ATHENS-HOCKING-VINTON 317 BOARD

Cybersecurity

Policy R-4

Current
Revised Date: N/A
Board Approved:
Effective Date:
Forms: N/A

Supersedes
Number: N/A
Effective Date: N/A
Citation: ORC section 9.64

PURPOSE.

To establish the governance framework for the Board's cybersecurity program in compliance with Ohio Revised Code § 9.64 and other applicable laws. The Board recognizes cybersecurity as a critical risk management and fiduciary responsibility necessary to safeguard public resources, confidential information, and the continuity of operations.

DEFINITIONS.

As used in this Policy and related Procedures:

(1) "Cybersecurity incident" means any of the following:

a. A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
b. A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
c. A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
d. Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is 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.

(2) "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.

POLICY.

The Board shall adopt and maintain a cybersecurity program designed to ensure the confidentiality, integrity, and availability of its information systems, data, and technology resources.

The cybersecurity program shall be aligned with generally accepted industry standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS).

The program shall include administrative, technical, and physical safeguards appropriate to the Board's size, complexity, and risk profile. The Board may utilize any current or future third-party IT contractors to work toward implementing a cybersecurity program that adheres to the above requirements.

In the event of any ransomware incident, the Board shall not pay or otherwise comply with a ransom demand unless the Board formally approves the payment or compliance with the ransom demand in a resolution that specifically states why the payment or compliance with the ransom demand is in the best interest of the Board.

Any records, documents, or reports related to the Board's cybersecurity and framework, and the reports of a cybersecurity incident or ransomware incident as described herein, are explicitly not public records under Ohio Revised Code Section 149.43.

Any record identifying cybersecurity-related hardware, goods, and services that are being considered for procurement, have been procured, or are being used by the Board, including the vendor name, product name, project name, or project description, is considered a security record under Ohio Revised Code Section 149.433.

RESPONSIBILITY.

The HIPAA Privacy and Security Officer and/or designee are responsible for the communication and the implementation of this policy.

See also:

Procedure R4: Cybersecurity