

BOROUGH OF BUENA
MUNICIPAL UTILITIES AUTHORITY

RESOLUTION ADOPTING THE
CYBER RISK MANAGEMENT PROGRAM
AND CYBER INCIDENT RESPONSE PLAN
IN COMPLIANCE WITH THE
NEW JERSEY MUNICIPAL EXCESS LIABILITY
JOINT INSURANCE FUND

R-25-2021

**CYBER RISK MANAGEMENT PROGRAM
CYBER INCIDENT RESPONSE PLAN**

WHEREAS, the Atlantic County Municipal Excess Liability Joint Insurance Fund requires all municipalities in their fund, to have a Cyber Risk Management Program & Cyber Incident Response Plan in place; and

WHEREAS, the Borough of Buena Municipal Utilities Authority has updated their policies to be compliant with the ACMELJIF Cyber Risk Management Program; and

NOW, THEREFORE, BE IT RESOLVED, that the Cyber Risk Management Program & Cyber Incident Response Plan be adopted by the Borough of Buena Municipal Utilities Authority, County of Atlantic, State of New Jersey.

BOROUGH OF BUENA MUNICIPAL UTILITIES AUTHORITY

By: 
JOSEPH SANTAGATA, CHAIRMAN

Attest:


CHERYL M. SANTORE, SECRETARY

I, Cheryl M. Santore, Secretary of the Borough of Buena Municipal Utilities Authority, do hereby certify that the foregoing Resolution was adopted at a meeting of the Borough of Buena Municipal Utilities Authority held on October 27, 2021.


CHERYL M. SANTORE, SECRETARY



Cyber Incident Response Plan

Document Management

Document Owner:	Borough of Buena Municipal Utilities Authority
Document Name:	Cyber Incident Response Plan
Version No:	Version: 2.1
Adoption Date:	October 13, 2021
Distribution Date:	October 13, 2021
Author (Source)	NJMEL
Last Review Date:	3/8/2021
Next Review Date:	1/1/2022
Data Classification:	Sensitive

Table of Contents

<i>Document Management</i>	2
1. Policy Statement	4
2. Reason for the Policy	4
3. Scope	4
4. Incident Identification	4
4.1 Cyber Extortion Threat	4
4.2 Cyber Security Breach	5
4.3 Data Breach	5
5. Designation of an Incident Response Manager	5
5.1 Responsibilities	5
6. Incident Response Team and Notification	6
7. Incident Response Phases	6
7.1 Detection, Reporting, & Analysis	6
7.2 Containment, Eradication, & Recovery	7
7.3 Forensics	8
7.4 Post-Incident Review	8
8. Periodic Review	8
9. Special Situations/Exceptions	9

1. Policy Statement

The Incident Response Plan defines our methods for identifying, tracking, and responding to technology-based security incidents.

2. Reason for the Policy

The Incident Response Plan is established to assist in protecting the integrity, availability, and confidentiality of technology and assist in complying with statutory, regulatory and contractual obligations.

Responding quickly and effectively to an Incident is critical to minimizing the spread of the Incident and/or the business, financial, legal, and/or reputational impact. Incident Response generally includes the following phases:

- Detection, Reporting, and Analysis.
- Legal.
- Forensics.
- Containment, Eradication, and Recovery.
- Other Responses (i.e. Public Relations).
- Post-Incident Review.

3. Scope

This plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information (hereinafter, "Incidents"). Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data (e.g., constituent data, Protected Health Information, Personally Identifiable Information, credit card data, and law enforcement records).

Minor events (e.g., routine detection, and remediation of a virus, a minor infraction of a security policy, or other similar issues that have little impact on day-to-day business operations) are not considered an Incident under this policy.

4. Incident Identification

For cyber insurance purposes, a security incident is an event that is a: cyber security breach, or cyber extortion threat, or data breach.

4.1 Cyber Extortion Threat

A threat against a network to:

1. Disrupt operations.
2. Alter, damage, or destroy data stored on the network.
3. Use the network to generate and transmit malware to third parties.
4. Deface the member's website.
5. Access personally identifiable information, protected health information, or confidential business information stored on the network; made by a person or group, whether acting alone,

or in collusion with others, demanding payment, or a series of payments in consideration for the elimination, mitigation, or removal of the threat.

4.2 Cyber Security Breach

Any unauthorized access to, use, or misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, viruses, worms, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

4.3 Data Breach

The actual or reasonably suspected theft, loss, or unauthorized acquisition of data that has or may compromise the security, confidentiality and/or integrity of personally identifiable information, protected health information, or confidential business information.

