



MEL Cyber Risk Management Program

2nd Edition

March 8, 2021

Version 2.1 – 1/1/22



BACKGROUND

The Municipal Excess Liability Joint Insurance Fund (MEL) has provided its members with cyber insurance coverage since 2013. The MEL has embarked on creating a cyber risk management framework to assist members in managing this evolving risk through the development of a set of minimum technology proficiency standards. The MEL established a Cyber Task Force to deploy cyber education, release a cyber risk management framework and monitor the cyber risk of its members. The task force is comprised of commissioners, risk managers, executive directors and other professionals, and it partnered with the Bloustein Local Government Research Center at Rutgers University.

The MEL recognizes that much of the terminology and technical aspects of the minimum standards might not make sense to everyone; therefore, it is critical this program be reviewed and enacted on with the assistance of a technology expert. Your technology expert should guide your officials in determining what your organization needs to do to comply.

While all members are covered by cyber insurance, the per claim deductible as of 1/1/2022 is \$25,000. Members become eligible for up to \$25,000 reimbursement of their deductible by achieving compliance with the program. Tier 1 = \$10,000 reimbursement, Tiers 1 & 2 = \$20,000 reimbursement, and Tiers 1, 2 & 3 = \$25,000 reimbursement.

In order to qualify for the deductible reimbursement, follow these steps:

1. Submit the Certification checklist. All items must be “Yes” in order to comply; you may submit any “No” or “Not Applicable” responses for consideration with detailed explanations.
2. At the time of a claim, submit the Deductible Reimbursement checklist and provide the supporting documentation requested in the checklist.

PLEASE NOTE, any item not at 100% may make you ineligible for deductible reimbursement.

Many of the minimum standards involve little or no cost (i.e., activating Microsoft Defender software on Windows 10 machines meets the anti-virus requirements), while others will incur costs (cloud-based services, i.e., Microsoft Office 365, Google Office, subscription-based cloud backup). In all cases, the program is designed considering the limited budgets of the members, and so the minimum standards will provide the most security for the lowest cost.

Keep in mind, these minimum standards will not eliminate all technology risks. The standards are only minimums, which will provide a strong level of protection if effectively carried out; however, cyber risks constantly evolve. This means you must constantly monitor your cybersecurity posture so your organization can respond to new threats and risks as warranted.





PROGRAM CONTENTS

1. Getting StartedPage 4

2. Minimum Technological Proficiency StandardsPage 5

APPENDICES

Master Technology Practices Policy Appendix 1

Cybersecurity Incident Response Plan Appendix 2

Initial Minimum Technological Standards Certification Appendix 3

Deductible Reimbursement Application..... Appendix 4

Additional Security Practices to Consider Appendix 5

Infographic Overview of Cyber Insurance Reimbursement Plan Appendix 6

Third-Party Security Questionnaire Appendix 7





Getting Started!

1. GET A TECHNOLOGY EXPERT!
2. Review the Cyber Risk Management Program with your technology expert.
3. Develop a plan, timetable and budget to implement the standards.
4. Once implemented, complete the Certification checklist.
5. Establish a process to at least annually review your technology risks, score how the organization is managing them and ensure the program continues to be met.

Want to learn more about technology risks? See the work done by the Rutgers Bloustein Local Government Research Center on Technology Risk or the MEL Cyber webpages:

MEL: <https://njmel.org/mel-safety-institute/resource-center/public-officials/public-officials-cyber-risk-control/>

