THE SUMMIT AND MEDINA WORKFORCE AREA COUNCIL OF GOVERNMENTS FOR OHIO LOCAL WORKFORCE AREA 2
RESOLUTION 2026-09

A Resolution approving and adopting the Summit and Medina Workforce Area Council of Governments Cybersecurity Policy and confirming the applicability of confidentiality provisions under Ohio Revised Code § 9.64(E).

WHEREAS, R.C. § 9.64(C), enacted by House Bill 96 (136th G.A.), requires the adoption of a cybersecurity program, or policy, by the legislative authority of each political subdivision, with the deadline, established by the Auditor of State for this type of governmental body to adopt the plan, of July 1, 2026; and

WHEREAS, the purpose of this requirement is to strengthen protections of public data, information systems, and technology resources from cybersecurity threats and risks; and

WHEREAS, the Summit and Medina Workforce Area Council of Governments (SAMWA COG) Executive Director and Deputy Director, with the assistance of legal counsel and the Director of the County of Summit Office of Information Technology, have prepared a Cybersecurity Policy (the "Policy"), attached hereto as Exhibit A, and recommends its approval and adoption; and

WHEREAS, pursuant to R.C. § 9.64(E), any records, documents, or reports related to the cybersecurity program and framework, including Exhibit A referenced above, are not public records under R.C. § 149.43; and

WHEREAS, the SAMWA COG finds and determines, after reviewing all pertinent information, that it is necessary and in the best interest of Area 2 to approve the SAMWA COG Cybersecurity Policy.

NOW, THEREFORE, BE IT RESOLVED, by the SAMWA COG that:

SECTION 1
The SAMWA COG hereby approves and adopts the Cybersecurity Policy attached hereto as Exhibit A, with the details of said Cybersecurity Policy, identified in Exhibit A, being exempt from public disclosure under R.C. § 9.64(C).

SECTION 2
This Directive shall take effect immediately upon its adoption.

Ayes: 2
Nays: 0
Abstain: 0
Absent: 0

ADOPTED, this 25th day of June, 2026.

THE SUMMIT AND MEDINA WORKFORCE AREA COUNCIL OF GOVERNMENTS
FOR OHIO LOCAL WORKFORCE AREA 2
RESOLUTION 2026-09

Summit County Executive

Medina County Commissioner

SAMWA COG Cybersecurity Program

Effective Date: July 1, 2026

Legislative Authority: Resolution No. 2026-09

1. Purpose & Scope

This Cybersecurity Program establishes the **Summit and Medina Workforce Area Council of Government's (SAMWA COG)** security governance, safeguarding the information systems, data, and infrastructure of all charter agencies. It satisfies the requirements of **Ohio House Bill 96**, including risk management, asset protection, training, incident preparedness, and third-party oversight.

2. Governance & Responsibilities

- The SAMWA COG owns and maintains the Cybersecurity Program, policies, and security architecture
- The SAMWA COG Deputy Director, with the assistance of the Summit County Office of Information Technology, provides strategic oversight and cybersecurity program review and reports to the SAMWA COG Executive Director
- The SAMWA COG approves cybersecurity policies and receives program status updates
- **All Employees** must comply with policy, complete annual training, and promptly report incidents

3. Risk Management & Controls

SAMWA COG uses a layered defense-in-depth approach to prohibit a variety of cyberattacks.

Technical Controls

- **Endpoint Detection & Response (EDR):** Microsoft Windows Defender and Cynet is on all SAMWA COG computers and provides 24/7 threat detection and escalation.

Cybersecurity Program

- Multi-Factor Authentication: Microsoft is used for all user logins and remote access; expansion to sensitive systems is in progress.
- Back & Recovery: Microsoft Office 365 provides backup resiliency.

- Patch Management: application patch cycles are managed through Microsoft Windows security.

Administrative & Physical Controls

- An annual risk assessment and review of security posture is conducted.
- The principle of least privilege is applied to all user accounts (in process).
- Secure configuration standards are applied to servers, endpoints, and network equipment.
- Data center access is controlled, and facility safeguards are maintained.

4. Training & Awareness

- All users must complete one hour of cybersecurity awareness training annually.
- Phishing simulations are conducted regularly to strengthen user vigilance.
- Phish reporting is provided via Microsoft Outlook.
- Targeted training is provided for privileged and technical staff (in progress).

5. Vendor & Third-Party Management

- Security considerations are incorporated into procurement and contract reviews.
- Vendors with access to SAMWA COG systems must meet minimum cybersecurity requirements.
- Third-party risk is assessed and reviewed annually (in progress).

6. Program Review & Updates

This Cybersecurity Program is reviewed **annually** by the SAMWA COG Deputy Director, with updates submitted to the SAMWA COG. Adjustments are made to reflect emerging threats, new technologies, and legal or regulatory changes.