City of Gahanna Cybersecurity Program Policy

Department of Origin: Technology	Total # of Pages: 5
Subject: City of Gahanna Cybersecurity Program	Mayor's Approval Date:
Scope: City of Gahanna Employees, contractors, elected officials, board and commission members, and vendors	Effective Date:

Purpose and Authority

This policy establishes the City of Gahanna's Cybersecurity Program in compliance with Ohio Revised Code,

The purpose of this program is to safeguard the confidentiality, integrity, and availability of city information systems and data, while ensuring continuity of public services. This policy shall be adopted by City Council resolution and maintained under the authority of the Mayor.

Scope

This policy applies to:

- All City of Gahanna departments, offices, and divisions;
- All employees, Elected Officials, Board and Commission Members; contractors, and vendors who access or manage city technology resources; and
- All city-owned information systems, networks, and data assets, whether hosted on-premises or in the cloud.

Program Objectives

1. Establish a unified cybersecurity framework across all city operations.
2. Protect city information assets from unauthorized access, disclosure, alteration, or destruction.
3. Promote security awareness and accountability among employees and partners.
4. Ensure compliance with state, federal, and local requirements.
5. Support continuity of operations through effective backup, recovery, and response plans.

Governance and Responsibilities

- Director of Information Technology – Serves as Program Administrator, responsible for implementation, monitoring, and reporting as necessary.
- Department Heads – Ensure compliance with cybersecurity requirements within their departments.
- Employees, Elected Officials, Board and Commission members, and Contractors – Follow city security policies, complete required training, and report suspected incidents promptly.
- Vendors / Third Parties – Must meet minimum security standards and notify the city of any data breach or compromise involving city data.

Cybersecurity Framework

The City of Gahanna's Cybersecurity Program will align with the NIST Cybersecurity Framework and include the following functional areas:

Identify

- Maintain an inventory of hardware, software, and data assets.
- Conduct periodic risk assessments to evaluate threats and vulnerabilities.

Protect

- Implement access control, password standards, and multifactor authentication.
- Enforce regular patching, encryption, and endpoint protection.
- Maintain secure network configurations and physical safeguards.

Detect

- Monitor systems for anomalous or unauthorized activity.
- Maintain audit logs and review them regularly for signs of compromise.

Respond

- Follow the City's Incident Response Plan for cybersecurity events.
- Coordinate communication with affected departments, law enforcement, and state authorities as needed.

Recover

- Maintain verified data backups and disaster-recovery capabilities.
- Conduct periodic restoration testing to ensure operational continuity.

Cybersecurity Program Requirements

To comply with Ohio Revised Code 9.64, the City of Gahanna's Cybersecurity Program will be consistent with generally accepted best practices for cybersecurity and shall include, at minimum, the following components:

Identify and Address Critical Functions and Cybersecurity Risks

- The program shall identify mission-critical systems, essential public services, sensitive datasets, and core business functions.
- Risk assessments shall evaluate internal and external threats, vulnerabilities, business impacts, and the likelihood of compromise.

Identify the Potential Impacts of a Cybersecurity Breach

Each department shall collaborate with the Technology Department to document operational, financial, legal, and service-delivery impacts that may result from a cybersecurity incident. These assessments will support prioritization of protective measures and recovery objectives.

Mechanisms to Detect Potential Threats and Cybersecurity Events

The City shall maintain and continuously improve processes and technologies designed to detect suspicious activity, including but not limited to:

- System monitoring and alerting

- Log collection and analysis
- Endpoint detection and response
- Email threat detection and filtering
- Network intrusion detection and anomaly monitoring

Procedures for Communication, Analysis, and Containment

The City shall establish and maintain procedures for:

- Immediate notification to the IT Department of suspected incidents
- Activation of the City's Incident Response Plan
- Communication channels between IT, Department Heads, Legal, HR, Communications, and Public Safety
- Analysis of incident severity, scope, and potential data exposure
- Containment strategies to prevent further compromise
- Engagement of outside cybersecurity partners when appropriate

Repair, Restoration, and Post-Incident Security

The City shall maintain procedures for:

- Rapid repair or replacement of systems impacted by a cybersecurity incident
- Recovery of data from secure, verified backups
- Post-incident vulnerability remediation
- Verification that systems are securely restored before returning to service

Cybersecurity Training Requirements

All users of City technology shall receive cybersecurity awareness training corresponding to the sensitivity of their duties. Training frequency, depth, and format will be role-based and may include:

- General annual cybersecurity awareness training
- Specialized training for administrators, finance, HR, law enforcement, and privileged users
- Tabletop exercises and scenario-based drills

Cybersecurity Incident and Ransomware Reporting Requirements (ORC 9.64)

Upon discovering a cybersecurity incident or ransomware incident, the City of Gahanna shall comply with the reporting requirements established under Ohio Revised Code 9.64.

Required Notifications:

• Notify the Executive Director of Ohio Homeland Security within the Ohio Department of Public Safety as soon as possible, but no later than seven (7) days after discovering the incident.

Incidents may be reported to the Ohio Cyber Integration Center (OCIC):
Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
Email: OCIC@dps.ohio.gov
Phone: 614-387-1089

• Notify the Ohio Auditor of State as soon as possible, but no later than thirty (30) days after discovering the incident.

Incidents may be reported via email to Cyber@ohioauditor.gov using the reporting form available at: https://ohioauditor.gov/fraud/cybersecurity.html

Cybersecurity Incident Definition:

A cybersecurity incident includes any of the following:

- A substantial loss of confidentiality, integrity, or availability of the City's information systems or network.
- A serious impact on the safety and resiliency of operational systems and processes.
- A disruption of the City's ability to conduct government operations or deliver services, including but not limited to payment redirect, payroll redirect, or spear phishing.
- Unauthorized access to the City's information systems, networks, or nonpublic information caused by:
- A compromise of a cloud service provider, managed service provider, or third-party hosting provider; or
- A supply chain compromise.

A cybersecurity incident does NOT include:

- Mere threats of disruption or extortion without actual compromise;
- Good-faith cybersecurity research or testing conducted at the request of the system owner;
- Lawfully authorized activity by U.S., state, local, or tribal government entities.

Ransomware Incident Definition:

- A ransomware incident is a malicious cybersecurity incident in which software is introduced that:
- Gains unauthorized access to, encrypts, modifies, or renders unavailable City systems or data; and
- Is followed by a ransom demand to prevent publication, restore access, or remediate the impact.

Ransomware Payment Restrictions:

The City of Gahanna shall NOT pay or comply with any ransom demand unless formally approved by City Council. The approval must be made by resolution or ordinance and must specifically state why payment or compliance is in the City's best interest, as required under ORC 9.64.

Public Records Exemptions

Records, documents, and reports related to the City of Gahanna's cybersecurity program or cybersecurity framework, as well as any reports of a cybersecurity incident or ransomware incident, are NOT public records.

In addition, any records that identify cybersecurity-related software, hardware, goods, or services that are being considered for procurement, have been procured, or are currently in use by the City,

including, but not limited to, the vendor name, product name, project name, or project description, constitute security records.

Security records are expressly exempt from disclosure and shall not be produced in response to a public records request.

Compliance and Review

- The Technology Department shall perform an annual review of the Cybersecurity Program and recommend updates as needed.
- Non-compliance with this policy may result in disciplinary action consistent with Employee Handbook.

History

Original policy creation date, reviewed, and revision dates:

Original Policy Creation Date: 11/19/25	**Review Frequency: Every year**
Revision Date(s): 11/19/25	**Review Date(s):**

Approval

Mayor:

_____	_____	_____
Print Name	Signature	Date