Rutgers Bloustein: <http://blousteinlocal.rutgers.edu/managing-technology-risk/>





MEL Cyber Risk Management Program

Tier	Subject	Requirements	Comments
1	Information Backup	<ol style="list-style-type: none"> 1. Use of standardized system images or virtualized desktops 2. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises 3. Locally Stored Data (including MS 365, Google Workspace and similar): <ol style="list-style-type: none"> a. Daily incremental backups with minimum of 14 days of versioning on off-network device. b. Weekly, off-network, off-premises full backup of all data. c. All backups are spot-checked monthly. 4. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data. 5. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data. 	<ol style="list-style-type: none"> 1. Images and virtual desktops must be kept current with manufacturer patches. 2. Back-up such software or have current installation files available. 3. Backup all locally stored data to local, cloud or off-network devices. MS 365/Google cloud-based and locally stored files require a separate local or cloud-based backup. As this applies to all non-application software, consider cloud storage data. 4. Includes Azure, Google Cloud, AWS, etc. Cloud service application and data files must be backed-up using appropriate cloud services. 5. Obtain in writing the backup practices used by application vendors, and ensure they meet these practices or provide equivalent protection. <p>Consider utilizing FedRamp certified service providers/products.</p>
1	Patch Management	<ol style="list-style-type: none"> 1. Keep all operating software, application software and infrastructure equipment current with latest versions. 2. Use automatic updating where practicable, particularly as related to security patches. 3. Install all security and critical updates and patches as soon as prudent and practicable following release. 4. Annually review all non-standard applications for possible replacement/upgrade. 	<ol style="list-style-type: none"> 1. No comment 2. No comment 3. System administrators need to coordinate patch upgrades with applications residing on systems managed by third parties to ensure upgrades will not disable their applications. Consider a procedure for these upgrades/patches when Technology Manager may not be available (i.e. vacation). 4. Outdated or non-supported operating systems and software should not be used unless there is no practical alternative available, in which case appropriate steps must be taken to mitigate potential security threats.
1	Defensive Software	<ol style="list-style-type: none"> 1. Antivirus and firewalls enabled for all desktops and laptops 2. Antispam and antivirus filters enabled for the mail server 3. Firewall enabled on all active ports, unused ports closed, antivirus enabled and antimalware enabled for network servers that connect to the internet 4. Firewall rules and policies need to be reviewed or reassessed at least twice per year 5. Microsoft Office applications open all downloaded files in "Protected Mode" 	<ol style="list-style-type: none"> 1. Should have automatic updates. Microsoft Windows comes with a preloaded firewall. 2. No comment 3. All network servers must have antimalware software running with automatic updates. 4. No comment 5. No comment





MEL Cyber Risk Management Program

1	Security Awareness Training	All computer users receive annual training of at least one hour. Training includes, but is not limited to: <ol style="list-style-type: none"> 1. Malware Identification 2. Password construction 3. Identifying and responding to security incidents 4. Social engineering attacks 	An expert should perform the training in either virtual or in-person format, which includes the various online training services. Best practice (although not required) is to perform training each quarter. Phishing testing is highly recommended twice per year. You may want to work with your counsel on an employee policy whereby access is removed or other actions taken for not completing/failing the training
1	Password	Must adopt a Technology Password Policy that at least meets the standards set in the MEL's Password Policy, at a minimum, or meet the NIST Password Standards 800-63B (03/02/2020 Updates).	NIST: https://pages.nist.gov/800-63-3/sp800-63b.html
1	Email Warning	Add a clear and obvious automatic warning label to all emails coming from outside of your organization.	No comment
1	Cyber Incident Response Plan	Management/Governing Body adopts 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 MEL Cybersecurity Incident Response Plan.	See the MEL's template Incident Response Plan. The Plan should be annually reviewed, tested and updated.
1	Technology Practices Policy	Management/Governing Body adopts a Technology Practices Policy, which must include at a minimum each of the subject items outlined in the MEL Cyber Risk Management Program, as respects Tier 1.	See the MEL's Technology Practices Policy template. The Policy should be annually reviewed and updated.
1	Government Cyber Memberships	<ol style="list-style-type: none"> 1. Register with New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) 2. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC) 	<ol style="list-style-type: none"> 1. IT'S FREE! 2. ALSO FREE! If you are/have a utility authority/department, also register for your respective ISAC, such as ICS-CERT (industrial controls), Water-ISAC (water/wastewater) or E-ISAC (electric).





MEL Cyber Risk Management Program

Tier	Subject	Requirements	Comments
2	Servers	Servers are physically protected from unauthorized access	Access-controlled rooms, locked cages, etc.
2	Access Privilege Controls	<ol style="list-style-type: none"> Users with administrator rights are limited to those who need them Non-administrator users are granted limited rights based on job function and responsibility Access rights are updated upon any personnel status change action Access rights for each individual are reviewed at least every six (6) months 	<ol style="list-style-type: none"> No comment No Comment This should be added to your personnel action form and routed to technology management No comment
2	Technology Support	Staff or contractors are available for technology guidance	For vendors, a contract needs to be in place. It does not suffice that the organization has the ability to call someone.
2	Logging	Logging must be setup for entire network/all devices, such as System, Application and Security logs.	Consider utilizing log-monitoring tools.
2	Protected Information	Files with personally identifiable information (PII) and protected health information (PHI) are password protected or encrypted	No comment
2	Remote Access	Utilize a Virtual Private Network (VPN) for all remote connections.	This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.).
2	Leadership Expertise	Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting)	This can be any combination of officials, employees, contractors/consultants or citizen volunteers
2	Technology Business Continuity Plan	Update your organization's Emergency Management/Continuity of Government (CoG) plan to include digital assets and technology management.	Address most items in your CoG in the Technology Practices Policy. Periodically perform tabletop exercises to ensure effective and efficient disaster response.
2	Banking Controls	Implement internal controls and controls with your bank: <ol style="list-style-type: none"> Establish procedures requiring multiple approvals for requests to change banking information. Establish procedures requiring multiple approvals and source verification for financial transaction requests over a certain threshold. 	Ensure compliance with NJDLGS Electronic Payroll and EFT/P-Card rules. <ol style="list-style-type: none"> No comment Consider setting a low amount, such as \$5,000
2	Technology Practices	Adopt a Technology Practices Policy, which must include at a minimum each of the subject items in the MEL Cyber Risk Management Program, as respects Tier 1 and 2.	See the MEL's template Technology Practices Policy. Annually review and update the Policy.
2	Remote Access	Adopt a Remote Access practice policy, which must at a minimum include the items in the MEL's Remote Access Policy	





