CITY OF CLAYTON

ORDINANCE NO. O – 11 – 25 – 33

AN ORDINANCE ADOPTING AND IMPLEMENTING THE CITY OF CLAYTON CYBER SECURITY POLICY; AUTHORIZING RELATED ADMINISTRATIVE PROCEDURES; PROVIDING FOR PUBLICATION AND POSTING; AND SUPERSEDING PRIOR INCONSISTENT ORDINANCES, RESOLUTIONS, AND POLICIES

1. Title and Authority

   1.1. This Ordinance is adopted pursuant to the Charter of the City of Clayton, Ohio (the Charter), which empowers Council to define duties and set terms for positions by ordinance, to adopt administrative policies governing the operation of the City, and to provide for emergency measures and publication.

   1.2. Council finds it necessary to formally adopt a comprehensive Cyber Security Policy to safeguard the City's information systems, protect sensitive data, ensure continuity of public services, and mitigate operational, financial, and legal risk.

2. Adoption of Cyber Security Policy

   2.1. Council hereby adopts the City of Clayton Cyber Security Policy (the Policy) as set forth in the document titled "City of Clayton Cyber Security Policy," attached hereto as Exhibit A and incorporated herein by reference.

3. Applicability; Compliance

   3.1. The Policy applies to all City departments, officers, employees, contract personnel, volunteers, and third parties with authorized access to City information systems, networks, devices, applications, or data.

   3.2. The City Manager, or designee, shall ensure organizational compliance with the Policy and shall promulgate administrative procedures, standards, and guidelines necessary to implement the Policy, including user access controls, incident response protocols, business continuity and disaster recovery procedures, vendor and third-party risk management, data classification and retention standards, acceptable use, and training.

   3.3. All personnel and third parties within scope shall comply with the Policy and related procedures as a condition of access to City systems and data.

4. Incident Response; Notification

   4.1. The City shall maintain an Incident Response Plan (IRP) aligned with the Policy, defining detection, escalation, containment, eradication, recovery, and post-incident review.

5. Data Governance; Records; Privacy

   5.1. The Policy shall align with applicable public records, records retention schedules, and privacy obligations.

6. Superseding Clause
   6.1. This Ordinance and the Policy supersede any prior ordinances, resolutions, rules, or policies of the City to the extent they are inconsistent with the provisions herein or in the Policy.

7. Readings; Effective Date
   7.1. Readings. This Ordinance shall be read on two different days in accordance with Charter Section 4.031 unless duly dispensed with by the requisite vote.
   7.2. Effective Date. This Ordinance shall take effect and be in force from and after the earliest period allowed by law and the Charter of the City of Clayton.

8. Administrative Authority; Non-Substantive Updates
   8.1. The City Manager, in consultation with the Law Director and IT, is authorized to issue and update administrative procedures and standards to implement the Policy. Non-substantive updates that do not materially alter the rights or obligations established by the Policy may be approved administratively. Material amendments to the Policy shall be submitted to Council for approval.

9. Severability
   9.1. If any provision of this Ordinance or the Policy is held invalid by a court of competent jurisdiction, such invalidity shall not affect the remaining provisions, which shall continue in full force and effect, and to this end the provisions are declared severable.

10. Authentication; Approval as to Form
    10.1. This Ordinance shall be authenticated by the signatures of the Mayor and Clerk of Council.
    10.2. The Law Director shall approve this Ordinance and Exhibit A as to form.

ADOPTED BY COUNCIL ON DECEMBER 4, 2025

AUTHENTICATION:

Mayor (Presiding Officer of Council)   Clerk of Council

APPROVED AS TO FORM:

Law Director

Exhibit A

Cybersecurity Policy

PURPOSE AND AUTHORITY

This policy establishes the official cybersecurity program for the City of Clayton in compliance with Ohio Rev. Code § 9.64. The purpose of this policy is to safeguard City data, information technology (IT) systems, and IT resources against cybersecurity threats, including but not limited to ransomware, phishing, social engineering, and data breaches.

This program ensures the availability, confidentiality, and integrity of City information systems and aligns with recognized cybersecurity best practices, including the NIST Cybersecurity Framework and Center for Internet Security (CIS) Controls.

DEFINITIONS

Cybersecurity Program: A structured set of policies, practices, and controls adopted by the City to prevent, detect, respond to, and recover from cybersecurity incidents.

Cybersecurity Incident: Any event that results in a substantial loss of confidentiality, integrity, or availability of the City's information systems or network, unauthorized access to sensitive information, or disruption of City services.

