

**RESOLUTION TO ADOPT THE ASHTABULA COUNTY INCIDENT RESPONSE GUIDE (CYBER SECURITY) BASED ON NIST CYBERSECURITY FRAMEWORK**

WHEREAS, pursuant to Ohio Revised Code Section 9.64, as enacted through House Bill 96, political subdivisions are required to adopt a cybersecurity program designed to safeguard public data, information technology, and information technology (IT) resources to ensure the confidentiality, availability, and integrity of such systems and information; and

WHEREAS, Ohio Revised Code Section 9.64 requires that the cybersecurity program be based upon generally accepted cybersecurity best practices, including nationally recognized frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) best practices; and

WHEREAS, the Ashtabula County Board of Commissioners has reviewed the recommendations of County technology and information security personnel and finds it appropriate to adopt the NIST Cybersecurity Framework as the foundational cybersecurity controls framework for the County; now

THEREFORE, BE IT RESOLVED BY THE **BOARD OF COMMISSIONERS OF ASHTABULA COUNTY, OHIO:**

**SECTION 1.**

The Board of Commissioners hereby adopts the Ashtabula County Incident Response Guide based on the NIST Cybersecurity Framework, consistent with the requirements of Ohio Revised Code Section 9.64(C) and aligned with generally accepted cybersecurity best practices, including the National Institute of Standards and Technology (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 cybersecurity threats, restore affected systems, and maintain ongoing protection of County assets and data. The program shall include annual cybersecurity training for County employees, align with applicable state and federal best practices, and require third-party service providers to meet appropriate security standards, with the goal of achieving practical, measurable, and cost-effective improvements in defending against cyber threats, including ransomware and phishing.

**SECTION 3.**

The Chief Information Officer, as designated within the cybersecurity program, in coordination with the County Auditor, and appropriate public safety officials, shall oversee the implementation, documentation, and annual review of the cybersecurity program to ensure continued compliance with state law and alignment with best practices.

**SECTION 4.**

All records, documents, plans, and information related to the County's cybersecurity program are exempt from public records disclosure, to the extent permitted, pursuant to Ohio Revised Code Section 9.64(E).

**SECTION 5.**

The Board of Commissioners finds and determines that all formal actions of this Board concerning and relating to the adoption of this Resolution were taken in an open meeting of the Board, and that all deliberations of the Board and any of its committees that resulted in such formal actions were conducted in meetings open to the public in compliance with Ohio Revised Code Section 121.22.

**SECTION 6.**

This Resolution shall take effect immediately upon its adoption.

**ASHTABULA COUNTY COMMISSIONERS  
CERTIFICATION PAGE**

Resolution No. 2025-564

December 23, 2025

**RESOLUTION TO ADOPT THE ASHTABULA COUNTY INCIDENT RESPONSE  
GUIDE (CYBER SECURITY) BASED ON NIST CYBERSECURITY FRAMEWORK**

Upon the motion of Kathryn L. Whittington, seconded by Casey R. Kozlowski.

**VOTE:**

J.P. Ducro IV

Aye

Casey R. Kozlowski

Aye

Kathryn L. Whittington

Aye

**CERTIFICATE OF CLERK**

IT IS HEREBY CERTIFIED that the foregoing is a true and correct transcript of a resolution acted upon and duly passed by the Board of County Commissioners of Ashtabula County, Ohio, on the date noted above.

*Lisa Hawkins*

---

Lisa Hawkins, Clerk of the Board  
Board of County Commissioners  
Ashtabula County, Ohio