Bordentown Sewerage Authority

Master Technology Policy

Version 2.2

MEL Cyber Risk Management Program

Document Management

Document Owner:	**Bordentown Sewerage Authority**
Document Name:	Master Technology Policy
Version No:	2.2
Adoption Date:	1/13/2023
Distribution Date:	1/13/2023
Author (Source):	Lou Romero, Secure Data Consulting Services Lromero@SecureDataCS.com
Last Review Date:	1/13/2023
Next Review Date:	1/13/2024
Data Classification:	**Sensitive**

Table of Contents

It is essential to review these policies with a qualified and experienced Information Technology professional to ensure proper understanding and implementation.

1. Policy Statement

The Information Technology Policy defines the information security practices necessary to ensure the security of the member's information systems and the information it stores, processes, and/or transmits.

2. Reason for the Policy

We act as the custodian of a wealth of sensitive information relating to the services we provide and the constituents we serve. We also rely on information technology for much of our daily operations. Accordingly, an appropriate set of security measures must be implemented to guard against unauthorized access to, alteration, disclosure, or destruction of this information and/or the information systems that store, process, or transmit the information.

This policy affirms our commitment to information security by specifying the policies and standards necessary to achieve our security objectives, including compliance with all Federal and State requirements, as well as the Municipal Excess Liability Joint Insurance Fund's (MEL) Minimum Technology Proficiency Standards.

3. Scope

All information systems and users are expected to comply with this policy.

4. Tier 1 Operational Policies

The member shall implement practices and policies that meet or exceed the MEL's requirements at a minimum.

4.1. Information Backup Policy

Objective:

The objective of the Information Backup Policy is to ensure all data is regularly "backed up" and available when needed in the event of an incident (e.g., ransomware, flood, fire, etc.). If the network is virtual, meaning no local data is stored on devices, the requirement to backup devices does not apply.

Requirements:

a) Use of standardized system images or virtualized desktops
b) A back-up of applications, operating systems and network configuration software must always be available
c) Daily incremental backups with a minimum of 14 days of versioning on off-network device of all data
d) Weekly, off-network, full back-up of all data
e) All backups are spot-checked monthly
f) Third-party and cloud-based application data must also be backed-up to the same standards

4.2. Patch Management Policy

Objective:

The objective of the Patch Management Policy is to ensure all systems and applications are patched on a regular basis. Outdated and/or unsupported operating systems/applications shall not be used.

Requirements:

Patch all operating systems, applications, and infrastructure equipment with latest versions.

a. Use automatic updating where practicable, particularly as related to security patches.

b. All security and critical updates and patches are installed as soon as possible following release. Following are examples:

   - Microsoft products (Windows, Desktops, Servers, Office, SQL Data Bases, Outlook, etc.)
   - Search engines (Google, Firefox, Microsoft Edge, Bing, etc.)
   - Technical infrastructure equipment that requires regular security updates (switches, firewalls, routers, etc.)
   - Third-Party applications (finance, animal license, construction, code enforcement, etc.)

c. Annually review all non-standard applications for possible replacement/upgrade

4.3. Defensive Software Policy

Objective:

The objective of the Defensive Software Policy is to ensure all systems are protected by software that minimizes the likelihood of an attack by malicious individuals and/or malware that can compromise the confidentiality, integrity and availability of that system or information.

Requirements:

a. Antivirus and firewalls are enabled for all desktops and laptops
b. Antispam and antivirus filters are enabled for all email servers
c. Firewalls, switches, routers, and any interconnecting devices must ensure unused or non-active ports are closed
d. Antivirus and antimalware must be enabled for network servers that connect to the internet
e. Firewall rules and policies need to be reviewed at least twice per year
f. All Microsoft Office applications automatically open all downloaded files in “Protected Mode”

4.4. Security Awareness Training Policy

Objective:

The objective of the Security Awareness Training Policy is to ensure all personnel with access to the member’s technology assets receive appropriate cyber awareness education to reduce the likelihood of a cyber incident by understanding potential cyber threats.