Other cyber security incidents include:

- Attempts from unauthorized sources to access systems or data.
- Unplanned disruption to a service or denial of a service.
- Unauthorized processing or storage of data.
- Unauthorized changes to system hardware, access rights, firmware, or software.
- Presence of a malicious application, such as ransomware, or a virus.
- Presence of unexpected/unusual programs.

5. Designation of an Incident Response Manager

The municipality shall designate an Incident Response Manager who is either a full or part time technology person working in your municipality on a daily basis or the highest-ranking administrative person in your municipality that employees would normally contact when having computer or technology problems. Ideally, this person should be readily available to employees in the case of a cyber security event.

5.1 Responsibilities

- The municipality has designated an Incident Response Manager that is responsible for determining whether an event, or a series of security events, is declared an Incident.
- The Incident Response Manager is responsible for ensuring that this policy is followed.
- The Incident Response Manager is responsible for establishing an Incident Response Team to support the execution of this plan.
- The Incident Response Team is tasked with executing this plan in accordance with and at the direction of the Incident Response Manager.
- The highest-ranking administrative official in the municipality is responsible for ensuring that end-users have sufficient knowledge to recognize a potential security Incident and report it in accordance with this plan.
- Employees are responsible to report potential security incidents in a timely manner and provide any requires support during plan execution.

6. Incident Response Team and Notification

Establish an incident response team to be able to quickly respond to cyber security incidents, and a team broad enough to gather the needed resources and make the appropriate decisions to resolve the incident. Such team shall include the following.

Title / Position	Name	Telephone #
Highest-ranking Administrative Official	Joseph Santagata	(856) 697-0448
Chief of Police		
General Counsel	Testa, Heck, Testa & White – Michael Testa	(856) 691-2300
Human Resources Manager	Cheryl M. Santore	(856) 697-1784
Incident Response Manager	Cheryl M. Santore	(856) 697-1784
JIF Risk Management Consultant	Nick Cashan BCA Insurance Group	(609) 645-1700 ext 238
JIF Claims Administrator	Cheryl Santore	(856)-697-1784
Technology Support Contact	Wes Barber Barber Consulting Services	(609) 225-6856
AXA XL Data Breach Hotline		855-566-4724

Please verify with your breach advisor/counsel that their firm will be handling the required breach notifications including, but potentially not limited to, those agencies listed below.

IC3	FBI Internet Crime Complaint Center: https://www.ic3.gov/
NJ Cybersecurity and Communications Integration Cell (NJCCIC)	Incident Reporting: https://www.cyber.nj.gov/report 609-963-6900 x7865

7. Incident Response Phases

7.1 Detection, Reporting, & Analysis

1. If a user, employee, contractor, or vendor observes a potential security event they should notify the Incident Response Manager immediately. If the Incident Response Manager is not available, the events should be immediately reported to the highest-ranking administrative official.
2. The Incident Response Manager is responsible for communicating the Incident, its severity, and the action plan to the highest-ranking administrative official.
3. If the Incident Response Manager or the highest-ranking administrative official are not available, a user should isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. If isolating the machine from the network is not possible then unplug the machine from its power source.
4. If you have determined or suspect that the Incident is a cyber security breach, cyber extortion threat, or data breach (*see Definitions Related to Cyber Liability Insurance – Section 4 of this document*) proceed to Step 5. If not, proceed to Step 6.

5. For a cyber security breach, please follow this process:

If the AXA XL Data Breach Hotline does not answer, leave a message with your contact information. Do not delay in calling the Hotline. When they respond, follow their instructions. They will refer the matter to a "breach advisor/counsel" (an attorney experienced in cybersecurity incidents) who will coordinate the response. The Breach Counsel will gather information about the Incident and work with you to determine an action plan.

The Incident Response Manager should follow the advice from the Breach Counsel until the issue is resolved.

6. *If the Incident is determined not to be a cyber security breach, cyber extortion threat, or data breach,* the Incident Response Manager should work with the Incident Response Team to assess the Incident, develop a plan to contain the Incident, and ensure the plan is communicated to and approved by the highest-ranking administrative official.
7. The Incident Response Manager should ensure that all actions are documented as they are taken and that the highest-ranking administrative official, Incident Response Team, and outside support are regularly updated.

7.2 Containment, Eradication, & Recovery

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage.

