ORDINANCE NO. 180-21

AN ORDINANCE ADOPTING A CYBER SECURITY INCIDENT RESPONSE POLICY FOR THE CITY OF MEDINA.

BE IT ORDAINED BY THE COUNCIL OF THE CITY OF MEDINA, OHIO:

SEC. 1: That the Cyber Security Incident Response Policy for the City of Medina is hereby adopted, subject to the final approval by the Law Director.

SEC. 2: That a copy of the Cyber Security Incident Response Policy is marked Exhibit A, attached hereto and incorporated herein.

SEC. 3: That it is found and determined that all formal actions of this Council concerning and relating to the passage of this Ordinance were adopted in an open meeting of this Council, and that all deliberations of this Council and any of its committees that resulted in such formal action, were in meetings open to the public, in compliance with the law.

SEC. 4: That this Ordinance shall be in full force and effect at the earliest period allowed by law.

PASSED: November 8, 2021

SIGNED: John M. Coyne, III
President of Council

ATTEST: Kathy Patton
Clerk of Council

APPROVED: November 9, 2021

SIGNED: Dennis Hanwell
Mayor

Ord. 180-21
Exhibit A

CITY OF MEDINA
CYBER SECURITY INCIDENT RESPONSE POLICY

PURPOSE AND SCOPE

This policy ensures the City of Medina is prepared to respond to cyber security incidents, to protect systems and data, and prevent disruption of government services by providing the required controls for incident handling, reporting, and monitoring, as well as incident response training, testing and assistance.

An incident, as defined in National Institute of Standard and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

RESPONSIBILITIES

All users of City of Medina computing resources shall be aware of what constitutes a cyber security incident and shall understand incident reporting procedures.

Incident response support resources may include, for example, IT Help Desk and access to forensic services.

AGENCY MANAGEMENT, INFORMATION TECHNOLOGY ORGANIZATION:

Develop organization and system-level cyber security incident response procedures to ensure management and key personnel are notified of cyber security incidents as required.

Organizations that support information systems shall develop incident response plans and/or procedures that:

- Provide the organization with a roadmap for implementing its incident response capability
- Describes the structure and organization of the incident response capability
- Provides a high-level approach for how the incident response capability fits into the overall organization

- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
- Defines reportable incidents
- Provides metrics for measuring the incident response capability within the organization
- Defines the resources and management support needed to effectively maintain and mature an incident response capability
- Is reviewed and approved by the Mayor or his designee

Revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing.

Distribute copies of the incident response plan/procedures to incident response personnel.

Communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed.

Provide incident response training to information system users consistent with assigned roles and responsibilities before authorizing access to the information system or performing assigned duties, when required by information system changes; and annually thereafter.

Organizations that support information systems shall implement an incident handling capability for cyber security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinate incident handling activities with contingency planning activities.

Track and document information system security incidents. Retain and safeguard cyber security incident documentation as evidence for investigation, corrective actions, potential disciplinary actions and/or prosecution.

Promptly report cyber security incident information to appropriate authorities in accordance with organization incident reporting procedures.

Organizations that support information systems shall provide an incident response support resource integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Possible implementations of incident support resources in an organization include a help desk or an assistance group and, when required, access to forensics services.

EMPLOYEES:

Employees are the biggest threat to an organization's cyber security. They can cause damage either purposefully or through unintentional acts. Layers of security must be implemented to compensate for this. Steps to protect against these issues include the following:

- Limit user access to only appropriate systems
- Never share login credentials with coworkers or others
- Limit user access to employees that are disciplined or reassigned.
- Physically secure technology and information assets so that only authorized individuals have access.

ACCESS CONTROL:

Controlling access to critical information is required to protect assets from unauthorized disclosure or modification. Access control is the permissions assigned to users of the system that are authorized to access specific resources. Access control is implemented by utilizing user ID and passwords.

User and Network Access:

Users are required to have unique credentials (user ID and password) for system access. Credentials should be confidential and should not be shared with management, supervisors, other employees or anyone outside the City. Users must comply with the following rules for creating and maintaining passwords.

- Passwords should not be posted near computers nor written down where they are easily accessible
- Passwords should not contain words that are found in dictionaries. These are easily cracked by hackers
- Windows passwords must change every 90 days
- Windows user accounts will be frozen after 5 failed login attempts
- Windows password complexity must involve at least three different character sets (e.g., uppercase characters, lowercase characters, numbers, or symbols) and be 10 characters long.
- Windows accounts will be set to an automatic screen lock after 10 minutes of inactivity
- User IDs will be suspended after 90 days of inactivity

Connecting to Third-Party Systems:

Connecting to third-party systems requires a secure connection to allow for the safe exchange of information.

Third-party refers to vendors, consultants and business partners that need to exchange digital information with the City. Third-party system connections are to be used only for business purposes of the organization by authorized third-party employees. Third-party connections will be reviewed annually to determine if they are still valid connections.

This policy applies to all new third-party connection requests and any existing third-party connections. Any existing third-party system connections that do not meet the requirements will need to be redesigned.

Any third-party connection requests must be submitted in writing and approved by the IT Manager.

Remote Access:
Users must be authorized to remotely access the City's network. Remote access is given to employees, contractors and business partners of the City that have an authorized business purpose to access computers, programs, copy files or exchange information. All remote connections must be authorized and secure by City standards.

CYBER SECURITY BEST PRACTICE:

DO:

- Lock your computer when not in use
- Stay alert to suspicious activity
- Password protect all devices
- Use hard to guess passwords
- Be cautious of suspicious or unknown e-mails or links
- Ask questions when in doubt

DON'T:

- Be tricked into giving away confidential information
- Use an unprotected computer
- Leave sensitive information or passwords lying around
- Plug in personal devices without permission
- Install unauthorized programs