Cybersecurity

708.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines to protect the city's information technology infrastructure from cyber threats.

Additional guidelines for the use of city information technology infrastructure are found in the Information Technology Use Policy.

708.1.1 DEFINITIONS

Definitions related to this policy include:

Cybersecurity – The practice of protecting an information technology infrastructure from digital attacks.

Cybersecurity incident - Any incident that compromises the security of the information technology infrastructure of the city. This includes but is not limited to data breaches, unauthorized access attempts, malware infections, phishing attacks, and any other suspicious activity.

Cyber threats – Unauthorized access, use, disclosure, disruption, modification, or destruction of the city's information technology infrastructure.

Information technology infrastructure – All electronic devices, networks, systems (e.g., hardware, software, firmware), and data owned, operated, or managed by the City, including but not limited to computers, servers, mobile devices, networking equipment, and cloud-based services.

708.2 POLICY

The City is committed to maintaining the security and integrity of its information technology infrastructure and will take reasonable cybersecurity measures to safeguard its information technology infrastructure from cyber threats.

708.3 CITY MANAGER RESPONSIBILITIES

The City Manager is responsible for securing and allocating the necessary resources, support, and guidance to provide effective cybersecurity measures.

708.4 EMPLOYEE AND ELECTED OFFICIAL RESPONSIBILITIES

All City employees and elected officials share responsibility for proactively protecting the city information technology infrastructure from cyber threats and cybersecurity incidents.

Employees and elected officials shall immediately report any suspicious activity, actual or suspected cyber threats, or cybersecurity incidents pursuant to the procedures established by the ISO.

708.5 ACCESS CONTROL, PASSWORD, AND USER MANAGEMENT

Access to city information technology infrastructure shall be granted based on the principle of least privilege so that city employees have only the necessary access rights required for their specific job duties.

The city shall require password access to the city information technology infrastructure. Passwords shall be required to meet the minimum length and complexity requirements, be changed periodically, and not be shared, reused, or stored in plain text. The City shall implement multi-factor authentication for systems containing sensitive or critical information.

Upon separation from employment, an employee's access to the city information technology infrastructure shall be immediately terminated.

708.6 NETWORK SECURITY

The City shall implement firewalls and other intrusion prevention systems to protect the city information technology infrastructure from unauthorized access, malware, and other cyber threats.

The City shall ensure that city wireless networks are secured using encryption, strong passwords, firewall configurations, and any additional security protocols necessary to protect against cyber threats.

Information systems shall be configured securely to protect the security of city data.

708.7 DATA CLASSIFICATION, PROTECTION, AND DISPOSAL

Data should be classified by the City based on its sensitivity. Appropriate security controls should be implemented based on the classification level of the data.

Regular data backups shall be performed by the city and shall be stored in a secure location. The process used for data backup and recovery shall be regularly tested to confirm it can adequately recover data if needed. All testing should be documented.

The ISO shall also ensure that sensitive data at rest and in transit is encrypted using industry standard encryption algorithms and protocols.

The disposal of sensitive information should follow appropriate protocols to prevent unauthorized retrieval (e.g., secure erasure, destruction of data).

708.8 INCIDENT RESPONSE PLAN

The City should maintain an incident response plan that addresses cybersecurity incidents promptly. The incident response plan should include procedures for:

a. The receipt and processing of reported cybersecurity incidents or events.
b. Specific steps for identifying, containing, and mitigating security incidents.
c. Coordination with relevant departments, external agencies, and other stakeholders to develop an appropriate response.
d. Regular audits to determine compliance with incident response procedures.
e. Post-incident recovery actions and protocols, including:
    1. Containment and eradication of threat.
    2. Recovery of data.
    3. Required reporting.
    4. Continuity of services.
f. The investigation of any reported cybersecurity incidents, including steps to prevent future occurrences.
g. Regular interactive simulations and practical exercises to test compliance and awareness of incident response procedures.

708.9 CYBER INCIDENT NOTIFICATION REQUIREMENTS

There are new reporting requirements to the State of Ohio following a cyber security or ransom ware incident. Following all such incidents notify both of the following:

1. The Executive Director of the Division of Homeland Security within the Ohio 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. Notification will be made to OHS's Cyber Integration Center (OCIC), and guidelines will be issued soon as to the appropriate means of notifying.
2. The Ohio Auditor of State (AOS), in a manner prescribed by the AOS, as soon as possible but not later than thirty days after the political subdivision discovers the incident.

Importantly, any records, documents, or reports related to the cyber security program and framework in division (C) of this section, and the reports of a cyber security incident or ransom ware incident under division (D) of this section, are not public records under section 149.43 of the Revised Code. Under this section, a reportable "Cyber security incident" is broad and means any of the following:

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network.
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes.
- A disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services.
- Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:

- A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
- A supply chain compromise.

"Cyber security incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a United States, state, local, tribal, or territorial government entity.

708.10 NEW RANSOM WARE PAYMENT REQUIREMENTS

Local governments experiencing a ransom ware incident shall not pay or otherwise comply with a ransom demand, unless their legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the local government. For purposes of this section, "ransom ware incident" means a malicious cyber security incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

708.11 CYBERSECURITY TRAINING PROGRAM

All employees and elected officials shall complete initial and annual cybersecurity awareness training consistent with the requirements established in the cybersecurity training program.

The cybersecurity training program should include instruction on the following:

a. Recognizing and avoiding threats (e.g., phishing awareness, social engineering tactics, safe browsing).
b. Secure device use (e.g., keeping devices updated and secure, mobile device security, physical device security).
c. Safe network practices (e.g., Wi-Fi security considerations, virtual private networks, firewall and antivirus software).
d. Data security (e.g., data encryption and backup, handling confidential data).
e. This policy and all related policies and procedures, including:
    1. Acceptable use, password protection, and remote access procedures.
    2. Procedures for data classification.
    3. Incident reporting procedures.
    4. Incident response plans.
    5. Applicable state and federal law related to cybersecurity.