MEL Cyber Risk Management Program

Tier	Subject	Requirements	Comments
3	Network Segmentation	Network segmentation.	<p>Consider separating business units, but especially critical/sensitive units, such as finance, police and utilities. Utilities should consider an air-gap for their Industrial Control (ICS) / SCADA systems.</p> <p>Virtual and/or physical segmentation is acceptable.</p>
3	Logging	Spot-check logs on at least a monthly basis.	Logs should be spot-checked for accuracy and usability.
3	Remote Access	Enable MFA for login to the organization's network, organization's email service (if cloud-based) and with third-party applications passing/storing Protected Information.	This is only applicable if you allow remote access to your network (i.e. employees, vendors, etc.). It is also recommended to limit remote network access to only pre-approved devices with Network Access Control (NAC).
3	Password Integrity	Periodically test all email addresses against HaveIBeenPwned or a similar email breach service to determine if any emails have been compromised, and take necessary action to ensure integrity.	MS-ISAC, NJCCIC and some vendors may be able to provide this testing.
3	Third Party Risk Management	Utilize the MEL's 3 rd Party Risk Assessment Tool for new/renewing contracts.	<p>This is most applicable to certain vendors transmitting/storing confidential data, such as technology provider, payroll, HR, etc.</p> <p>You may also consider asking the vendor to become compliant with the MEL's Cyber Risk Management Program.</p>





Tier 1

Information Back-Up

1. Use of standardized system images or virtualized desktops. _____
2. Back-up copy of all application, operating and network configuration software must be available. _____
3. Daily incremental back-ups with a minimum of 14 days of versioning on off-network device of all data files. _____
4. Weekly, off-network, full back-up of all data files. _____
5. All back-ups are spot-checked monthly. _____
6. Third-party and cloud-based application data is backed-up to the same standards. _____

Patch Management

1. Patch all operating an application software with the latest versions. _____
2. Use automatic updating where applicable, particularly as related to security patches. _____
3. All security and critical updates and patches are installed as soon as prudent and practicable following release. _____
4. The member annually reviews all non-standard applications for possible replacement/upgrade. _____

Defensive Software

1. Antivirus and firewalls are enabled for all desktops and laptops. _____
2. Antispam and antivirus filters are enabled for the email server. _____
3. Firewalls are enabled on all active ports, and unused ports are closed. _____
4. Antivirus and antimalware enabled for network servers connecting to the internet. _____
5. Firewall rules and policies are reviewed or reassessed at least twice per year. _____
6. Microsoft Office applications open all downloaded files in "Protected Mode". _____

Security Awareness Training

1. All computer users receive annual training of at least one (1) hour on at least the following topics: _____
 - a. Malware Identification
 - b. Password Construction
 - c. Identifying Security Incidents
 - d. Social Engineering



Tier 1

Password Strength

1. Password policy that minimally meets the requirements outlined in the Password Policy under the MEL's Master Technology Policy v 2.2.

Email Warning

1. Implemented an automatic warning label to all emails coming from outside of your organization.

Cyber Incident Response Plan

1. Management/Governing Body adopts a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place. This must include at a minimum the items in the MEL's Cybersecurity Incident Response Plan.

Technology Practices Policy

1. Management/Governing Body adopts a technology practices policy, which must at a minimum include the items in the MEL's Master Technology Policy v 2.2 respective to Tier 1.