Requirements:

All personnel with access to the member's technology assets shall receive annual training of at least one hour that includes malware identification (email and websites), password construction, identifying security incidents, and social engineering.

4.5. Password Policy

Objective:

The objective of the Password Policy is to ensure that users construct passwords that minimize the likelihood of unauthorized access to the member's data and information systems.

Requirements:

There are two options for compliance: 1) Follow the set of standards below; or 2) Follow the NIST Password Standards 800-63B (03/02/2020 Updates).

Option 1

1- **Change Frequency**
   a. Network users' passwords are updated every three (3) months.
2- **Construction**
   b. Passwords must be unique from passwords used on all other programs, websites, devices, etc., both personal and work.
   c. Passwords must be a minimum of ten (10) characters.
   d. Sequential or repetitive characters of more than two in succession are not to be permitted.
      - Example: "123", "AAA", etc.
   e. Commonly used passwords are not to be permitted.
      - Example, "password", "123456789", "qwerty", "abc123", etc.
      - Full lists of commonly used passwords can be found in various cybersecurity reports.
   f. Context-specific words are not to be permitted.
      - Example, the name of the application or website being logged into.
3- **Previously Breached Passwords**
   The member shall implement a process for identifying breaches containing user email addresses and utilize a breach corpus search for breached passwords, and such passwords shall be updated and not used again.
4- **Failed Login Lockout**
   The user account shall be locked out after five (5) failed attempts for a period of no less than 30 minutes. In lieu of a timed lockout, the member may utilize a positive identification process to unlock the account.

Option 2 – (NIST)

1- **Failed Login Lockout**
   a. Limit the number of failed authentication attempts

2- **Password**
   a. Suggest users use "memorized secrets" instead of passwords
   b. Memorized Secrets are secret values intended to be chosen and memorized by the user; something you know.

3- Length

a. 8 characters minimum to at least 64 characters maximum

4- Change

a. Only change if there is evidence of compromise

5- Screening

a. Screen passwords against a list of known compromised passwords

6- Hints

a. Disable password hints and knowledge-based security questions

7- Composition Minimums

a. Skip character composition rules

8- Composition Restrictions

a. Do not allow
   I. Dictionary words
   II. Repetitive or sequential characters
   III. Context-specific words (i.e. service name or username)

9- Copy & Paste

a. Allow copying and pasting passwords from a password manager

10- Other Characters

a. Allow ASCII and UNICODE, including emojis

4.6. Email Warning Policy

Objective:

The objective of the Email Warning Policy is to reduce spoofing emails and social engineering emails by identifying when emails are coming from outside the organization.

Requirements:

Example of email warning label:

CAUTION:

This email originated from outside of our email domain. Do not click on links or open attachments unless you recognize the sender and know the content is safe. If unsure, do not reply to this email and call the sender directly.

4.7. Cyber Incident Response Plan

Objective:

The objective of the Incident Response Plan is to define the methods for identifying, tracking, and responding to technology security incidents.

Requirements:

Please refer to the Incident Response Plan.

Incident Response Plan - Ver 2.0.docx

4.8. Technology Practice Policy

Objective:

The objective of the Technology Practice Policy is to ensure management/governing bodies adopt a Technology Practices Policy that includes all the subject items outlined in the MEL Cyber Risk Management Program.

Guidelines:

This document shall serve as the Technology Practice Policy.

4.9. Government Cybersecurity Membership Policy

Objective:

The objective of the Cyber Government Membership policy is to ensure the member stays current with cyber threat notifications and relevant information.

Requirements:

The member shall register and become a member of New Jersey Cybersecurity Communications Integration Cell (NJCCIC) and Multi-State Information Sharing and Analysis Center (MS-ISAC). Both required below are free.

