RESOLUTION NO. 2026-09

ADOPTING A CYBERSECURITY POLICY

WHEREAS, the Port of Greater Cincinnati Development Authority (The "Port") is a body corporate and politic duly organized and validly existing under the laws of the State of Ohio; and

WHEREAS, the State of Ohio has implemented Ohio Revised Code §9.64, enacted in House Bill 96, requiring the legislative authority of political subdivisions in Ohio to 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, The Port has existing cybersecurity measures in place, most recently earning a BitSight rating of "Advanced," and wishes to further enhance its cybersecurity program as well as formalize a cybersecurity policy in compliance with Ohio Revised Code §9.64; and

WHEREAS, the Board of Directors of The Port wish to adopt the Cybersecurity Policy attached to this Resolution as **Exhibit A**:

NOW, THEREFORE, BE IT RESOLVED by the Board of the Port of Greater Cincinnati Development Authority:

Section 1. The Board hereby adopts the Cybersecurity Policy attached as **Exhibit A** in compliance with Ohio Revised Code §9.64. The Board authorizes The Port to update the policy from time to time as needed to comply with the statute.

Section 2. This Board finds and determines that all formal actions of this Board concerning and relating to the adoption of this resolution were taken, and that all deliberations of this Board that resulted in such formal action were held in meetings open to the public in compliance with the law.

Section 3. This resolution shall be in full force and effect upon its adoption.

Adopted:

Yeas: 10

Nays: 0

Chairperson

Attest: _____
Secretary

EXHIBIT A

PORT OF GREATER CINCINNATI DEVELOPMENT AUTHORITY
CYBERSECURITY POLICY

Purpose. The purpose of the Port of Greater Cincinnati Development Authority (The "Port") Cybersecurity Policy (the "Policy") is to establish a framework for protecting the availability, confidentiality, and integrity of The Port's data, information technology, and information technology resources in compliance with Ohio Revised Code §9.64. The Port is committed to safeguarding its information systems against cybersecurity threats by establishing baseline cybersecurity practices, providing ongoing cybersecurity awareness training, preparing for detection of and response to incidents, and periodically reviewing and updating its cybersecurity program as necessary.

Scope. The Policy applies to all employees, officials, contractors, vendors, and third parties who access or manage The Port's technology resources, including but not limited to the following:

- Computers, servers, and mobile devices
- Cloud services and hosted applications
- Networks and telecommunications systems
- Sensitive or confidential data

Roles and Responsibilities.

1. **Board of Directors**: Approve Cybersecurity Policy and ensure resources are allocated
2. **Information Technology Managers/Administrators**: Oversee policy implementation and coordinate with external providers and legal counsel
3. **IT Providers/Consultants**: Implement technical safeguards, monitor for threats, report incidents, assist with incident response
4. **Employees/Users**: Follow cybersecurity protocols, complete training, and report suspicious activity

Cybersecurity Controls.

1. **Access Control**
   - Require unique User IDs and strong passwords
   - Enforce multifactor authentication (MFA) for remote or administrative access
   - Limit access to sensitive data

2. **Network and System Security**
   - Maintain up-to-date firewalls, antivirus, and intrusion detection/prevention
   - Apply software patches and updates within 30 days of release

3. **Data Protection**
   - Encrypt sensitive data in transit
   - Regularly back up critical data and test restoration procedures
   - Retain records in compliance with The Port's records retention schedule

4. **Incident Response**
    - Designate an incident response lead
    - Establish procedures for detecting, reporting, and escalating incidents
    - Notify the executive director of the Division of Homeland Security within the department of public safety, in a manner prescribed by the executive director, as soon as possible but not later than seven days after discovery of the incident
    - Notify the Auditor of State, in a manner prescribed by the Auditor of State, as soon as possible but not later than 30 days after discovery of the incident
    - Notify law enforcement as appropriate
    - Notify insurance providers as appropriate
    - Do not pay ransom or respond to ransom demands absent authorization from the Board of Directors
    - Conduct a post-incident review and update policies as needed

5. **Training and Awareness**
    - Require all employees to complete cybersecurity training annually
    - Require role-specific training for administrators and staff handling sensitive data

6. **Vendor Management**
    - Require IT vendors/consultants to comply with this Policy and The Port's cybersecurity standards
    - Maintain the inclusion of cybersecurity clauses and breach notification requirements in contracts as appropriate

Compliance and Review. This Policy will be reviewed annually by Port management and updated as necessary to reflect changes in technology, law, and organizational needs.

Enforcement. Violations of this Policy may result in disciplinary action up to and including termination of employment or contract, as well as potential criminal penalties in accordance with applicable law.

Cybersecurity Program and Records Not Public Records. Records, documents, or reports related to The Port's cybersecurity policy, program, and framework are not public records under Ohio Revised Code §9.64.