Government Cyber Memberships

1. Registered with the New Jersey Cybersecurity & Communications Integration cell (NJCCIC).
2. Registered with the Multi-State Information Sharing & Analysis Center (MS-ISAC) and any other ISAC relevant to your organization's operations.



MEL Cyber Risk Management Certification

Tier 1

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

Print Name

Title

Signature

Date

TECHNOLOGY EXPERT

Print Name

Title

Signature

Date



Tier 2

Server Security

- 1. Servers and network equipment are protected from unauthorized access. _____

Access Privilege Controls

- 1. Users with administrative rights are limited to those who need them. _____
- 2. Non-administrator users are granted limited access rights based on job function and responsibilities. _____
- 3. Access rights are updated upon any personnel status change action. _____
- 4. Access rights for each individual are reviewed at least every six (6) months. _____

Technology Support

- 1. Has qualified staff or contractor(s) to provide technology support and guidance. _____

System / Event Logging

- 1. Has appropriate system and event logging is in place to detect and/or capture system/network performance and security anomalies. _____

Protected Information

- 1. Has a process that ensures all files containing Personally Identifiable Information (PII) or Protected Health Information (PHI) are password protected or encrypted. _____

Remote Access

- 1. Requires the use of a Virtual Private Network (VPN) when remotely accessing the network or cloud-base applications. This also includes adopting a Remote Access Policy. _____

Leadership Expertise

- 1. Senior management has access to resources with expertise in their respective fields to support technology decision making, i.e., risk assessments, planning, budgeting, etc. _____



Tier 2

Technology Business Continuity

1. The Emergency Management/Continuity of Government (CoG) plan shall
Include Technology Business Continuity Plan as part of the Disaster Recovery section. _____

Banking Controls

1. Has implemented internal controls to minimize fraudulent banking
transactions. _____

Technology Practice Policy

1. The Management/Governing Body has adopted the MEL's Technology Policy
as respects to Tier 2. _____



MEL Cyber Risk Management Certification

Tier 2

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

Print Name

Title

Signature

Date

TECHNOLOGY EXPERT

Print Name

Title

Signature

Date



Tier 3

Network Segmentation

1. The network is segmented, separating critical units (finance, police, utility, etc.) to minimize the spread of a cyber-attack. _____

Remote Access

1. Implemented the use of Multi Factor Authentication (MFA) when remotely accessing resources and/or accessing third-party applications that pass or store protected and or financial information. _____

Remote Access Policy

1. Adopted a Remote Access Policy that includes Multi-Factor Authentication and minimally includes the items in the Remote Access Policy – MFA in the MEL's Master Technology Policy v2.2. _____

Password Integrity

1. Implemented a process where employees can periodically validate their credentials against HaveIBeenPwned or a similar email breach service. _____

System and Event Logging

1. Logs are reviewed every three (3) months by the IT professional. _____

3rd Party Risk Management

1. Utilize the MEL's 3rd Party Risk Assessment Tool to assess a vendor's risk when issuing new or renewing contracts. _____



MEL Cyber Risk Management Certification

Tier 3

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

Print Name

Title

Signature

Date

TECHNOLOGY EXPERT

Print Name

Title

Signature

Date



Tier 1

Information Back-Up

1. Use of standardized system images or virtualized desktops. _____
2. Back-up copy of all application, operating and network configuration software must be available. _____
3. Daily incremental back-ups with a minimum of 14 days of versioning on off-network device of all data files. _____
4. Weekly, off-network, full back-up of all data files. _____
5. All back-ups are spot-checked monthly. _____
6. Third-party and cloud-based application data is backed-up to the same standards. _____

Patch Management

1. The member patches all operating an application software with the latest versions. _____
2. The member uses automatic updating where applicable, particularly as related to security patches. _____
3. All security and critical updates and patches are installed as soon as prudent and practicable following release. _____
4. The member annually reviews all non-standard applications for possible replacement/upgrade. _____

Defensive Software

1. The member's antivirus and firewalls are enabled for all desktops and laptops. _____
2. The member's antispam and antivirus filters are enabled for the email server. _____
3. The member's firewalls are enabled on all active ports, and unused ports are closed. _____
4. Antivirus and antimalware enabled for network servers connecting to the internet. _____
5. Firewall rules and policies are reviewed or reassessed at least twice per year. _____
6. Microsoft Office applications open all downloaded files in "Protected Mode". _____

Security Awareness Training

1. All computer users receive annual training of at least one (1) hour on at least the following topics: _____
 - a. Malware Identification
 - b. Password Construction
 - c. Identifying Security Incidents
 - d. Social Engineering



