CITY OF HUBBARD, OHIO
RECORD OF ORDINANCES AND RESOLUTIONS

THE FRED PROCTER CO., CINTI, O.

RESOLUTION NO. .....
ORDINANCE NO. 24-25 PASSED Oct 20 20 25

AN ORDINANCE

ADOPTING A CYBERSECURITY POLICY FOR THE CITY OF HUBBARD

Whereas, the City of Hubbard is desirous of establishing and implementing a cybersecurity policy, and,

Whereas, Ohio law requires the City of Hubbard establish a cybersecurity policy.

NOW, THEREFORE, BE IT ORDAINED by the Council of the City of Hubbard, County of Trumbull, State of Ohio, that:

SECTION 1: City of Hubbard Cybersecurity Policy is hereby adopted to read in total as follows:

CITY OF HUBBARD, CYBERSECURITY INCIDENT POLICY
September 30, 2025

The City of Hubbard (the "City") is committed to protecting the confidentiality, integrity, and availability of the City's systems and data. Nothing in this Policy creates special privileges or exemptions from standard administrative procedures. This policy will be superseded by changes in the laws and rules issued by governing agencies.

Definitions

Cybersecurity incident: Means any of the following: (a) a substantial loss of confidentiality, integrity, or availability of the City's information system or network; (b) a serious impact on the safety and resiliency of the City's operational systems and processes; (c) a disruption of the City's ability to engage in business or industrial operations, or deliver goods or services; (d) unauthorized access to the City's information system or network, or nonpublic information contained therein, that is facilitated through or caused by (i) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) a supply chain compromise.

"Cybersecurity 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.

Ransomware incident: Means a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable the City's information technology systems or data and thereafter demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software. A ransomware incident is a type of cybersecurity incident.

Cybersecurity Coordinator (Coordinator): Means the individual designated by the City to coordinate incident intake, reporting, documentation, and coordination with state agencies.

THE FRED PROCTER CO., CINTI, O.

RESOLUTION NO. .....
ORDINANCE NO. 24-25 PASSED Oct 20 20 25

Discovery: Means the first day the City knows, or by exercising reasonable diligence should have known, that a cybersecurity incident occurred. The City is deemed to know of an incident if any employee, officer, or agent (other than the person committing the act) knows of it.

Security Records: Means "Security record" as defined in O.R.C. §149.433 and includes details of the City's IT security infrastructure, records and files associated with protecting

the City's infrastructure, as well as records that are created or kept in response to cybersecurity or ransomware incident.

Employee Duties Regarding Cybersecurity Incidents

Any employee who becomes aware of, or reasonably suspects, a cybersecurity incident must immediately notify the Coordinator, or if unavailable, the employee's supervisor, who will notify the Coordinator without delay. Employees are not required to categorize the event. All employees must fully cooperate with the Coordinator's requests for facts, records, and updates related to the incident until it is closed.

Reporting Cybersecurity/Ransomware Incidents

The City, through the Coordinator, will submit the required notifications on behalf of the Council of the City of Hubbard, in the manner prescribed by the receiving agency, as soon as possible and within the statutory timelines measured from Discovery. Required notifications include reporting to the Executive Director of the Division of Homeland Security through the Ohio Cyber Integration Center within seven (7) days of Discovery and to the Auditor of State within thirty (30) days of Discovery. The Coordinator serves as the City's point of contact for follow-up inquiries from these agencies and will coordinate internal information-gathering and responses to ensure timely, complete submissions.

The Coordinator will maintain a current reporting kit (forms, agency contacts, and submission instructions) and will open an incident file that includes the initial report, basic facts, actions taken, copies of submitted notices, and closure documentation. The Coordinator will work with the City's outside IT consultant or vendors to gather and preserve any necessary technical information (such as logs or system details) and will ensure timely communication within the City and with state agencies.

The City shall, at all times and irrespective of personnel availability, ensure that all Coordinator duties under this Policy are performed and that all required incident notifications are timely and properly submitted.

Ransomware Incidents

No employee, officer, or agent of the City may pay, promise to pay, negotiate, or otherwise comply with any ransomware demand. No employee, officer, or agent of the City may contact or communicate with a threat actor, attempt decryption, or move, delete, or restore encrypted files unless directed by the City. Any suspected ransomware incident must be reported immediately consistent with this Policy. All employees must follow lawful directions issued during the response by the City and any assisting state or federal authorities.

If payment is ever considered, it will be handled **exclusively by City Council**. Any approval must be by **ordinance or resolution** stating why payment or compliance is in the City's best interest

Cybersecurity Training

Starting January 1, 2026, the City shall ensure that all employees complete cybersecurity training at least annually. The City shall determine the frequency, duration, and level of detail of each employee's training so that it corresponds to the employee's duties and system access. Training may be delivered online or in person and may include state-provided programs that satisfy statutory requirements.

Confidentiality and Records

The City shall ensure that all records, documents, and reports related to the City's cybersecurity program and incident files and reports under this Policy will be maintained

securely and treated as non-public records to the extent permitted by law. **For these purposes, "non-public information" includes,** records identifying **security infrastructure, cybersecurity incident investigative details,** cybersecurity-related software, hardware, goods, and services being considered for procurement, procured, or used by the City are treated as "security records" and/or "confidential law enforcement investigatory records" **under Ohio law, including O.R.C. §§ 9.64(E)–(F) and 149.433** to the extent permitted by law and are not subject to disclosure under public records law.

Where personal information may have been compromised, the Coordinator will promptly consult the City's Law Director regarding any additional resident-notification duties under other applicable law.

Employees shall not make statements to the media or the public on behalf of the City about any suspected or confirmed cybersecurity incident unless the City authorizes them to do so.
Media inquiries shall be directed to the City's designated spokesperson. Nothing in this Policy prohibits employees from speaking as private citizens on matters of public concern, from reporting concerns to law enforcement or oversight agencies, or from engaging in activity protected by a collective bargaining agreement, O.R.C. Chapter 4117, or O.R.C. § 4113.52.

SECTION 2: All prior Ordinances or Resolutions or parts thereof in conflict with this Ordinance are hereby repealed.

SECTION 3: All formal actions of the City Council of Hubbard, Ohio relating to the adoption of this Ordinance, and all deliberations of the City Council of Hubbard, Ohio and any of its committees leading to such action, were in meetings open to the public as required by law.

CITY OF HUBBARD, OHIO
RECORD OF ORDINANCES AND RESOLUTIONS

THE FRED PROCTER CO., CINTI, O.

RESOLUTION NO. .....
ORDINANCE NO. 24-25 PASSED Oct 20 20 25

PASSED IN COUNCIL THIS 20TH DAY OF OCTOBER, 2025.

Michael J Moss Sr
PRESIDENT OF COUNCIL PRO TEM

ATTEST:

Larrie Brown
CLERK OF COUNCIL

APPROVED:

Bryan A. Kyle
MAYOR

APPROVAL DATE: 10-20-25

FIRST READING: Oct 20, 25

SECOND READING: _____

THIRD READING: _____

I hereby certify that the foregoing Ordinance was published in The News of Hubbard on the dates hereinbelow set forth and was posted at the Hubbard City Municipal Building and the Hubbard Police Department on the days hereinbelow set forth.

DATES OF PUBLICATION:

_____ day of _____, 2025

_____ day of _____, 2025

_____ day of _____, 2025

POSTED:

21ST day of October, 2025