

RECORD OF ORDINANCES

GOVERNMENT FORMS & SUPPLIES 844-224-3338 FORM NO. 30043

Ordinance No. 2026-1-O Passed 07-13-2026, 20

AN ORDINANCE CREATING, ESTABLISHING, AND ADOPTING THE VILLAGE OF BREMEN CYBERSECURITY POLICY

WHEREAS, HB 96, signed by Governor DeWine in June 2025, created Ohio’s new cybersecurity law for political subdivisions under R.C. 9.64 (eff. September 30, 2025); and

WHEREAS, pursuant to R.C. 9.64, all political subdivisions must begin reporting cybersecurity incidents to the Ohio Department of Public Safety and Auditor of State; and

WHEREAS, R.C. 9.64 also requires political subdivisions to adopt a cybersecurity program to protect against potential cybersecurity threats; and

WHEREAS, the deadline for political subdivisions (other than cities and counties) to adopt a cybersecurity program is July 1, 2026; and

WHEREAS, Council for the Village of Bremen now wants to create, establish, and adopt a cybersecurity policy to protect the Village’s confidential data and to comply with R.C. 9.64.

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF BREMEN, FAIRFIELD COUNTY, STATE OF OHIO:

SECTION 1: Council for the Village of Bremen hereby creates, establishes, and adopts its Cybersecurity Policy. A copy of the Policy will be kept on file with the Village Administrator. The Policy may be amended, from time to time, to conform with evolving state cybersecurity laws and technological advancements.

SECTION 2: Pursuant to R.C. 9.64(E), the Village of Bremen Cybersecurity Policy shall not be considered a public record under R.C. 149.43 to ensure the safety of the Village’s digital infrastructure. Any public record requests for the Cybersecurity Policy shall be denied accordingly.

SECTION 3: All prior Ordinances, or any parts thereof, which is/are inconsistent with this Ordinance is/are hereby repealed as to the inconsistent parts thereto.

SECTION 4: It is hereby found and determined that all formal actions of this Council concerning and relating to the adoption of this Ordinance were adopted in an open meeting of this Council, and that any and 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 all legal requirements of the laws of the State of Ohio.

SECTION 5: This Ordinance shall take effect at the earliest time allowed by law.

RECORD OF ORDINANCES

GOVERNMENT FORMS & SUPPLIES 844-224-3338 FORM NO. 30043

Ordinance No. _____ Passed _____, 20____

Passed in Council this 13th day of June, 2026.

Approved as to form:

Motion by: Janet Schmeltzer

Second by: M. Brown

Yeas: 6 Nays: 0 Abstain: 0

Fiscal Officer: Lydia J. Carter

Mayor: Anthony M. Taylor

APPROVED:

Approved as to form this 8th day of May 2026:

Brian M. Zets

Brian M. Zets, Esq.
Village Solicitor



CYBERSECURITY POLICY

1. Purpose

The purpose of this policy is to establish the Village of Bremen's guidelines for computer security, the protection of its networks and its content or knowledge base, and to minimize the risk of external cyber threats.

2. Scope

This policy applies to all Village of Bremen elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the Village of Bremen.

3. Policy

The Village of Bremen is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. To achieve this, the Village of Bremen will identify, evaluate, and take steps to avoid or mitigate risk to the Village's information assets and prevent unauthorized access, damage, theft, compromise, or interference to the Village's information systems. These steps include implementing and operating controls to manage the Village's information security risks and ensuring that all users of information assets are aware of their responsibilities in protecting those assets while complying with all state regulations pursuant to R.C. 9.64.

4. Administrative Responsibilities

The Village Administrator will ensure this written Cybersecurity Policy is implemented, enforced, reviewed, and updated as necessary. The Village Administrator also will:

- Assign cybersecurity training for Village staff to complete, including the free training from the Ohio Persistent Cyber Initiation (O-PCI) and any other similar training he or she may deem necessary.
- Confirm acquisition and implementation of system security software.
- Identify locations where confidential information is stored and accessible.
- Provide input for who should have access to confidential information and what types of privileges or access rights the individual should have.
- Implement additional security tools and safeguards for protecting confidential information, as necessary.

- Ensure Village officials, employees, business partners, contractors, consultants, and authorized users adhere to this policy.

5. Security Standards

5.1 Password Protection and Access Control

The Village Administrator is responsible for ensuring that access to the Village of Bremen's systems and data is appropriately controlled. All systems housing Village data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Users with access to Village systems and data shall not share passwords with anyone. The Village has established the following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: eight (8) characters.
- Changed periodically.
- Invalid login attempts set to lock after three attempts.

Employees are encouraged to follow further safeguards such as:

- Not allowing confidential data on mobile storage media.
- Encrypting sensitive files on computers.

