MEL Cyber Risk Management Program

2nd Edition

March 8, 2021

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 assistant 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 1/1/2020 is $25,000. Members become eligible for up to $25,000 reimbursement of their deductible by achieving compliance with the program. Tier 1 = $20,000 reimbursement, Tier 2 = $22,500 reimbursement, and Tier 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

APPENDICES

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/

Tier	Subject	Requirements	Comments
1	**Information Backup**	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): 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.	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. Consider utilizing FedRamp certified service providers/products.
1	**Patch Management**	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.	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**	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”	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

1	**Security Awareness Training**	All computer users receive annual training of at least one hour. Training includes, but is not limited to: 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**	1. Register with New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) 2. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC)	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).

Tier	Subject	Requirements	Comments
2	**Servers**	Servers are physically protected from unauthorized access	Access-controlled rooms, locked cages, etc.
2	**Access Privilege Controls**	1. Users with administrator rights are limited to those who need them 2. Non-administrator users are granted limited rights based on job function and responsibility 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	1. No comment 2. No Comment 3. This should be added to your personnel action form and routed to technology management 4. 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: 1. Establish procedures requiring multiple approvals for requests to change banking information. 2. 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. 1. No comment 2. 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	

Tier	Subject	Requirements	Comments
3	**Network Segmentation**	Network segmentation.	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. Virtual and/or physical segmentation is acceptable.
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 3rd Party Risk Assessment Tool for new/renewing contracts.	This is most applicable to certain vendors transmitting/storing confidential data, such as technology provider, payroll, HR, etc. You may also consider asking the vendor to become compliant with the MEL's Cyber Risk Management Program.

<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

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/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.

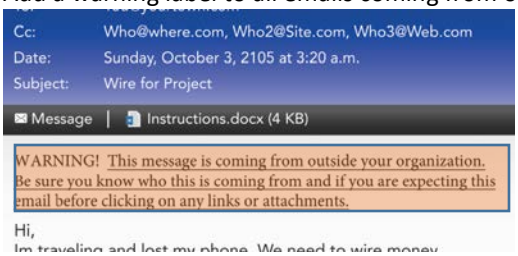
Government Cyber Memberships
NJCCIC: https://cyber.nj.gov/members/
MS-ISAC: https://learn.cisecurity.org/ms-isac-registration
Water-ISAC: https://www.waterisac.org/
E-ISAC: https://www.eisac.com/
US-CERT / CISA: https://us-cert.cisa.gov/
ICS-CERT: https://us-cert.cisa.gov/ics
IT-ISAC: https://www.it-isac.org/
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%20_agency_%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.



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.

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 municipality patches all operating an application software with the latest versions. _____
2. The municipality 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 municipality annually reviews all non-standard applications for possible replacement/upgrade. _____

Defensive Software

1. The municipality's antivirus and firewalls are enabled for all desktops and laptops. _____
2. The municipality's antispam and antivirus filters are enabled for the email server. _____
3. The municipality'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

Tier 1

Password Strength

1. The municipality 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 municipality 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 Information 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. _____

3rd Party Risk Management

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

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. The municipality'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 municipality has qualified staff or contractor(s) to provide technology support and guidance. _____

System / Event Logging

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

Protected Information

1. The municipality 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 municipality 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. (refer to Remote Access Policy – VPN in the Master Information Technology Policy v2.2). _____

Leadership Expertise

1. The municipality'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. _____

Tier 2

IT Business Continuity

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

Banking Controls

1. The municipality 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. _____

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

Remote Access

1. The municipality 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 municipality has adapted 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 Information Technology Policy v2.2. _____

Password Integrity

1. The municipality 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. _____

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 municipality patches all operating an application software with the latest versions. _____
2. The municipality 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 municipality annually reviews all non-standard applications for possible replacement/upgrade. _____

Defensive Software

1. The municipality's antivirus and firewalls are enabled for all desktops and laptops. _____
2. The municipality's antispam and antivirus filters are enabled for the email server. _____
3. The municipality'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 municipality 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 municipality 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 Information 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. _____

3rd Party Risk Management

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

Tier 2

Server Security

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

System / Event Logging

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

Protected Information

1. The municipality 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 municipality 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. (refer to Remote Access Policy – VPN in the Master Information Technology Policy v2.2). _____

Leadership Expertise

1. The municipality'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. _____

IT Business Continuity

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

Banking Controls

1. The municipality 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. _____

Tier 3

Network Segmentation

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

Remote Access

2. The municipality 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 municipality has adapted 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 Information Technology Policy v2.2. _____

Password Integrity

1. The municipality 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. _____

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. IT Business Continuity policy

Signature

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