MEL Cyber Risk Management Deductible Reimbursement

Password Strength

1. The member has a password policy that minimally meets the requirements outlined in the Password Policy under the MEL's Master Information Technology Policy v 2.2. _____

Email Warning

1. The member has implemented an automatic warning label to all emails coming from outside of your organization. _____

Cyber Incident Response Plan

1. Management/Governing Body adopts a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place. This must include at a minimum the items in the MEL's Cybersecurity Incident Response Plan. _____

Technology Practices Policy

1. Management/Governing Body adopts a technology practices policy, which must at a minimum include the items in the MEL's Master Technology Policy v 2.2 respective to Tier 1. _____

Government Cyber Memberships

1. Registered with the New Jersey Cybersecurity & Communications Integration cell (NJCCIC). _____
2. Registered with the Multi-State Information Sharing & Analysis Center (MS-ISAC) and any other ISAC relevant to your organization's operations. _____



Tier 2

Server Security

- 1. The member's servers and network equipment are protected from unauthorized access. _____

Access Privilege Controls

- 1. Users with administrative rights are limited to those who need them. _____
- 2. Non-administrator users are granted limited access rights based on job function and responsibilities. _____
- 3. Access rights are updated upon any personnel status change action. _____
- 4. Access rights for each individual are reviewed at least every six (6) months. _____

Technology Support

- 1. The member has qualified staff or contractor(s) to provide technology support and guidance. _____

System / Event Logging

- 1. The member has appropriate system and event logging in place to detect and/or capture system/network performance and security anomalies. _____

Protected Information

- 1. The member has a process that ensures all files containing Personally Identifiable Information (PII) or Protected Health Information (PHI) are password protected or encrypted. _____

Remote Access

- 1. The member requires the use of a Virtual Private Network (VPN) when remotely accessing the municipal network or cloud-base applications. This also includes adopting a Remote Access Policy. _____

Leadership Expertise

- 1. The member's senior management has access to resources with expertise in their respective fields to support technology decision making, i.e., risk assessments, planning, budgeting, etc. _____



MEL Cyber Risk Management Deductible Reimbursement

Technology Business Continuity

1. The member's Emergency Management/Continuity of Government (CoG) plan shall
Include an Technology Business Continuity Plan as part of their Disaster Recovery section. _____

Banking Controls

1. The member has implemented internal controls to minimize fraudulent banking
transactions. _____

Technology Practice Policy

1. The Management/Governing Body has adopted the MEL's Information Technology Policy
as respects to Tier 2. _____



MEL Cyber Risk Management Deductible Reimbursement

Tier 3

Network Segmentation

2. The member network is segmented, separating critical units (finance, police, utility, etc.) to minimize the spread of a cyber-attack. _____

Remote Access

2. The member has implemented the use of Multi Factor Authentication (MFA) when remotely accessing municipal resources and/or accessing third-party applications that pass or store protected and or financial information. _____

Remote Access Policy

1. The member has adopted a Remote Access Policy that includes Multi-Factor Authentication and minimally includes the items in the Remote Access Policy – MFA in the MEL's Master Technology Policy v2.2. _____

Password Integrity

1. The member has implemented a process where employees can periodically validate their credentials against HaveIBeenPwned or a similar email breach service. _____

System and Event Logging

1. Logs are reviewed every three (3) months by the IT professional. _____

3rd Party Risk Management

1. The member utilizes the MEL's 3rd Party Risk Assessment Tool to assess a vendor's risk when issuing new or renewing contracts. _____



Required Documentation

All supporting documentation noted below are discussed in detail in the Minimum Technological Proficiency Standards.

1. Cyber training completion certificates or signed attendance
2. Screen shots of antivirus coverage
3. Screen shots of patches
4. Backup reports showing offsite backups
5. Copies of adopted Incident Response Plan and Technology Practices Policy
6. Email warning label screenshot
7. List of staff or contractors that support technology
8. Copies of adopted policies
 - a. Access, use, & control policy
 - b. PII & PHI encryption policy
 - c. Password policy
 - d. Banking Control policy
 - e. Remote Access policy
 - f. Technology Business Continuity policy



MEL Cyber Risk Management Deductible Reimbursement

Signature

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

MEMBER ENTITY

Print Name

Title

Signature

Date

TECHNOLOGY EXPERT

Print Name

Title

Signature

Date

<Member Entity>

Master Technology Policy

Version 2.2

MEL Cyber Risk Management Program

Document Management

Document Owner:	<Member Entity>
Document Name:	Master Technology Policy
Version No:	2.2
Adoption Date:	3/8/2021
Distribution Date:	3/8/2021
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

