NJ MEL Cyber Risk Management Program

Minimum Technology Proficiency Standards

Introducing the NJ Municipal Excess Liability Joint Insurance Fund Cyber Risk Management Program. The program establishes a minimum set of technology proficiency standards and provides reimbursement of up to $7,500 of a member's deductible if they were in compliance with the minimum standards at the time of the claim.

OVERVIEW

Since 2013, the N.J. Municipal Excess Liability Joint Insurance Fund (MEL) has provided its members with cyber insurance coverage. As the risks associated with the use of technology by municipalities and affiliated entities has evolved over time, the MEL has embarked on a process to assist members in managing this evolving risk through the development of a set of minimum technology proficiency standards. To assist in this process, the MEL partnered with the Bloustein Local Government Research Center at Rutgers University.

The Program goals fall into three categories: 1) achieve a minimum level of technical and cyber security competency with computers and networks; 2) ensure that employees practice sound cyber hygiene; and 3) ensure that members have basic technology management support, including the adoption of a basic plan to respond to a cybersecurity incident.

In developing this Program, the MEL recognized that much of the terminology and technical aspects of the minimum standards might not make sense to you; therefore, it is critical **you share this Program with your technology expert**. Your technology expert will be able to determine whether your municipality is already in compliance with all or some of the Program standards and/or what needs to be done to come into compliance. **In addition, your technology expert will be asked to help certify your municipality is in compliance with the minimum standards**. In the event your organization does not have a technology expert to advise it, you need to get that support. This is discussed in the next session.

While all members are covered by cyber insurance, the per claim deductible is $10,000. By coming into compliance with the standards, members become eligible for reimbursement of a portion of their deductible. Meeting the Tier 1 requirements will result in a deductible reimbursement of $5,000; meeting Tier 2 requirements will gain the member an additional $2,500 ($7,500 total) reimbursement. To initially apply for either deductible reimbursement, submit the Initial Technological Minimum Standards Certification form in Appendix 3. At the time of the claim, you will be required to complete the Deductible Reimbursement Application in Appendix 4 and provide the supporting documentation.

Some of these minimum standards involve little or no cost (i.e., activating Microsoft Defender software on Windows 8 and 10 machines meets the anti-virus requirements). Cloud-based services can also support data backup requirements (e.g., Microsoft Office 365, Google Office, subscription-based cloud backup). One of the Tier 1 items involves adopting an incident response plan. This is a no-cost item, as the MEL has developed a plan consistent with the cyber insurance policy.

In meeting these goals, some members may incur one-time and ongoing expenses. This is a trade-off for achieving the maximum deductible reimbursement and reducing your security risk profile. In some cases, added one-time or annual costs may exceed the maximum $7,500 reimbursement; however, the costs of those upgrades are likely justifiable, as they can lead to increased productivity and further risk reduction, allowing members to avoid future claims and keep insurance costs from rising in the future.

It is also important to keep in mind these minimum standards will not eliminate all technology risks; given technology's evolving nature, there is no set of actions that will eliminate all technology risks. **As a result, the NJ MEL will periodically review, update, and distribute revised or additional minimum technology standards to assist members in addressing the risk associated with using technology into the future**.

Finally, it is important to understand perfect cybersecurity is not a specific status that can be attained. Addressing this exposure will require ongoing resources and attention to reduce risks. This initial set of standards is designed to reduce the majority of cybersecurity risks and provide an effective pathway to system and data recovery in the event of a cybersecurity incident. These standards should be considered a starting point. Failing to act accordingly can be construed as ignoring critical risks facing the member.

NJ MEL Cyber Risk Management Program

PROGRAM CONTENTS

APPENDICES

Getting Started!