New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) - https://www.cyber.nj.gov/

The New Jersey Cybersecurity and Communications Integration Cell is the state's one-stop shop for cybersecurity information sharing, threat intelligence, and incident reporting. Acting in a cyber fusion center capacity, the NJCCIC is a component organization within the New Jersey Office of Homeland Security and Preparedness.

The NJCCIC works to make New Jersey more resilient to cyberattacks by promoting statewide awareness of cyber threats and widespread adoption of best practices. We provide a wide array of cybersecurity services, including the development and distribution of cyber alerts and advisories, cyber tips, and best practices for effectively managing cyber risk. Other services include threat briefings, risk assessments, incident response support, and training.

Multi-State Information Sharing & Analysis Center (MS-ISAC) - https://www.cisecurity.org/ms-isac/

The mission of MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

5. Tier 2 Operational Policies

5.1. Server Security Policy

Objective:

The objective of the Server Security Policy is to prevent unauthorized physical access, damage, and interference to the member's server(s) and network equipment.

Requirements:

The member's servers and network equipment shall be protected by defined barriers with restricted access controls and must not be in common public areas. The servers and network equipment may be stored in an enclosed cabinet, data closet, or office with secure entries and adequate ventilation.

5.2. Access Privilege Controls Policy

Objective:

The objective of the Access Privilege Control Policy is to control access to all technology digital assets. Access to all technology shall be controlled by role-based access controls.

Requirements:

a. System and Network administrative rights are to be limited to those who are authorized to make changes to the systems, computers, and network.
b. Network and system access to file and folders are granted based on the individual's job function and level of responsibility.
c. Access rights need to be reviewed and updated upon any personnel change. Exiting employees' access must be revoked immediately upon separation.
d. A review process is to be implemented to ensure access rights are up to date. Minimal review frequency is six (6) months.

5.3. Technology Support Policy

Objective:

The objective of the Technology Support Policy is to ensure the member has the technical support expertise and structure in place to effectively mitigate and triage information technology and cyber related issues.

Requirements:

Technical support can be provided by a qualified and experienced employee or vendor.

5.4. System and Event Logging Policy

Objective:

The objective of the Logging Policy is to ensure system activities, information security events, and system utilization and performance are captured.

Requirements:

The member shall use the following Microsoft logs (or similar for other operating systems) to monitor system activities, information security events, and system utilization and performance.

a- System
b- Application
c- Security

Note: There are numerous free and for-cost log management tools on the market.

5.5. Protected Information Policy

Objective:

The objective of the Protected Information Policy is to ensure all digital files and data containing sensitive information, Personally Identifiable Information (PII), and Protected Health Information (PHI) are protected in accordance with statutory, regulatory, and contractual requirements.

Requirements:

All digital documents containing Personally Identifiable Information (PII), Protected Health Information (PHI) and documents deemed by the member as sensitive shall be encrypted.

5.6. Remote Access Policy

Objective:

The purpose of Remote Access Policy is to secure remote access connectivity into the member's network using a Virtual Private Network (VPN).

Requirements:

The member shall deploy a Virtual Private Network (VPN) for those who need to remotely access the member's network. Only approved users, third-parties, vendors, and contractors may utilize the VPN service to connect to the member's network. VPN profiles shall be created upon request from the relevant department head, approving authorities, or designated sponsor.

Using Personal Devices:

The following requirements only apply to those approved users, third-party, vendor or contractors who use their personal devices to access the member's network.

- All personal devices must be up to date with all applicable operating systems, security patches and virus/malware protection software.
- Users with remote access privileges shall ensure their remote access connection is used explicitly for member work and used in a manner consistent with their on-site connection to the member's network.
- Personal equipment shall not be used to connect to the member network unless authorized and approved in writing by someone in senior management charged with approving cybersecurity changes.
- VPN users are automatically disconnected from the member network after thirty (30) minutes of inactivity. The user must then logon again to re-authenticate in order to reconnect to the network.
- All personal devices are required to use a password to protect from tampering using the same standards and requirements as the member's equipment.
- The member shall not allow remote users to save any data to their personal devices (i.e. member can utilize Content Access Controls or a Cloud Access Security Broker).