<i>Document Management</i>	2
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>	5
6.3. <i>Defensive Software Policy</i>	6
6.4. <i>Security Awareness Training Policy</i>	6
6.5. <i>Password Policy</i>	7
6.6. <i>Email Warning Policy</i>	8
6.7. <i>Cyber Incident Response Plan</i>	8
6.8. <i>Technology Practice Policy</i>	9
6.9. <i>Government Cybersecurity Membership Policy</i>	9
5. Tier 2 Operational Policies	10
5.1. <i>Server Security Policy</i>	10
5.2. <i>Access Privilege Controls Policy</i>	10
5.3. <i>Technology Support Policy</i>	10
5.4. <i>System and Event Logging Policy</i>	11
5.5. <i>Protected Information Policy</i>	11
5.6. <i>Remote Access Policy</i>	11
5.8. <i>Technology Business Continuity Plan Policy</i>	12
5.9. <i>Banking Control Policy</i>	13
6. Tier 3 Operational Policies	13
6.1. <i>Network Segmentation Policy</i>	13
6.2. <i>Remote Access Policy</i>	13
6.3. <i>Password Integrity Policy</i>	14
6.4. <i>System and Event Logging Policy</i>	14
6.5. <i>Third-Party Risk Management Policy</i>	15

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 Incident Response Plan

Document Management

Document Owner:	Member
Document Name:	Cyber Incident Response Plan
Version No:	Version: 2.1
Adoption Date:	
Distribution Date:	
Author (Source)	
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	8

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		
Chief of Police		
General Counsel		
Human Resources Manager		
Incident Response Manager		
JIF Risk Management Consultant		
JIF Claims Administrator		
Technology Support Contact		
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.

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/wp-content/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/instructional-guides/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-access-security>.

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

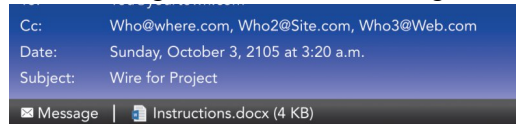
Banking Controls

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.



WARNING! This message is coming from outside your organization. Be sure you know who this is coming from and if you are expecting this email before clicking on any links or attachments.

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.



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

Members can meet the Cyber Risk Management Program requirement for employee cyber hygiene training (Tier 1 - at least one hour spread over two years) in several different ways. When considering their approach, JIFs and their members should consider: 1) the technology and cybersecurity risks they face, as measured against 2) the quality and elements of the training program and 3) the cost. As in most risk management training programs, there is a direct correlation between the three elements. The better educational quality programs address a wider range of risks and are of better educational quality but cost more. The following graphic adds depth to the issues to consider; an explanation of the different types of programs follows:

Training Quality	<ul style="list-style-type: none">• Different video styles may appeal to different audiences• Phishing tests increase the value and reduce risks• Level of customization desired
Phishing Tests	<ul style="list-style-type: none">• Cost is either fees to vendor or time spent by local program manager to customize testing
Program Overhead	<ul style="list-style-type: none">• Staff needs to be assigned to manage the program, track employees, and decide what training is used.
Accountability and Cost	<ul style="list-style-type: none">• The most flexible programs are the most accountable and have higher costs (fees plus time of local manager); The least flexible and accountable are the least expensive
Pricing	<ul style="list-style-type: none">• Prices vary by:<ul style="list-style-type: none">• Level of service provided by the vendor (higher price) as opposed to effort provided by customer (lower price)• Customization of training material
Flexibility	<ul style="list-style-type: none">• Different vendors have different approaches and options• Some provide collateral printed and online material, periodically refreshed



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center



Review and Analysis of Cyber Hygiene Services (Fall 2017)

Overview

All of the reviewed providers¹ offer online cyber hygiene (a.k.a. security awareness) videos and phishing training (companies only doing phishing training were excluded), and all do the same things with similar user enrollment and management reporting tools. The depth, pricing, management feature flexibility, and to some degree, the quality/style of videos are what differentiates them, making choices very JIF/member-dependent. While pricing is driven by the number of participants covered by contract, general pricing runs in the \$8-\$15/employee/year range (often based on a training service fee plus a phishing service fee), with variations driven by phishing training management, customization needs, and personnel (i.e., who manages the administrative overhead).

Generally, company-managed overhead will be slightly more expensive than a management by a local official or JIF. Depending on the service, member maintenance may require the time and attention of a JIF or member staff person to manage that aspect. Deciding on a vendor may hinge on the capacity of the JIF or individual member to handle the effort required by its choice of service.

