

RECORD OF RESOLUTION

Resolution No. 2026-R-03 Passed June 2nd, 2026
YEAR

VILLAGE COUNCIL OF GREENWICH, OHIO RESOLUTION NO.: 2026-R-03

CYBERSECURITY PROGRAM

Cybersecurity Policy ORC 9.64

A RESOLUTION ADOPTING A CYBERSECURITY PROGRAM AND POLICY THAT SAFEGUARDS THE POLITICAL SUBDIVISION'S DATA, INFORMATION TECHNOLOGY, AND INFORMATION TECHNOLOGY RESOURCES TO ENSURE AVAILABILITY, CONFIDENTIALITY, AND INTEGRITY AS REQUIRED BY OHIO REVISED CODE SECTION 9.64(B)

WHEREAS, Ohio recently enacted HB 96, ORC 9.64, effective: September 30, 2025, regarding pollical subdivision cybersecurity; and

WHEREAS, Ohio Revised Code 9.64 requires:

ORC Section 9.64 | Political subdivision cybersecurity.

(A) As used in this section:

(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) "Political subdivision" means a county, township, municipal corporation, or other body corporate and politic responsible for governmental activities in a geographic area smaller than that of the state.

(3) "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.

(B) A political subdivision experiencing a ransomware incident shall not pay or otherwise comply with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision.

(C) The legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program shall be consistent with generally accepted best practices for cybersecurity, such as the national institute of standards and technology cybersecurity framework, and the center for internet security cybersecurity best practices, and may include, but are not limited to, the following:

- (1) Identify and address the critical functions and cybersecurity risks of the political subdivision.*
- (2) Identify the potential impacts of a cybersecurity breach.*
- (3) Specify mechanisms to detect potential threats and cybersecurity events.*
- (4) Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.*
- (5) Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.*

RECORD OF RESOLUTION

Resolution No. 2026-R-03 Passed June 2nd, 2026
YEAR

(6) Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. Annual cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program of the Ohio cyber range institute, satisfy the requirements of this division.

(D) The legislative authority of a political subdivision, following each cybersecurity incident or ransomware incident, shall notify both of the following:

(1) The executive director of the division of homeland security within the department of public safety, in a manner prescribed by the executive director, as soon as possible but not later than seven days after the political subdivision discovers the incident;

(2) The auditor of state, in a manner prescribed by the auditor of state, as soon as possible but not later than thirty days after the political subdivision discovers the incident.

(E) Any records, documents, or reports related to the cybersecurity program and framework in division (C) of this section, and the reports of a cybersecurity incident or ransomware incident under division (D) of this section, are not public records under section 149.43 of the Revised Code.

(F) A record identifying cybersecurity-related software, hardware, goods, and services, that are being considered for procurement, have been procured, or are being used by a political subdivision, including the vendor name, product name, project name, or project description, is a security record under section 149.433 of the Revised Code.

WHEREAS, ORC Section 9.64(C) requires that Village Council adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.

WHEREAS, Village officers consulted with the current Village I.T. Company, E.S. Consulting in the development of this proposed cybersecurity policy.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF GREENWICH, STATE OF OHIO: (ORC 731.18)

SECTION 1. That Village Council hereby adopts the attached CYBERSECURITY PROGRAM / Cybersecurity Policy. (ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE)

SECTION 2. PUBLIC MEETING. That it is found and determined that all formal actions of this public body concerning or relating to the passage of this legislation were adopted in a public meeting open to the public at all times, and that all deliberations of the public body and any of its committees that resulted in such formal action, were in public meetings open to the public, in compliance with all legal requirements including all lawful ordinances and any applicable provisions of Section 121.22 of the Ohio Revised Code.

WHEREFORE, this legislation shall be in full force and effect from and after the earliest period allowed by law.

PASSED AND ADOPTED on this 2nd day of June, 2026.

ATTESTATION (ORC 731.20)

We hereby attest and affirm that the foregoing legislation received the necessary affirmative roll call votes required for passage by ORC 731.17.


MAYOR


FISCAL OFFICER

RECORD OF RESOLUTION

Resolution No. 2026-R-03 Passed June 2nd, 2026
YEAR

LEGISLATION READINGS

ORC 731.17(A)

- (1) Each ordinance and resolution shall be read by title only, provided the legislative authority may require any reading to be in full by a majority vote of its members.
(2) Each ordinance or resolution shall be read on three different days, provided the legislative authority may dispense with this rule by a vote of at least three-fourths of its members.

First Reading: 3/3/2026 Second Reading: 5/19/2026 Third Reading: 6/2/2026

ROLL CALL VOTE

ORC 731.17(A)(3)

The vote on the passage was taken by yeas and nays and entered upon the journal. Each ordinance or resolution shall be passed, except as otherwise provided by law, by a vote of at least a majority of all the members of the legislative authority. Yeas, nays, abstentions, excused or absent votes were recorded as follows:

aye
Randy Wilson

aye
Lynne Phillips

aye
Jason Hunter

aye
Dorene Beverly

aye
Larry Risner

aye
Randy Stephens

PREPARED BY AND APPROVED AS TO LEGAL FORM [See also ORC 731.21(B)]:

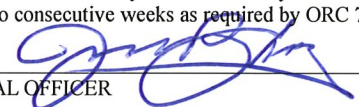

VILLAGE SOLICITOR, Steve Palmer

CERTIFICATE OF PUBLICATION

ORC 731.21 and 731.22

Pursuant to ORC 731.21(A)(3), I hereby certify that a succinct summary of the above legislation was/will be published using the following method: **ON THE WEBSITE AND SOCIAL MEDIA ACCOUNT OF THE MUNICIPAL CORPORATION**

The succinct summary was reviewed by the village solicitor as required by ORC 731.21(B). Publication was/will be made at least once a week for two consecutive weeks as required by ORC 731.22.


FISCAL OFFICER

ATTACHMENT(S) TO FOLLOW