*Village of Crooksville,*
*Perry County, Ohio*

**ORC 9.64 (C)**
**RESOLUTION NO. 64-2026**

**A RESOLUTION ADOPTING THE VILLAGE OF CROOKSVILLE'S CYBERSECURITY POLICY AND DECLARING AN EMERGENCY**

**WHEREAS**, the Village of Crooksville utilizes technology for Village business purposes; and

**WHEREAS**, Ohio Revised Code Section 9.64(C) mandates that "[t]he 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"; and

**WHEREAS**, Ohio Revised Code Section 9.64(C) further mandates "[t]he 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

**WHEREAS**, the Village of Crooksville has set to writing a Cybersecurity Policy in compliance with the mandates of Ohio Revised Code Section 9.64(C), a copy of which is attached hereto and incorporated herein by reference; and

**WHEREAS**, in order to adhere to policy adoption deadline and other requirements of Ohio Revised Code Section 9.64(C), and for the general welfare, public safety and health of the Village's residents, it is necessary to pass, adopt and implement this Cybersecurity Policy as an emergency.

**NOW THEREFORE, BE IT RESOLVED** by the Village Council of the Village of Crooksville, Perry County, Ohio, as follows:

1. Pursuant to Ohio Revised Code Section 9.64(C), the Village of Crooksville Cybersecurity Policy, a copy of which is attached hereto and fully incorporated herein by reference, is adopted and implemented as Policy in the Village of Crooksville.

2. This Resolution is hereby declared an emergency measure and shall take effect and be in full force immediately upon its passage, in order to comply with the mandates of Ohio Revised

Code Section 9.64(C) and for the general welfare, public safety and health of the Village's residents.

**1st Reading**: Waived/Suspended on ¾ Vote ;
**2nd Reading**: Waived/Suspended on ¾ Vote ;
**3rd Reading**: Passed on 2/3 Vote July 6, 2026 .

**Passed:** July 6, 2026 .

Christopher Mohler, Mayor Date

ATTESTED:

Courtney Edwards 7/6/26

Courtney Edwards, Fiscal Officer Date

**APPROVED**:

7/6/26

Bill Hampton, Council President Date

Scott Locke, Councilman Date

7/6/26

John Loomis, Councilman Date

7/6/26

Kathy J. McKinney, Councilwoman Date

Billie Smith, Councilman Date

7/6/26

Fred Redfern, Councilman Date

**Posting Certification**

This ordinance was posted at the five prescribed locations within the Village of Crooksville, Ohio, on the 7th day of July, 2026.

Courtney Edwards

Courtney Edwards, Fiscal Officer

**Village of Crooksville**
**HB 96 Cybersecurity Program & Policy**
**Perry County, Ohio**

## 1. Purpose

This Cybersecurity Program is adopted in accordance with **Ohio House Bill 96 (HB 96)** to establish safeguards that protect the confidentiality, integrity, and availability of Village systems, data, and financial operations.
The Village recognizes increasing cybersecurity threats and adopts this program to reduce risk, protect public resources, and maintain compliance with state requirements.

## 2. Scope

This program applies to:

- All Village Officials
- All employees (full-time, part-time, seasonal)
- All Village-owned or managed systems and devices
- All systems used to conduct Village business (including third-party systems such as UAN)

## 3. Village Environment

The Village operates the following systems:

- **Fiscal System:** UAN
- **Number of Council Members:** ____6___
- **Fiscal Officer:** _____1_____
- **Number of Full Time Employees:** ___15____
- **Devices Used:**
  - Desktop Computers
  - Laptops
  - Tablet
  - Personal Devices

## 4. Governance & Responsibilities

### 4.1 Board Members/Trustees

- Adopt and oversee this cybersecurity program
- Review cybersecurity status annually
- Allocate reasonable resources for security controls

### 4.2 Fiscal Officer

- Serves as primary cybersecurity coordinator
- Oversees financial system security (UAN or equivalent)
- Maintains documentation and compliance evidence
- Coordinates incident response

### 4.3 Employees

- Comply with all cybersecurity requirements
- Immediately report suspicious activity

## 5. Risk Management

The Village acknowledges key risks, including:

- Phishing and social engineering attacks
- Ransomware and malware
- Unauthorized system access
- Financial fraud (wire and vendor fraud)
- Loss or theft of devices

The Village mitigates these risks through:

- Strong password controls
- User awareness training
- Controlled system access
- Financial verification processes

**6. Access Control Policy**

- Each user must have **unique login credentials**
- Passwords must:
  - Be at least **12 characters**
  - Include letters, numbers, and symbols
- Passwords must not be shared or written in unsecured locations
- Access is limited to **only what is necessary**
- Accounts must be disabled immediately upon termination

**7. System & Device Security**

All Village devices must:

- Be password protected
- Automatically lock after inactivity
- Use updated antivirus protection (if applicable)
- Receive security updates regularly

**Restrictions:**

- No unauthorized software installation
- No use of unsecured public Wi-Fi for financial transactions
- Personal device use must be limited and approved

**8. Data Protection & Backup**

- Financial data is maintained in **[Software Solutions, UAN]**
- Village ensures:
  - Regular backups (automated where possible)
  - Secure storage of sensitive data
- Sensitive data must not be stored on unsecured personal devices

**9. Email & Phishing Security**

Users must:

- Be cautious of suspicious emails and attachments
- Never click unknown links
- Verify financial requests independently (phone confirmation required)
- Report phishing attempts immediately

**10. Financial Controls (Critical for HB 96 Compliance)**

To prevent fraud:

- Any change to vendor payment information must be:
  - Independently verified by phone
- All unusual or urgent payment requests must be:
  - Verified through a secondary channel
- Dual review is recommended for large transactions

**11. Incident Response Plan**

**11.1 Incident Definition**

An incident includes:

- Unauthorized access
- Malware/ransomware detection
- Suspicious financial activity
- Loss or theft of devices

**11.2 Immediate Actions**

- Disconnect affected device from network
- Notify Fiscal Officer immediately
- Preserve evidence

**11.3 Notification**

The Fiscal Officer will:

- Inform the Village Council
- Contact relevant support (e.g., UAN helpdesk)
- Notify law enforcement if necessary

**11.4 Recovery**

- Restore systems from backup (if needed)
- Reset passwords
- Document incident and corrective actions

**12. Training Requirements**

All Village personnel must receive **annual cybersecurity training**, covering:

- Phishing awareness
- Password security
- Financial fraud prevention

Training may include:

- OTARMA resources
- Auditor of State materials
- Free online cybersecurity awareness training

**13. Vendor & Third-Party Management**

- The Village will only use trusted vendors
- Vendors must:
  - Access only necessary systems
  - Use secure methods
- No vendor may install software without approval

**14. Physical Security**

- Devices must be stored securely
- Office areas should be locked when unattended
- Sensitive documents must be securely stored and disposed of properly

---

**15. Acceptable Use Policy**

Village systems may only be used for official business.
Users may not:

- Download unauthorized software
- Access unsafe websites
- Use Village systems for personal business

---

**16. Data Retention & Disposal**

- Follow Ohio public records retention schedules
- Dispose of sensitive records securely (e.g., shredding)
- Ensure electronic data is properly deleted when no longer needed

---

**17. Compliance & Review**

- This program is intended to meet **HB 96 requirements**
- The Village will:
    - Review this policy annually
    - Update as needed
    - Document compliance efforts

---

**18. Documentation Checklist for The Village of Crooksville**

✓ Adopted cybersecurity policy
✓ Incident response documented
✓ Training completed annually
✓ Password controls in place
✓ Financial verification procedures established
✓ Vendor list maintained