Immediate triage:

1. Immediately contact technology expert to report the event and follow their instructions. It is now the responsibility of technology expert to notify management of the incident and to execute the security incident response plan.
2. If technology expert is not available, isolate the affected devices from the network or internet by removing the network cable from the device. If operating via wireless, turn off the wireless connection. DO NOT TURN OFF DEVICE OR REMOVE POWER SOURCE unless instructed by technology expert.
3. Incident response team assembles and assesses if the incident is a cyber security breach, cyber extortion threat, or data breach. If it is, or if there is any question the incident may or may not be one, management contacts their JIF Claims Administrator to advise them of the incident and management (or technology support) will call the Cyber Insurer Hotline. Work with the breach coach and the other partners they suggest to help resolve the incident.
4. Document all actions as they are taken.

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred.

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications.
- Change all user and system credentials.
- Restore data to the system.
- Return affected systems to an operationally ready state.
- Confirm that the affected systems are functioning normally.

7.3 Forensics

Security incidents of a significant magnitude may require that a forensics investigation take place. Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The highest-ranking administrative official, in consultation with the Incident Response Manager and/or XL Caitlin will advise if engaging a forensics firm is required.

7.4 Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered.
- Information about the systems that were affected.
- Information about who was responsible for the system and its data.
- A description of what caused the Incident.
- A description of the response to the Incident and whether it was effective.
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents.
- A discussion of lessons learned that will improve future responses.

8. Periodic Review

This policy and associated subordinate procedures will be reviewed at least annually by the Incident Response Manager to adjust processes considering new risks and security best practices. Material changes in this policy should be approved by the highest-ranking administrative official and/or governing body of the municipality.

9. Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.

Borough of Buena Municipal Utilities Authority

Master Technology Policy

Version 2.2

MEL Cyber Risk Management Program

Document Owner:	Borough of Buena Municipal Utilities Authority
Document Name:	Master Technology Policy
Version No:	2.2
Adoption Date:	10/27/2021
Distribution Date:	10/27/2021
Author (Source):	Lou Romero, Secure Data Consulting Services Lromero@SecureDataCS.com
Last Review Date:	3/8/2021
Next Review Date:	1/1/2022
Data Classification:	Sensitive

Table of Contents

Document Management

Error! Bookmark not defined.

1. Policy Statement	5
2. Reason for the Policy	5
3. Scope	5
4. Tier 1 Operational Policies	5
6.1. <i>Information Backup Policy</i>	5
6.2. <i>Patch Management Policy</i>	6
6.3. <i>Defensive Software Policy</i>	6
6.4. <i>Security Awareness Training Policy</i>	7
6.5. <i>Password Policy</i>	7
6.6. <i>Email Warning Policy</i>	8
6.7. <i>Cyber Incident Response Plan</i>	9
6.8. <i>Technology Practice Policy</i>	9
6.9. <i>Government Cybersecurity Membership Policy</i>	9
5. Tier 2 Operational Policies	11
5.1. <i>Server Security Policy</i>	11
5.2. <i>Access Privilege Controls Policy</i>	11
5.3. <i>Technology Support Policy</i>	11
5.4. <i>System and Event Logging Policy</i>	12
5.5. <i>Protected Information Policy</i>	12
5.6. <i>Remote Access Policy</i>	12
5.8. <i>Technology Business Continuity Plan Policy</i>	13
5.9. <i>Banking Control Policy</i>	14
6. Tier 3 Operational Policies	14
6.1. <i>Network Segmentation Policy</i>	14
6.2. <i>Remote Access Policy</i>	15
6.3. <i>Password Integrity Policy</i>	15
6.4. <i>System and Event Logging Policy</i>	16
6.5. <i>Third-Party Risk Management Policy</i>	16

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

1. Policy Statement

The Technology Policy defines the technology security practices necessary to ensure the security of the member's technology 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 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 technology systems that store, process, or transmit the information.

This policy affirms our commitment to technology 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 technology 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.

6.1. 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

6.2. Patch Management Policy

Objective:

The objective of the Patch Management Policy is to ensure all systems and applications are patched on a timely 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

6.3. 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"

6.4. 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.

6.5. 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 technology 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

6.6. 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.

6.7. 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.



MEL Cyber Incident
Response Plan - v2.1

6.8. 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.

Requirements:

This document shall serve as the Technology Practice Policy.

6.9. Government Cybersecurity Membership Policy

Objective:

The objective of the Government Cybersecurity Membership policy is to ensure the member stays current with cyber threat notifications and relevant information. Both required below are FREE.

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).

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 technology systems and data. We lead a global community of technology 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 physical 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.