5.7. Leadership Expertise Policy

Objective:

The objective of the Leadership Expertise Policy is to ensure the member's senior management has access to resources with expertise in their respective fields to support technology decision making, such as risk assessments, planning, budgeting, etc.

Requirements:

The member's senior management shall have access to resources with expertise in their respective fields leveraging their IT support and the JIF's or MEL's available resources.

5.8. IT Business Continuity Plan Policy

Objective:

The objective of the IT Business Continuity Plan Policy is to ensure the member is prepared and can effectively recover from a disruption in service, including cyber breaches, denial of service or ransomware attacks, and be able to restore continuity of operations.

Requirements:

The Emergency Management/Continuity of Government (CoG) plan shall include an IT Business Continuity Plan as part of its Disaster Recovery section.

When developing an IT Business Continuity Plan the member shall consider the following:

Recovery Strategies

5.1. Identify all operational functions

5.2. Identify key support personnel and communications plan

5.3. Prioritize based on Recovery Time Objectives (RTOs)
5.4. Consider and accommodate the following impacts:
- ✓ Loss of Computing (Systems and Data)
- ✓ Loss of Telecommunications
- ✓ Loss of Personnel
- ✓ Denial of Physical Access
- ✓ Critical vendors' services

5.9. Banking Control Policy

Objective:

The objective of the Banking Control Policy is to prevent or reduce fraudulent banking transactions.

Requirements:

The member shall implement internal controls to minimize fraudulent banking transactions. The following are required:

- Use Multi-Factor Authentication when accessing the bank's system and making financial transactions, where available.
- Establish procedures requiring multiple approvals for request to change banking information.
- Establish procedures requiring multiple approvals and source verification for financial transaction requests over $5,000.

6. Tier 3 Operational Policies

6.1. Network Segmentation Policy

Objective:

The objective of the Network Segmentation Policy is to reduce the spread of a cyber-attack by dividing the network into multiple zones or sub-networks and applying security protocols to each zone. The member shall consider isolating key business units or sensitive departments, such as finance and human resources.

Requirements:

Divide the network into multiple zones or sub-networks, virtually or physically, and apply security protocols to each zone. The member shall consider isolating key business units or sensitive departments, such as finance and human resources.

Utilities shall have an "air gap" between their primary network and their Industrial Control System (ICS) / SCADA system. An air gap is a network security measure that physically isolates one network from another to prevent external connections.

6.2. Remote Access Policy

Objective:

The objective of the Remote Access Policy is to enhance the security level by adding a second layer of authentication when remotely accessing the member's network, as well as giving the member certain controls over the device remotely accessing the network.

Requirements:

This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.). Consider using Network Access Control (NAC) to limit remote network access to only pre-approved devices.

MFA shall be enabled for the following remote connections:

- Member's network
- Email service (if cloud based)
- Third-Party applications that store or transmit PII or PHI information

The following Remote Security Controls shall be enabled for devices remotely accessing the above connections:

- The member shall require employees to immediately report a lost or stolen device.
- The member shall maintain the ability to remotely wipe a user's member-owned device.
- The member shall maintain the ability to disconnect any user from the member's network.

6.3. Password Integrity Policy

Objective:

The objective of the Password Integrity Policy is to frequently validate users' emails and passwords to ensure they have not been compromised.

Requirements:

The member shall implement a process where user emails are checked against an email breach service, such as HaveIBeenPwned, to determine if any email addresses have been compromised. Member must take necessary action to ensure integrity of any emails found to in the breach database.

The HaveIBeenPwned website is: https://haveibeenpwned.com/

6.4. System and Event Logging Policy

Objective:

Logs shall be reviewed every three (3) months by the IT professional.

Requirements:

Logs shall be reviewed every three (3) months by the technology professional.

Note: There are numerous free and for-cost log management tools on the market.

