ORDINANCE -2026- 05

AN ORDINANCE SETTING FORTH POLICIES AND PROCEDURES IN THE EVENT OF A CYBERSECURITY INCIDENT

Whereas, Ohio Revised Code Section 9.64 requires each municipality within the State of Ohio to adopt a policy to deal with ransomware payments and reporting requirements in cybersecurity breaches of the Municipality's computers, networks or software;

Whereas, it is necessary the Municipality enacted policies regarding notification of breaches to the Municipality's cybersecurity and to address ransomware payments or compliance in order to protect the confidential information of the citizens and employees of the Municipality;

Now Therefore Be It Hereby Ordained by the Village of Lewisburg, Ohio as follows:

1. The Municipality shall not make any payments or comply with a ransomware demand in a ransomware incident unless expressly authorized by the Village Council in Resolution or Ordnance form that specifically states why the payment or compliance is in the best interest of the Municipality.

2. In the event an employee of the Municipality shall become aware or suspect a cybersecurity incident has occurred in the Municipality's computer infrastructure such employee shall immediately notify the Municipal Manager and the Municipal Fiscal Officer.

   A. Upon discovering or being informed of a cybersecurity incident of the Municipality's computer infrastructure, the Municipal Fiscal Officer shall notify the Executive Director of the State of Ohio Division of Homeland Security within the Department of Public Safety within seven days after notification.

   B. Upon discovering or being informed of a cybersecurity incident of the Municipality's computer infrastructure the Municipal Fiscal Officer shall notify the Ohio Auditor of State within thirty days after notification.

3. For the purpose of this Ordinance, "Cybersecurity incident" shall be defined as:

    A. A substantial loss of confidentiality, integrity, or availability of the Municipality's information system or network;

    B. A serious impact on the safety and resiliency of the Municipality's operational systems and processes;

    C. A disruption of the Municipality's ability to engage in business or industrial operations, or deliver goods, or services;

    D. Unauthorized access to the Municipality's information, or network, or nonpublic information contained therein, that is facilitated or caused by:

        1. A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or

        2. A supply chain compromise.

4. For the purpose of this ordinance, a "Ransomware incident" is defined as 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 Municipality's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

5. For the purpose of this Ordinance, "Computer infrastructure" is defined as the computers, networks, cloud-based storage or local storage device upon which data used or owned by the Municipality is kept or administered.

6. This Ordinance shall be effective at the earlies date permitted by

Passed: 02-18-2026 Vote: 6-0

Mayor

Clerk of Council