VILLAGE OF MINERVA PARK CYBERSECURITY PLAN - 2026

The Village of Minerva Park, recognizing the importance of having an official policy and set of procedures for responding to "cyber incidents", creates the following rules and regulations for dealing with incidents involving breaches of cyber-security on Village-owned and operated computers and computer systems.

SECTION 1: DEFINITION OF A CYBER INCIDENT

A "cyber incident" shall mean any event that:

a) Compromises, or is suspected of compromising, the confidentiality, integrity or availability of the Village's information systems, networks, software or digital data; or

b) Results in unauthorized access, loss, alteration, theft, destruction, or disruption of the Village's digital resources; or

c) Requires investigation by the Village's IT contractors, cyber-security vendors, the Franklin County Prosecutor's office, law enforcement, or other governmental cyber-security authorities.

SECTION 2: INITIAL REPORTING AND NOTIFICATION

Upon identification or reasonable suspicion of a cyber incident:

a) Any Village employee head shall immediately notify the Mayor, the Village Council President and the Village Solicitor;

b) The Village shall immediately work with its IT vendor to begin preliminary containment efforts and document all procedures and findings;

c) The Mayor may authorize engagement of outside cyber-security professionals as necessary.

SECTION 3: CASE-BY-CASE REVIEW BY VILLAGE COUNCIL

Upon receiving notice of a potential cyber incident, Village Council shall convene, either at a regular meeting, special meeting or emergency meeting, to review the facts and circumstances of the cyber incident.

East cyber incident shall be evaluated on a case-by-case basis, taking to account:

a) The nature and severity of the incident;

b) The impact on Village operations or public services;

c) Potential exposure of personal, financial or confidential information;

d) Recommended actions from IT staff or cyber-security professionals;

e) Any legal or regulatory reporting requirements.

After review, Village Council shall determine appropriate actions, which may include:

a) Allocating funds for remediation;

b) Authorizing emergency expenditures;

c) Approving temporary operational adjustments;

d) Directing staff to notify affected individuals, businesses or agencies;

e) Approving policy updates or further security measures.

SECTION 4: RECORDS AND DOCUMENTATION

After every report and review of a cyber incident, a written report shall be completed by Village Council or other appropriate Village staff, which shall include:

a) A summary of the event;

b) The Village's response or action;

c) Findings of any investigation;

d) Recommendations for prevention of similar incidents.

All such reports and other records shall be considered public records, to the extent that no exceptions to the public records laws apply, and all records of all cyber incidents, whether deemed to be public records or not, shall be retained in accordance with Ohio's records retention laws.

SECTION 5: AUTHORITY TO IMPLEMENT PROTECTIVE MEASURES

Nothing in this policy shall prevent the Mayor, IT vendors/contractors, or the Village Solicitor from taking immediate protective actions necessary to preserve Village systems and operations, or to comply with legal obligations prior to Village Council review.

SECTION 6: SEVERABILITY

If any section, clause or provision of this policy is found to be invalid or unlawful, such finding shall not affect the remaining portions of this policy.

Prepared by:

Jesse J. Shamp, Village Solicitor

0128887.0615708 4931-1625-0027v1