6.5. Third-Party Risk Management Policy

Objective:

The objective of the Third-Party Risk Management (TPRM) Policy and Procedure is to ensure the protection of information that is accessible to outside vendors. It is important to properly identify and manage risks associated when working with third-party vendors.

Requirements:

Vendor Review Process *(New and Existing Vendors)*

A Vendor Review shall take place for those vendors/partnerships who store, handle, access, and/or transmit any of the following sensitive data:

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial information
- Credit card information
- Access to the member's information system and/or computer network
- Any asset deemed sensitive and/or of value

The Vendor Review shall be in the form of an extensive Third-Party Security Questionnaire (attached and embedded below) which shall be forwarded to the vendor for completion. Following receipt of the questionnaire and any requested supporting documentation, the *Vendor Relationship Manager*** shall engage the appropriate qualified and experienced professionals, including their Risk Manager, to review and opine on the information provided. The overall risk associated with the selection of the vendor shall be carefully considered.

***Vendor Relationship Manager* – Person responsible for the service, product, or agreement being requested.

Third-Party Security Questionaire - Ver 2.0

Technology Vendors

It is paramount to select an IT vendor that has the expertise, experience, and certification to effectively design, implement, manage, and maintain your information system.

Requirements:

The following is a sample list of items that should be considered:

- Do they have the experience?
- Are they reliable and with references?
- Do they stay current with technology and trends?
- Can they perform manufacturer's warranty work?

- Do they provide a contract with Service Level Agreements (SLA)?
- Do they recommend ways to improve the performance and security of your network?
- Can they recommend how to design your network with security controls in mind?
- Can they design a network with redundancy built in to recover from a major incident?

Use the IT Support Certification Guidelines below when selecting an IT vendor.

IT Support Certification Guidelines

Use these guidelines when selecting an IT vendor to support your IT infrastructure.

Industry Standard Certifications	Certifications required based on support role					
	Help Desk Support	PC / Printer Repair	Server Repair & Support	System Administration	Network & Infrastructure Support	Information Security
HDI technical support professional certification	✓					
CompTIA IT Fundamentals (ITF+)	✓	✓				
CompTIA A+	✓	✓	✓	✓		
CompTIA Network +			✓	✓	✓	
CompTIA Server +			✓	✓	✓	
CompTIA Security +			●	●	✓	✓
MCSE			●	✓	●	●
CCNA					✓	✓
CISSP						✓
CEH						✓

CompTIA IT Fundamentals (ITF+)	Entry level certification focusing on essential IT skills and knowledge such as the functions and features of common operating systems, establishing network connectivity, security best practices and how to identify common software applications.
CompTIA A+	The certification focuses on validating nine major IT skills, including hardware, operating systems, software troubleshooting, networking, hardware and network troubleshooting, security, mobile devices, virtualization and cloud computing and operational procedures.
CompTIA Network +	The certification focuses on configuring, managing, and maintaining network devices, implementing, and designing functional networks, network troubleshooting and network security.
CompTIA Server +	The certification focuses on knowledge of server hardware and technology as well as troubleshooting and repairing server issues, including disaster recovery.
CompTIA Security +	The certification focuses on threats, attacks and vulnerabilities, risk management, architecture and design, technology and tools, cryptography and PKI and identity and access management.
MCSE Microsoft Certified Systems Engineer	Though Microsoft has retired the MCSE certification program as of June 30, 2020, the certification focuses on designing, managing, and supporting Windows products and architecture.
CCNA Cisco Certified Network Associate	The CCNA certification focuses network fundamentals, network access, IP connectivity, IP services, security fundamentals and automation and programmability.
CISSP Certified Information Systems Security Professional	The CISSP certification focuses on critical security issues, including risk management, cloud computing, application development security, mobile security, etc.
Certified Ethical Hacker	The CEH certification specializes in penetration testing, vulnerability testing, and cyber forensics analysis.

● Optional or preferable certifications but not required