Where possible, multi-factor authentication will be used when users authenticate to the Village's systems. The following user access requirements shall also apply:

- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged access to confidential information is limited to authorized users who require such access for their job responsibilities.
- The Village Administrator shall make sure all system access is removed from all users who separate from the Village within 48 hours.

5.3 Awareness and Training

The Village of Bremen staff are required to complete the free cybersecurity training from the Ohio Persistent Cyber Initiation (O-PCI) and any other similar training assigned by the Village Administrator.

5.4 Data Storage

All Village of Bremen data shall be stored on local servers and, if possible, on cloud backups. Confidential information must be secured by password and removed from computer screens unless it is currently in use.

5.5 Data Transmission

Confidential data SHALL NOT be transmitted outside the Village of Bremen's network without proper authorization. If confidential data is transmitted outside of the Village's network, a strong encryption shall be used when possible.

6. Information Protection Processes and Procedures

6.1 Data Recovery

If one or more of the Village's systems or applications are corrupted or inaccessible, the Village Administrator will collaborate with the respective vendor(s) to restore data from the most recent local and/or cloud backup and, if necessary, acquire replacement hardware.

6.2 Network Infrastructure

The Village of Bremen will protect its system and network from cyber threats by utilizing a firewall. For maximum protection, the network devices shall meet the following configuration standards:

- Vendor and industry standard configurations, including those recommended by the National Institute of Standards and Technology (NIST), shall be used when possible.
- Network servers and routers shall be protected by a firewall.
- Changes to any firewall shall be approved by the Village Administrator.
- Both firewall and router passwords shall be secured and difficult to guess.

6.3 Network Segmentation

The Village shall maintain, at a minimum, two wireless networks should it desire to provide the public with network service. The guest/public wireless network will grant the user internet access only. Access to the secure wireless network is limited to Village officials, staff, employees, contractors, consultants, and other users specifically authorized.

7. Protective Technology

7.1 Email Filtering

Email filtering and anti-malware programs may be implemented to identify and quarantine emails that are deemed suspicious.

7.2 Internet Filtering

There shall be no access to internet websites and protocols that are deemed inappropriate or pose a security risk by the Village Administrator or his/her designee.

7.3 Anti-Malware Tools

All Village of Bremen computer devices shall utilize appropriate firewall security software to protect systems from malware and viruses.

8. Incident Response

A security incident, as it relates to the Village of Bremen's informational assets, may be a Cybersecurity Incident or Ransomware Incident. The Village Administrator is responsible for coordinating all activities during a security incident, including notification and communication activities and the chain of escalation, and deciding if/when outside agencies (e.g., LEADS) need to be contacted.

8.1 Cybersecurity Incidents

A Cybersecurity Incident includes a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network, a serious impact on the safety and resiliency of a covered entity's operational systems and processes, a disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services, or unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or a supply chain compromise.

A Cybersecurity Incident does not include mere threats of disruption as extortion (as opposed to a Ransomware Incident, as defined within **Section 8.2**); 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.

When a Cybersecurity Incident is suspected, the steps below should be taken in order:

- 1.) Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
- 2.) Report the incident to the Village Administrator.
 - a. The Village Administrator shall report the incident to the Executive Director of the Ohio Department of Public Safety within seven (7) days.
 - b. The Village Administrator shall report the incident to the Ohio Auditor of State within 30 days.
- 3.) Contact the third-party service provider (and/or computer forensic specialist) as needed.
- 4.) Disable the compromised account(s) as appropriate.
- 5.) If possible, back up all uncompromised data on the device or copy the device to another system.

- 6.) Determine exactly what happened and the scope of the incident.
- 7.) Determine how the attacker gained access and, if possible, disable it.
- 8.) Restore any needed data from the last known uncompromised backup and put the system back online.
- 9.) Take action to ensure that the vulnerability will not reappear.

8.2 Ransomware Incident; Payment

A 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 a political subdivision'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.

Should a Ransomware Incident occur, no Village of Bremen employee, contractor, consultant, or others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the Village shall pay any amount of the ransom demand unless the Village Council passes a resolution approving such payment specifically stating why the payment or compliance with the ransom demand is in the best interest of the Village.

8.3 Notification

If a Cybersecurity Incident is suspected of having resulted in the loss of, or unauthorized access to employee or third-party data, notify the Village Administrator and Village Solicitor for direction on procedures for notification of the public or affected entities as well as necessary government agencies. The Village Administrator shall report the incident to the Executive Director of the Ohio Department of Public Safety within 7 days and the Ohio Auditor of State within 30 days.

9. Recovery & Restoration

Restoration and recovery processes and procedures shall be executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events. The Village Administrator is responsible for managing and directing activities during an incident, including any recovery steps that may be necessary other than those outlined above.

10. Review of Policy and Procedures

This policy will be reviewed annually or as state regulations under R.C. 9.64 are revised and necessitate a change in the policy or procedures.