoption of Cybersecurity Policy

The City of Mount Vernon hereby adopts the Cybersecurity Policy attached hereto as Exhibit A, which is incorporated by reference and shall govern the City's cybersecurity program.

Section 2. Ransomware Restriction

No ransom demand shall be paid in response to a cybersecurity incident unless authorized by ordinance or resolution of City Council in compliance with Ohio Revised Code § 9.64.

Section 3. Reporting

The City shall report cybersecurity incidents to the Ohio Department of Public Safety, Office of Homeland Security, and the Auditor of State, within the time frames required by law.

Section 4. Confidentiality

Cybersecurity plans, records, and related documentation are deemed non-public records under Ohio law and shall be exempt from public disclosure.

Section 5. Emergency Clause

This Resolution is hereby declared to be an emergency measure necessary for the immediate preservation of the public peace, health and safety, and for the further reason that this

policy must be in place by September 30, to comply with the Revised Code, and said Resolution shall, therefore, become effective upon its date of passage and approval by the Mayor, provided that it receives the affirmative vote of two-thirds (2/3) of the members elected to the Council of the City of Mount Vernon; otherwise it shall take effect and be in force from and after the earliest period allowed by law.

HISTORY:

09/08/25	**City Council**	**FIRST READING**

Ordinance was given its first reading. Mahan requested a 10-minute Fire, Police, and Civil Defense committee meeting to discuss the ordinance.

EXHIBIT A

Cybersecurity Policy for the City of Mount Vernon, Ohio

Section 1. Purpose

The City of Mount Vernon ("City") is committed to safeguarding the confidentiality, integrity, and availability of its information systems and data. In compliance with Ohio Revised Code § 9.64, this Cybersecurity Policy establishes requirements for risk management, training, incident reporting, and ransomware response.

Section 2. Scope

This policy applies to all elected officials, employees, contractors, vendors, and volunteers who have access to City technology systems, data, or networks.

Section 3. Cybersecurity Program

The City shall maintain a cybersecurity program consistent with recognized best practices, including the **National Institute of Standards and Technology (NIST) Cybersecurity Framework** and **Center for Internet Security (CIS) Controls**. At a minimum, the program shall include:

- **Risk Assessment:** Annual review of vulnerabilities and critical functions.
- **Access Control:** Role-based access, strong authentication, and least-privilege principles.
- **Multi-Factor Authentication (MFA):** Required for remote access and sensitive systems.
- **Encryption:** Encryption of data at rest and in transit.
- **Patch Management:** Timely updates and security patches for all systems.
- **Monitoring & Logging:** Continuous monitoring, detection, and logging of cyber events.
- **Vendor Oversight:** Security due diligence for third-party contractors and service providers.
- **Incident Response Plan:** Documented and tested response procedures.

Section 4. Training & Awareness

All City employees shall receive annual cybersecurity training, with role-based training for IT staff and department heads.

Section 5. Ransomware Restrictions

The City shall not pay ransom demands resulting from a ransomware incident unless:

1. City Council authorizes such payment by ordinance or resolution, and

2. The authorization clearly states why the payment is in the best interest of the City.

Section 6. Reporting Requirements

- The City shall report cybersecurity incidents within **seven (7) days** to the Ohio Department of Public Safety, Office of Homeland Security.

- The City shall provide notice to the Auditor of State as required by law.

Section 7. Confidentiality of Records

All cybersecurity plans, procurement records, and incident documentation shall be maintained as confidential and are exempt from disclosure under Ohio public records law.

Section 8. Compliance & Review

The Utilities Director (or designated Information Security Officer) shall ensure compliance with this policy, provide annual reports to City Council, and recommend updates as needed