

3  
4 CITY OF CUYAHOGA FALLS, OHIO

5  
6 ORDINANCE NO. 101 - 2025

7  
8 AN ORDINANCE ADOPTING A CYBERSECURITY  
9 PROGRAM AS REQUIRED BY LAW, AND DECLARING AN  
10 EMERGENCY.

11  
12 WHEREAS, political subdivisions have increasingly become targets for cybercriminals  
13 because of limited cybersecurity budgets and outdated systems; and

14  
15 WHEREAS, these cyber-attacks can disrupt government services, expose personal  
16 and financial information, cause political subdivisions to incur significant costs, and  
17 reduce the public trust; and

18  
19 WHEREAS, Ohio House Bill 96, effective September 30, 2025, established Ohio  
20 Revised Code Section §9.64 that requires political subdivisions to adopt a cybersecurity  
21 program; and

22  
23 WHEREAS, said cybersecurity program must safeguard data and information  
24 technology and be consistent with generally accepted best practices; and

25  
26 WHEREAS, it is necessary for the City to adopt such a program.

27  
28 NOW, THEREFORE, BE IT ORDAINED by the Council of the City of Cuyahoga Falls,  
29 County of Summit and State of Ohio, that:

30  
31 Section 1. The City of Cuyahoga Falls hereby adopts the cybersecurity program, as  
32 summarized in Exhibit A attached hereto, as required by Ohio Revised Code §9.64.


33  
34 Section 2. Any other ordinances and resolutions or portions of ordinances and  
35 resolutions inconsistent herewith are hereby repealed, but any ordinances and  
36 resolutions or portions of ordinances and resolutions not inconsistent herewith and  
37 which have not previously been repealed are hereby ratified and confirmed.

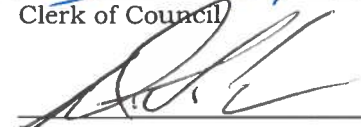
38  
39 Section 3. It is found and determined that all formal actions of this Council  
40 concerning and relating to the adoption of this ordinance were adopted in an open  
41 meeting of this Council and that all deliberations of this Council and of any of its  
42 committees that resulted in such formal action were in meetings open to the public, in  
43 compliance with all legal requirements including, to the extent applicable, including  
44 Chapter 107 of the Codified Ordinances.

45  
46 Section 4. This ordinance is hereby declared to be an emergency measure necessary  
47 for the preservation of the public peace, health, safety, convenience and welfare of the  
48 City of Cuyahoga Falls and the inhabitants thereof, and provided it receives the  
49 affirmative vote of two thirds of the members elected or appointed to Council, it shall take  
50 effect and be in force immediately upon its passage and approval by the Mayor; otherwise  
51 it shall take effect and be in force at the earliest period allowed by law.

56 Passed: 12-22-2025  
57  
58  
59  
60  
61  
62  
63  
64 Approved: 12-22-25  
65  
66 12/8/25

  
\_\_\_\_\_  
President of Council

  
\_\_\_\_\_  
Clerk of Council

  
\_\_\_\_\_  
Mayor

## **EXHIBIT A**

### **1. Purpose**

The purpose of this policy is to establish a framework for protecting the confidentiality, integrity, and availability of the City's information systems, data, and technology resources in compliance with R.C. §9.64 cybersecurity requirements.

### **2. Scope**

This policy applies to all elected officials, employees, contractors, vendors, and third parties who access or the City's technology resources, including but not limited to:

- Computers, servers, and mobile devices
- Cloud services and hosted applications
- Networks and telecommunications systems
- Sensitive or confidential data (e.g., PII, financial, law enforcement, health-related, or other protected records)

### **3. Policy Statement**

The City is committed to safeguarding its information systems against cybersecurity threats and ensuring compliance with R.C. §9.64 by:

- Establishing baseline cybersecurity practices
- Providing ongoing cybersecurity awareness training
- Preparing for detection, response, and recovery from incidents
- Reviewing and updating cybersecurity policies annually

### **4. Roles and Responsibilities**

- **City Council:** Approves cybersecurity policy and ensures resources are allocated
- **Administrator/Manager:** Oversees policy implementation, coordinates with IT providers and legal counsel
- **IT Department:** Implements technical safeguards, monitors for threats, and reports incidents
- **Employees/Users:** Follow cybersecurity protocols, complete training, and report suspicious activity

### **5. Cybersecurity Controls**

#### **5.1 Access Control**

- Require unique user IDs and strong passwords
- Enforce multi-factor authentication (MFA) for remote or administrative access wherever possible
- Limit access to sensitive data on a "least privilege" basis

#### **5.2 Network and System Security**

- Maintain up-to-date firewalls, antivirus, and intrusion detection/prevention
- Apply software patches and updates within 30 days of release
- Segregate critical systems from public networks when possible

### **5.3 Data Protection**

- Encrypt sensitive data at rest and in transit
- Regularly back up critical data and test restoration procedures
- Retain records according to Ohio records retention schedules

### **5.4 Incident Response**

- Designate an Incident Response Lead
- Establish procedures for detecting, reporting, and escalating incidents.
- Conduct a post-incident review and update policies as needed
- Establish procedures for the repair and subsequent maintenance of infrastructure after a cybersecurity incident
- In the event of a cybersecurity incident, notify the appropriate parties outlined in R.C. §9.64

### **5.5 Training and Awareness**

- Require all employees to complete cybersecurity awareness training at least once per year
- Provide role-specific training for IT administrators and staff handling sensitive data

### **5.6 Vendor and Third-Party Management**

- Require vendors to comply with The City's cybersecurity standards

## **6. Compliance and Review**

This policy will be reviewed annually and updated to reflect changes in technology, law, and organizational needs

## **7. Enforcement**

Violations of this policy may result in disciplinary action up to and including termination of employment or contract, as well as potential civil and criminal penalties in accordance with applicable law

## **8. Effective Date**

This policy takes effect on January 1, 2026, to meet R.C. §9.64 requirements. Implementation of technical and training requirements must be completed no later than June 30, 2026.