ORDINANCE 2026-012

AN ORDINANCE TO ADOPT A CYBERSECURITY PROGRAM ESTABLISHING RANSOMWARE PAYMENT AUTHORIZATION PROCEDURES, PRESCRIBING CYBERSECURITY INCIDENT REPORTING REQUIREMENTS, AND DECLARING AN EMERGENCY

WHEREAS, in accordance with Ohio revised Code Section 9.64, enacted through House Bill 96, the Village is required to adopt a cybersecurity program that safeguards public data, information technology, and Information Technology (IT) resources to ensure confidentiality, availability, and integrity;

WHEREAS, the law mandates use of generally accepted cybersecurity best practices, including frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security best practices;

WHEREAS, Ohio Revised Code Section 9.64 further requires that political subdivisions report cybersecurity incidents to the Ohio Department of Public Safety, Division of Homeland Security, and to the Auditor of State within prescribed deadlines;

WHEREAS, Ohio Revised Code Section 9.64(B) prohibits political subdivisions from paying a ransom demand arising from a ransomware attack unless the legislative authority formally approves such payment by resolution or ordinance; and

WHEREAS, Council, having reviewed the recommendations of the Communications and Technology Director and the Information Security Officer, hereby adopts the NIST Cybersecurity Framework as its foundational cybersecurity controls framework.

NOW, THEREFORE, BE IT ORDAINED BY THE COUNCIL OF THE VILLAGE OF JACKSON CENTER, OHIO:

Section 1.

The Village hereby adopts a cybersecurity program consistent with the requirements of Ohio Revised Code Section 9.64(C) and aligned with generally accepted best practices, such as the NIST Cybersecurity Framework.

Section 2.

The cybersecurity program shall implement the NIST Cybersecurity Framework to identify and mitigate risks, assess potential impacts, detect and respond to threats, restore affected systems, and maintain ongoing protection of Village assets and data. The program shall include annual cybersecurity training for all employees, align with state and federal best practices, and ensure third-party providers meet applicable security standards to achieve practical, measurable, and cost-effective improvements in defending against cyber threats such as ransomware and phishing.

Section 3.

The Village Administrator and Village's IT Administrator, as defined in the cybersecurity program, in coordination with the Village's Solicitor shall oversee the

implementation, documentation, and annual review of the cybersecurity program to ensure continued alignment with state requirements and best practices.

Section 4. Ransomware Payment Authorization.

(A) Prohibition. Consistent with Ohio Revised Code Section 9.64(B), the Village shall not pay or authorize payment of any ransom demand arising from a ransomware attack without the prior formal approval of Council by resolution or ordinance.

(B) Authorization Process. If the Village Administrator, in consultation with the IT Administrator and Village Solicitor, determines that a ransomware payment may be necessary to restore critical Village functions or protect public safety, the Village Administrator shall promptly present a recommendation to Council. Council shall consider and vote on the proposed payment at a duly noticed public meeting, or by emergency session if circumstances require. No payment shall be disbursed until Council has approved the same by resolution or ordinance.

(C) Law Enforcement Coordination. Prior to authorizing any ransomware payment, the Village shall consult with the Ohio Department of Public Safety, the Federal Bureau of Investigation, or other applicable law enforcement agencies, and shall comply with all applicable federal and state legal requirements governing such payments.

Section 5. Cybersecurity Incident Reporting.

(A) Definitions. As used in this Section, **"Cybersecurity Incident"** means a substantial loss of confidentiality, integrity, or availability of the Village's information systems; a serious impact on the safety and resiliency of the Village's operational systems and processes; or a disruption of the Village's ability to deliver services to the public. **"Ransomware Incident"** means a cybersecurity incident involving ransomware or a ransom demand. The term **"Cybersecurity Incident"** does not include mere threats of disruption as extortion, events performed in good faith at the request of the system owner, or lawfully authorized governmental activity.

(B) Ransomware Incidents — 7-Day Reporting. In the event of a Ransomware Incident, the Village Administrator, in coordination with the IT Administrator, shall notify both (i) the Executive Director of the Division of Homeland Security within the Ohio Department of Public Safety, and (ii) the Ohio Auditor of State, within seven (7) calendar days of discovery of the incident.

(C) Other Cybersecurity Incidents — 30-Day Reporting. In the event of a Cybersecurity Incident that does not involve ransomware, the Village Administrator, in coordination with the IT Administrator, shall notify both (i) the Executive Director of the Division of Homeland Security within the Ohio Department of Public Safety, and (ii) the Ohio Auditor of State, within thirty (30) calendar days of discovery of the incident.

(D) Internal Notification. The IT Administrator shall promptly notify the Village Administrator and the Village Solicitor upon discovery of any potential Cybersecurity

Incident or Ransomware Incident, and shall take reasonable steps to preserve system logs, forensic data, and other relevant evidence.

Section 6. Confidentiality of Cybersecurity Records.

(A) All records and documents related to the Village's cybersecurity program are exempt from public records disclosure, consistent with Ohio Revised Code Section 9.64(E).

(B) Procurement records that identify cybersecurity-related software, hardware, or services utilized by the Village are classified as security records under Ohio law and are likewise exempt from public records disclosure, consistent with Ohio Revised Code Section 9.64(F).

Section 7.

That it is found and determined that all formal actions of this Council concerning and relating to the adoption of this Ordinance were taken in an open meeting of this Council, and that all deliberations of this Council and any of its committees, which resulted in such formal actions, were in meetings open to the public in compliance with all legal requirements, including Section 121.22 of the Ohio Revised Code.

Section 8.

That this Ordinance is hereby declared to be an emergency measure, the emergency being the necessity to adopt a cybersecurity program to be in compliance with ORC Section 9.64. Therefore, this Ordinance shall be in full force and effect immediately upon its passage and approval by the Mayor.

Adopted on this date:

June 22, 2026

Jesse Fark, Mayor

Attest:

James Gooding, Fiscal Officer

CERTIFICATE OF FISCAL OFFICER AS TO POSTING

I certify that the above Ordinance 2026-000 has been posted as required by law. Posted on the village website, and social media page.

Date of Posting: *June 23, 2026*

Signed: _____