RECORD OF RESOLUTION

Resolution No. 2026 - R - 02 Passed April, 2026 YEAR

VILLAGE COUNCIL OF NORTH FAIRFIELD, OHIO
RESOLUTION NO.: 2026-R-02

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 - 02 Passed Apr 6, 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 in the development of this proposed cybersecurity policy.

NOW THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF NORTH FAIRFIELD, 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 06 day of April, 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

Shellie Cherry
FISCAL OFFICER

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: 3/2/26 Second Reading: 3/16/26 Third Reading: 4/6/26

RECORD OF RESOLUTION

Resolution No. 2026-R-02 Passed Apr 6, 2026 YEAR

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:

yes Adam Rouse	yes Jeremy Amill	yes Cody Hacker
absent Trevor Arnold	yes Mickala Hacker	yes Ben Cherry

PREPARED BY AND APPROVED AS TO 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.

Shellie Cherry

FISCAL OFFICER

ATTACHMENT(S) TO FOLLOW

Village of North Fairfield, Ohio

CYBERSECURITY PROGRAM
Cybersecurity Policy
ORC 9.64

LOCAL OVERVIEW

This Cybersecurity Program / Policy is to protect the Village's electronic information, computer systems, and communications from unauthorized access, data loss, and cyber threats. This Policy establishes minimum security standards appropriate for a small local government operation. This Policy applies to all Village Officials along with any part-time or contracted staff. This Policy further applies to all computers, email accounts, and information systems owned or managed by the Village. In addition, it also applies to any personal devices used for official Village business (e.g., email, document access).

A. DEFINITIONS. Terms as used herein are defined as provided in ORC 9.64(A).

B. RANSOMWARE INCIDENT. *See ORC 9.64(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. PROGRAM SCOPE. *See ORC 9.64(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.
(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. INCIDENT NOTICE. *See ORC 9.64(D)*

Village Council, 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; and
(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. INCIDENT RECORDS *See ORC 9.64(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. PROCUREMENT RECORDS *See ORC 9.64(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.

G. BEST LOCAL PRACTICES

(1) IDENTIFY AND ADDRESS THE CRITICAL FUNCTIONS AND CYBERSECURITY RISKS OF THE VILLAGE

a. No MFA on workstations or emails
b. No DMARC record

(2) IDENTIFY THE POTENTIAL IMPACTS OF A CYBERSECURITY BREACH.

a. Data loss or exfiltration
b. Operational disruption - system downtime affects staff and daily operation
c. Financial loss

(3) SPECIFY MECHANISMS TO DETECT POTENTIAL THREATS AND CYBERSECURITY EVENTS.

a. MailProtector email security
b. Huntress
c. Sentinel One

(4) SPECIFY PROCEDURES FOR THE VILLAGE TO ESTABLISH COMMUNICATION CHANNELS, ANALYZE INCIDENTS, AND TAKE ACTIONS TO CONTAIN CYBERSECURITY INCIDENTS.

a. Immediately report incident to supervisor
b. Immediately call ES Consulting

(5) ESTABLISH PROCEDURES FOR THE REPAIR OF INFRASTRUCTURE IMPACTED BY A CYBERSECURITY INCIDENT, AND THE MAINTENANCE OF SECURITY AFTER THE INCIDENT.

a. Call ES Consulting
b. Contain by disconnect systems that are compromised and blocking malicious IP's
c. Identify any affected assets, such as data
d. eradicate – patch any found exploitations or malware, reset credentials
e. If necessary, restore data from a backup

(6) ESTABLISH CYBERSECURITY TRAINING REQUIREMENTS FOR ALL EMPLOYEES OF THE VILLAGE; 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.

1. <u>FREQUENCY</u>:

Elected Officials every term of office after election and each reelection.

Village Administrator, annually each calendar year.
Fiscal Officer annually each calendar year.

All positions shall complete training no later than 3 months after assuming their position.

*The cybersecurity training required herein may be satisfied by providing proof of cybersecurity training required for other positions or employment.

2. <u>DURATION</u>:

All employees shall complete general cybersecurity training which may be conducted online for 1-2 hours.

3. DETAIL:

Training must be directly related to cybersecurity issues (as determined by supervisor) to satisfy the training requirements established herein.
Proof of training shall be submitted by each official/employee to the Fiscal Officer and maintained in the official/employee personnel file.

H. OTHER LOCAL PRACTICES

1. LOCAL ROLES AND RESPONSIBILITIES

Village Administrator:
Serves as the cybersecurity oversight officer and ensures compliance with this policy.

Fiscal Officer / Clerk:
Responsible for maintaining records, ensuring backups are performed, and following safe data handling practices.

All Users:
Must use Village systems responsibly, report security incidents immediately, and follow password and data protection rules.

2. ACCEPTABLE USE

Computers and email accounts are for official Village business only.
Personal use should be minimal and must not include downloading unapproved software or accessing inappropriate websites.
Users must not share passwords or allow others to use their accounts.

3. PASSWORD AND ACCESS MANAGEMENT

Passwords must be at least 12 characters long and include letters, numbers, and symbols.
Passwords must not be reused or shared.
Enable two-factor authentication (2FA) for email and cloud services whenever possible.
Lock computers when unattended.

4. DATA PROTECTION AND BACKUP

All Village electronic files (meeting minutes, financial records, contracts, etc.) must be stored on a secure cloud account (Microsoft 365).
Data backups should occur at least weekly.
Sensitive information (Social Security numbers, banking info) must not be sent via unencrypted email.

5. EMAIL AND PHISHING AWARENESS

Do not click links or open attachments from unknown senders.
Verify unexpected messages from known contacts before responding.
Report suspected phishing or malware emails to the Village Administrator or Fiscal Officer immediately.

6. DEVICE AND SOFTWARE SECURITY

Use only Village-approved devices and software for official work.
Keep all devices and software updated automatically.
Install antivirus software and allow automatic scans.
USB drives should be scanned before use.

7. LOCAL INCIDENT RESPONSE

If a cybersecurity incident occurs (e.g., lost laptop, ransomware, suspicious email, data breach):

a. Disconnect affected devices from the internet immediately.
b. Notify the Mayor and Fiscal Officer.
c. Contact the Ohio Cyber Reserve or State of Ohio Cybersecurity Office for assistance.
d. Document the event and response steps.
e. Notify local and state law enforcement.

8. REMOTE ACCESS AND PERSONAL DEVICES

If working from home, use a password-protected Wi-Fi network.
Do not store official files permanently on personal devices.
Immediately delete local copies of official files after uploading to the secure Village account.

9. COMPLIANCE

Failure to comply with this policy may result in termination, disciplinary action, and/or loss of system access.

10. ANNUAL REVIEW.

Village Council shall review this policy annually at its organizational meeting in January of each year, and shall update it as needed to reflect new threats or technologies.

11. ACKNOWLEDGEMENT

All employees and officials must sign a statement acknowledging receipt and confirming that they have read, understand, and agree to follow this policy.

Adopted and approved via Resolution No.: 2026-R-02 on the 6 day of April 2026.
2027Annual Review, January _____, 2027 at Organizational Meeting of Council.

ACKNOWLEDGEMENT

I hereby acknowledge receipt of the Village of North Fairfield Cybersecurity Program and Policy and hereby confirm that I have read, understand and agree to this Cybersecurity Policy.

_____ _____
Official/Employee Signature Date

_____
Position

_____
Print name

Original to Personnel file
Copy to Official/Employee