RESOLUTION 2025-113

BORDENTOWN SEWERAGE AUTHORITY
COUNTY OF BURLINGTON

A RESOLUTION ADOPTING TECHNOLOGY RISK MANAGEMENT STANDARDS IN COMPLIANCE WITH THE NEW JERSEY MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND'S CYBER RISK MANAGEMENT PLAN'S BASIC SECURITY REQUIREMENTS

Whereas, the Bordentown Sewerage Authority is a member of the New Jersey Utility Authorities Joint Insurance Fund which secures insurance protection through the New Jersey Municipal Excess Liability Joint Insurance Fund (NJ MEL); and

Whereas, through its membership in the New Jersey Utility Authorities Joint Insurance Fund, the Bordentown Sewerage Authority enjoys cyber liability insurance coverage to protect the Bordentown Sewerage Authority from the potential devastating costs associated with a cyber related claim; and

Whereas, in an attempt to prevent as many cyber related claims as possible, the NJ MEL developed and released to its members the NJ MEL Cyber Risk Management Plan; and

Whereas, the NJ MEL Cyber Risk Management Plan outlines a set of best practices and standards broken out into Basic, Intermediate, and Advanced Security standards that if adopted and followed will reduce many of the risks associated with the use of technology by the Bordentown Sewerage Authority; and

Whereas, in addition to the reduction of potential claims, implementing the following best practices and standards will enable the Bordentown Sewerage Authority to claim a reimbursement of a paid insurance deductible in the event the member files a claim against Bordentown Sewerage Authority's cyber insurance policy, administered through the New Jersey Utility Authorities Joint Insurance Fund and the Municipal Excess Liability Joint Insurance Fund;

Now Therefore Be It Resolved that the Bordentown Sewerage Authority does hereby adopt the following best practices and standards, a copy of which is attached hereto and incorporated herein by reference, in accordance with Basic Security of the NJ MEL Cyber Risk Management Plan;

Data Management and Recovery
Security Patches and Updates
Defensive Software
Security Awareness Training
Access Control Management
Email Warning
Incident Response Plan
Government Cyber Membership

And, Be It Further Resolved, that a copy of this resolution along with all required checklists and correspondence be provided to the NJ MEL Underwriter for their consideration and approval.

Date of adoption: September 15, 2025

THE BORDENTOWN SEWERAGE AUTHORITY

By: M. Ellen Gulbinsky
M. Ellen Gulbinksy, Chairwoman

ATTEST:

Aneka Miller, Secretary

Basic Security

Control	CIS v8	Description	Completed
Data Management	Data Recovery (CIS 11)	1. Weekly, off-network, off-premises full backup of all data.	Completed
Account Management	Access Control Management (CIS 6)	1. Must implement a password policy that at least meets the standards set in the attached Cyber JIF Password Policy or meet the NIST Password Standards 800-63B (03/02/2020 Updates), and as further updated. 2. Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections to your network.	Completed
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Implement a practice of installing all security and critical updates and patches as soon as practicable based on risk and operational impact, but no longer than a month for high and critical vulnerabilities as defined by CVSS. 2. Scan your ecosystem with a vulnerability management tool on a monthly or more frequent basis.	Completed
Cyber Hygiene	Security Awareness and Skills Training (CIS 14)	1. All computer, network or email users receive annual training of at least one hour, including these topics, with such training including phishing exercises: a. Malware Identification b. Password construction c. Identifying and responding to security incidents d. Social engineering attacks 2. Leadership briefed annually on state of security for the organization, including high impact incidents (breach/loss of PII, funds fraud, intrusion, etc.). 3. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC) and New Jersey Cybersecurity Communication and Integration Cell (NJCCIC). If a Utility Authority, register with your respective ISAC, such as Water ISAC.	Completed
Policies & Procedures	Incident Response Management (CIS 17)	1. Management implements a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place, which must include at a minimum the items in the Cyber JIF's Cybersecurity Incident Response Plan. 2. Banking Controls: Establish wire and/or ACH payment procedures in accordance with the JCMI Banking Best Practices (10-31-23).	Completed BSA
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	1. Inventory your technology ecosystem: Workstations, end-user devices, network devices, servers, etc.	Completed
	Inventory and Control of Software Assets (CIS 2)	1. Inventory your technology ecosystem: Software: Operating systems and applications	Completed

Any "No" or "N/A" responses for which you are requesting an exception must be accompanied by a detailed explanation for our review.

Certification

This document must be signed by the mayor, municipal administrator, or municipal clerk (or director of entity if not a municipality) AND your technology expert.

MEMBER ENTITY

Charles Bluhm, Jr
Print Name

Executive Director
Title

Signature

9/3/2025
Date

TECHNOLOGY EXPERT

Marc Macanas
Print Name

IT Manager
Title

Signature

8/28/2025
Date