All vendors tend to update their material regularly as cyber threats continuously evolve. There are various industry perspectives on how to deal with some cyber threats; different vendors offer different guidance on how to do so; there might be minor differences on how those recommendations affect local governments, but these are not substantial issues. It is important to note most of the videos are focused on private businesses, and the nomenclature reflects that; however, the risks and solutions are generally the same. One vendor (PivotPoint) has developed videos specifically for MEL municipalities.

The videos all differ by style (lifelike animation, cartoon, or live actors) and approach (from serious to relaxed), though the content is similar. All include interactive quizzes to reinforce the videos. National vendors also provide various types of free collateral materials designed to reinforce training. Phishing services involve sending emails to employees to see if they can be fooled into clicking on a dangerous link. Each vendor has a different approach and will propose various options to dealing with this form of penetration testing.

¹ Research began using the Gartner Group's "Magic Quadrant for Security Awareness Computer-Based Training" 10/16 (most recent available when researched). Six of the vendors were selected from "Leader's" quadrant (high ability to execute and completeness of vision), then reduced to those who services seem most relevant to JIF need (i.e., US-focused, end-user security training, and phishing testing, plus two NJ based firms that JIF member have worked with).



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

<i>Phishing Test (Online) Service</i>		
<i>Service Level</i>	<i>Sophistication of Test</i>	<i>Costs</i>
Best	<i>Fully customized templates and schedule</i>	<i>Fees and management time and attention vary by service provider</i>
Better	<i>Limited templates and schedule</i>	<i>Limited management engagement</i>
Marginal	<i>None</i>	<i>None</i>

The following analysis is organized into two vendor categories: New Jersey-based companies and large national ones. Following the analysis is a review of criteria that can be part of a contracting decisions (Training Management Considerations).

NJ-Based Vendors

D2Cybersecurity/Kean University

www.d2cybersecurity.com/industries/municipalities.html

D2 specializes in developing cybersecurity education and training for all levels of government and various private sector industries. It has a full line of videos that, depending on the level of service desired, can be branded or customized with the appearance of organization officials (this option requires video recording). Its program is made up of 8 individual modules. Terminology tends to lean corporate, but not overwhelmingly so. Each module has an interactive quiz. It has a contract and marketing arrangement with Kean University that effectively eliminates public contracting issues (over \$17,500 or \$40,000 if that becomes an issue). D2’s phishing service has 25+ sample templates it can modify based on specific needs or target groups (i.e., police may get something targeted to them). The company manages the overhead; the user works with them to determine what they want. Extreme customization for a specific user group might result in additional costs, but it appears flexible. Members only need to provide email addresses of employees, but deeper customization is available (depending on complexity, there could be a fee). If contracted by a JIF, it will provide an aggregate, anonymized management report to the JIF, and a detailed report to the member. D2 has a representative (Brian Lau) available to meet with members considering its services.

PivotPoint

www.pivotpointsecurity.com/security-awareness-training/

PivotPoint has developed a video training series specifically targeted to NJ municipalities². It uses a personally narrated, less formal, self-deprecating, tongue-in-cheek humorous approach; this is different from the other firms (the video presenter is John Verry, the head of the firm). It was developed by technologists (other firms

² This was informed in part through a contract PivotPoint has with A.J Gallagher managed JIFs; partly developed on the possibility of obtaining work with other JIFs



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

combine education specialists and technologists) and includes some superfluous technology jargon and detailed administrative information that are not present (and sometimes not relevant) in other vendor videos. The videos and site features are not fully active, but it is anticipated this will be addressed over time³. Given its interest in specifically serving JIFs, it has the capacity to meet with JIF officials to customize content. It uses a third-party service to manager its phishing program. As such, it has limited mailing flexibility, customization options and a smaller number of templates and landing pages. These limitations are offset by reduced management overhead. Mailings go to enrolled users; the service sends a link to management, who resends it to employee-users so they can self-enroll. A management dashboard provides basic reporting functions for video use and phishing.