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 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 technology support and the JIF's or MEL's available resources.

5.8. Technology Business Continuity Plan Policy

Objective:

The objective of the Technology 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 Technology Business Continuity Plan as part of its Disaster Recovery section.

When developing an Technology 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, virtually or physically, 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 technology 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
Questionnaire.xlsx

Technology Vendors

It is paramount to select a technology vendor that has the expertise, experience, and certification to effectively design, implement, manage, and maintain your technology 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?
- 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?

Technology Support Guidelines

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						✓

- Certifications marked with a bullet are not required but good to have depending on customer needs.

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.

Cyber Risk Management Resources

We want to provide many resources and guides on many of the requirements in the MEL Cyber Risk Management Program, but your technology expert should be your first resource. You will find most the resources we highlight below are governmental entities, most notably MS-ISAC, US-CERT, CIS, NJCCIC and NIST. These organizations provide an extensive array of free resources to public entities, so we encourage contacting them for services. See the MEL's Cyber Resources guide: <https://njmel.org/wpcontent/uploads/2019/06/Cyber-News-Free-Member-Resources.rev.pdf>

Backups

NJCCIC offers tips for data back-up setups: <https://cyber.nj.gov/mitigation-guides/backups-the-cure-to-viral-cyber-infections>.

Training

Consider using an outside vendor to provide the training. See the MEL's Cyber Hygiene Training Vendor guide attached.

Cybersecurity

Ventures, along with many other organizations, publishes an annual report of top vendors: <https://cybersecurityventures.com/security-awareness-training-companies/>.

Passwords

Review NJCCIC's and NIST's password recommendations. NIST is the go-to source for cybersecurity standards and NJCCIC typically follows and provides some additional commentary:

<https://cyber.nj.gov/instructional-guides/passwords-passwords-passwords> <https://pages.nist.gov/800-63-3/>

There are many services available to run your organization's email addresses against known breaches, which are typically provided by your security software/SaaS provider, such as Norton, BitDefender, etc. A very popular provider is "Have I Been Pwned?": <https://haveibeenpwned.com/>.

Multi-Factor Authentication (MFA)

NJCCIC offers an easy technical guide to deploying multi-factor authentication in your organization:

<https://cyber.nj.gov/instructionalguides/stop-what-you-are-doing-and-enable-mfa>.

Government Cyber Memberships

NJCCIC: <https://cyber.nj.gov/members/>

MS-ISAC: <https://learn.cisecurity.org/ms-isac-registration>

Water-ISAC: <https://www.waterisac.org/>

E-ISAC: <https://www.eisac.com/>

US-CERT / CISA: <https://us-cert.cisa.gov/>

ICS-CERT: <https://us-cert.cisa.gov/ics>

IT-ISAC: <https://www.it-isac.org/>

Elections-ISAC: <https://www.cisecurity.org/ei-isac/>

Surface Transportation-ISAC: <http://www.surfacetransportationisac.org/>

Remote Access

This NJCCIC guide offers security tips for remote access: <https://cyber.nj.gov/this-is-security/tips-for-teleworkers-remote-accesssecurity>.

NJCCIC Router security: <https://www.cyber.nj.gov/instructional-guides/how-to-configure-and-secure-a-home-wi-fi-router>

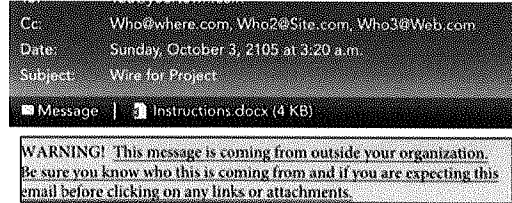
Banking Controls

See NJ DCA's electronic payroll guide for assistance in this area of banking controls:

<https://www.state.nj.us/dca/divisions/dlgs/resources/pdf/payroll%20agency%20handbook.pdf>

Email Warning Label for Outside Senders

Add a warning label to all emails coming from outside of your organization via the transport server.



Hi,
Im traveling and lost my phone. We need to wire money.

Segmentation

NJCCIC guide to Network Segmentation: <https://www.cyber.nj.gov/this-is-security/network-segmentation>

Employee Policies

Remote Working: Via the MEL's Cyber insurer (AXA XL), their partner InformationShield has provided a template Remote Working policy to use with your employees. See attached.

Mobile Device Access & Waiver: Via the MEL's Cyber insurer (AXA XL), their partner NetDiligence has provided a template policy for your employee's use of personal devices for work, giving authorization for you to access and wipe the device.