Managed Service Provider (MSP) A third-party technology vendor contracted by the City of Clayton to provide information technology services, including system monitoring, cybersecurity support, and incident response assistance. The MSP operates under contract and in coordination with the City IT Liaison(s) but does not independently act on behalf of the City unless specifically authorized.

Ransomware Incident: A malicious cybersecurity incident in which software gains unauthorized access to City systems or data, rendering them unavailable, followed by a demand for ransom.

Political Subdivision: As defined in ORC § 9.64, including counties, townships, and municipalities.

CYBERSECURITY PROGRAM STANDARDS

The City of Clayton shall maintain a cybersecurity program that:

(a) **Risk Identification**: Identifies critical functions, IT assets, and cybersecurity risks to City operations.

(b) **Impact Assessment**: Evaluates the potential impacts of a cybersecurity breach on City operations and public safety.

(c) **Threat Detection**: Implements monitoring tools, alerts, and procedures to detect potential cybersecurity threats or incidents.

(d) **Incident Response Procedures**: Establishes communication channels and processes to analyze, contain, and recover from cybersecurity incidents.

(e) **Recovery and Maintenance**: Provides procedures for restoring affected systems, securing infrastructure post-incident, and maintaining ongoing resilience.

Exhibit A

EMPLOYEE CYBERSECURITY TRAINING

- **Mandatory Training**: All City employees shall complete annual cybersecurity awareness training.
- **Approved Training Programs**: Training provided by the **Ohio Persistent Cyber Initiative (O-PCI)** or equivalent programs satisfies this requirement.
- **Role-Based Training**: Additional training may be required for employees with elevated IT access or responsibilities.
- **Tracking Compliance**: The City Personnel Director shall track and report training completion annually to the City Manager.

INCIDENT REPORTING REQUIREMENTS

In the event of a cybersecurity or ransomware incident, the City of Clayton shall:

(a) Notify the **Ohio Department of Public Safety – Ohio Homeland Security (OCIC)** within **7 days** of discovery.

- OCIC Contact: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
- Email: OCIC@dps.ohio.gov
- Phone: (614) 387-1089

(b) Notify the **Ohio Auditor of State** within **30 days** of discovery.

- Email: Cyber@ohioauditor.gov
- Reporting form: https://ohioauditor.gov/fraud/cybersecurity.html

(c) Internally, incidents shall be reported immediately to the City IT Liaison(s), who will notify the City Manager. The City Manager will then make notification to Mayor/Council.

Managed Service Provider (MSP) Notification and Coordination (if under contract)

1. MSP Notification Requirement
   a. Upon discovery or suspicion of a cybersecurity or ransomware incident, the City IT Liaison(s) shall immediately notify the City's contracted Managed Service Provider (MSP).
   b. If the IT Liaison(s) is unavailable, City personnel discovering the incident shall notify both the MSP and the City Manager directly.
2. MSP Role in Incident Response
   a. The MSP shall assist in investigating, containing, and remediating the incident in coordination with the City IT Liaison(s).

Exhibit A

b. The MSP shall provide technical documentation, logs, and analysis to support required state reporting.

3. Coordination with State Reporting
   a. The MSP shall not directly report to state authorities unless specifically authorized by the City IT Liaison(s) or City Manager.
   b. The MSP's role is to provide timely information and technical support to ensure that required reports to Ohio Homeland Security and the Ohio Auditor of State are accurate and complete.

RANSOMWARE RESPONSE

- **Prohibition on Payment**: The City shall not pay or comply with ransom demands unless authorized by a formal vote of City Council.
- **Council Resolution Requirement**: Any authorization must be in the form of a resolution or ordinance stating why payment or compliance is in the City's best interest.
- **Documentation**: All actions taken in response to ransomware incidents must be documented and retained by the City Manager or City IT Liaison(s).

RECORDS AND PUBLIC RECORDS EXEMPTION

- Cybersecurity programs, incident reports, and related records are exempt from disclosure under Ohio Rev. Code § 9.64.
- Procurement records identifying cybersecurity-related software, hardware, vendors, or services are designated as security records and are not public records.

OVERSIGHT AND COMPLIANCE

- The City IT Liaison(s) shall be responsible for implementing and maintaining the cybersecurity program.
- The cybersecurity program will be reviewed annually and updated as necessary.
- Compliance procedures will align with the Ohio Compliance Supplement as developed by the Auditor of State.

Exhibit A

EFFECTIVE DATE

This policy shall become effective upon adoption by the Clayton City Council and shall be fully implemented by January 1, 2026 in accordance with ORC § 9.64.