Large National Vendors

The following vendors (in alphabetical order) are very similar in capabilities and approaches. All services are highly automated with dashboards and pick-lists to manage the process. They compete with each other and, over time, generally match each other's features. Video styles are varied. The narratives below are a summary of highlights from observations, limited demonstrations, and, in some cases, discussions with representatives. The firms all have website links to contact representatives who can discuss details for specific potential clients (the study made specific contacts with staff from MediaPro and Wombat, and information about KnowBe4 was obtained from its website and some JIF users of the service). The Gartner Group maintains a user review site of "security awareness computer-based training" companies. The three companies are all included (among others). This can be seen here: www.gartner.com/reviews/market/security-awareness-computer-based-training

KnowBe4

www.knowbe4.com/

KnowBe4 is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, ongoing training and phishing ID software tools. It has multiple short modules and longer comprehensive ones from which the member can choose. It also provides a Microsoft Outlook "add-in" feature that lets a user report a phishing attack to it (available separately for a small fee, but installation requires technical skill). System management is highly automated, providing the member a high degree of customization, though it requires the thoughtful attention of a local coordinator to take advantage of all the features (including developing individualized, or edited templates, customized unlimited phishing emails and penetration attempts). Due to its high level of automation and member responsibility for making it all work via dashboards and menu-driven options, its per user cost tends to be lower than other services. KnowBe4's services, support,

³ These issues have been brought to their attention and will likely be addressed in future revisions.



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

sales and technical support staff are available through its website. It also provides a free phishing test (up to 100 employees).

MediaPro

www.mediapro.com

Media Pro is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, and ongoing training. It provides a very flexible platform with a wide variety of training packages that permit a “build your own” approach of mixing and matching interactive animated and photo-realistic videos from a wide selection of topics. Its videos include interactive quizzes and tests. Its integrated phishing dashboard has templates, but permits users to edit them and/or provide their own email. It also provides a variety of editable landing pages (the page that comes up when a phish is clicked on) with reinforcing videos that can be modified for specific users. Additionally, it has pre-packaged bundles that simplify the process. It would permit a JIF-based individual to manage the process for all member employees or permit a member who has a coordinator to handle training for the member. From a business standpoint, its representatives appear to understand government procurement issues and will work with resellers to handle RFPs. Its platform appears easy to use and allows a great degree of customization. Pricing is variable, based on the number of users and the services selected. It also has supplemental collateral materials, some of which can be locally branded.

Wombat

www.wombatsecurity.com

Wombat security is a full-service application including assessment tools, phishing/attack simulations, education modules, collateral materials, ongoing training and phishing ID software tools. Its videos run in 5-15 minutes modules, are interactive, and animated. It has various bundled packages, as well as the ability to customize packages. It has a phishing tool platform designed to send out emails. Pricing is variable; it can be purchased by the package or priced for individual modules; the more modules, the better the pricing. It also has an Outlook add-in if its phishing tools are used. It provides unlimited access to exercises. Its educational focus is on behavioral modification. Its pricing is a little different from the other companies; it charges extra if you want it to manage the process for you. It also provides a dedicated “customer success manager” who helps customize its platform and branding as part of its base service.



Employee Cyber Hygiene Training Options

Prepared by the Bloustein Local Government Research Center

Training Management Considerations

Cyber hygiene training requires management time and attention in ways similar to, but may exceed, other employee training programs. Members need to address the typical aspects of training management, such as assigning activities to individual employees and tracking their compliance and progress. Furthermore, each form of cyber hygiene training requires different levels of management attention. For example, online services require enrollment of employees, usually done by providing the company a list of employee email addresses or providing employees a link for logging into the service. Most services provide a management dashboard that tracks participants' status and the results of testing.

If a JIF is going to administer the program, each member will need to assign an individual to work with a JIF program coordinator to ensure employee lists and participation are effectively managed. If members are going to administer their own program, the office or individual that usually coordinates employee training (often found in the human resources/personnel function) will need to add cyber hygiene to their portfolio. Whether tracking employee participation is managed centrally or in each department, internal management procedures must be established to ensure adequate recordkeeping and oversight.

The member's technology coordinator (by whatever title or function) should be engaged in decision-making for cyber hygiene training to ensure the risks presented to the member's employees are adequately addressed in the training program. Options include: selecting videos by subject matter or customizing the content of phishing emails. While the technology coordinator may not be an expert in employee training techniques, they have expertise in understanding the cyber threats presented to the organization. The coordinator should also be involved in reviewing the results of employee testing.

Finally, as in all risk threats, members should establish an incident review practice whenever a cyber incident takes place. Reviewing cyber incidents from a risk management perspective will highlight gaps in training or internal procedures that can lead management to make improvements in its activities and improve employee training. As in other areas of administration, if an employee is involved in multiple incidents, found to knowingly disregard training or other technology policies, or repeatedly fail the training, the member should employ progressive disciplinary actions in accordance with its disciplinary procedures in other areas.