Actions to Meet MEL Cyber Risk Management Program

Before you start, it is important to review this Program with your technology expert. Whether that person is an employee or an outside consultant, engaging this person at the beginning of this process can make conforming to the Program easier. Also, appreciate that each member will have different considerations and approaches to meeting the standards. Some will already meet various standards, some more, some less. There is no one-size-fits-all plan when it comes to technology, but there are some minimum standards. Your goal is to accomplish the following:

- Understand the risks
- Spend the time and attention to develop a plan to address the risks
- Appropriate funds to meet the needs, if necessary
- Manage the implementation
- Establish an ongoing process to review technology.

These steps will get you started, caught up, or confirm your compliance:

1. If you don't have one, get a knowledgeable technology expert to advise you, your governing body, and senior management on implementing the **Minimum Technological Proficiency Standards** and technology issues in general. The technology expert can be an existing employee, contractor, citizen committee, employee committee, or combination thereof. If not done prior to engaging a technology expert, ensuring computer systems are backed up in a way that meets the minimum technology standard should be your top priority.

2. Have the technology expert review your existing security standards against the **Minimum Technological Proficiency Standards Chart** to determine your current status.

3. Once this review is complete, work with your technology adviser to develop a plan, timetable, and budget to implement any standards you do not currently meet. Plan to implement the standards to meet both tiers as outlined in the **Minimum Technological Proficiency Standards**. Consider the risks if either or both tiers are not implemented. Review with senior management and the governing body and get approval.

4. Put funding in place, if necessary, and move forward with implementation.

5. Once implemented, send notice to the MEL by completing the **MEL Cyber Risk Management Program Certification Form (Appendix 3)**, also available on the MEL Cyber Risk Control webpage (below).

6. Establish a process to periodically (at least annually) review your technology risks, how the organization is managing them, and ensure the Minimum Technological Proficiency Standards continue to be met.

Want to learn more about technology risks? See the work done by the Bloustein Local Government Research Center on Technology Risk and local governments or the MEL Cyber Risk Control webpage:

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

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

Minimum Technological Proficiency Standards

Tier values: Meeting all five Tier 1 requirements = $5,000 reimbursement (from original $10,000 deductible)
Meeting all remaining items (Tier 2) = additional $2,500 deductible reimbursement ($7,500 total)

Subject	Tier	Requirement	Comment
		A. TECHNICAL COMPTENCY	
Minimum- back-up practices	**1**	**1. Daily incremental backups** or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files 2. **Weekly off-network full backups** of all devices: a. Use of non-versioned, synchronized cloud-based drives are **not** acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files b. A full backup of non-networked/standalone (desk and laptop) computers must include all storage drives **Alternative**: consult with technology professional to assess and make recommendations for agency backup needs. 3. All backups are spot-checked monthly 4. Consult with third party application providers to ensure their data files are part of a backup practice	"Versioning" is where a backup system stores multiple copies of files going back in time. This permits a file encrypted by ransomware to be recovered by going to an earlier version of it. Cloud-based backup solutions include services such as Carbonite, Mozy, and Crashplan that include several weeks of versioning or similar ransomware protection. Most Office 365 and Google Drive users have at least 14 days of versioning for *data* files; but it should be verified as being active before using it as a backup plan. If these are used, a separate backup or imaging plan for system and applications files must be in place.
Patch	**1**	**Patch** all operating and application software with latest versions as released (use automatic updating where practicable); particularly as related to security patches. Outdated or non-supported operating systems and software are not used	Security patches should be applied immediately unless testing shows the patch will create application problems. System administrators need to coordinate patch upgrades with applications residing on systems managed by third parties to ensure upgrades will not disable their applications.
Defensive software is used and regularly updated	**1**	1. For all desktops and laptops: antivirus, firewall enabled 2. Mail server: antispam and anti-virus filters 3. For network servers that connect to the internet: firewall on all active ports, unused ports closed, anti-virus, anti-malware 4. Microsoft Office applications open all downloaded files in "Protected Mode"	Microsoft Windows 10 includes a built-in firewall (as do earlier versions) and anti-virus software. Third party applications that incorporate combinations of defensive software are available commercially.

Minimum Technological Proficiency Standards

Subject	Tier	Requirement	Comment
A. TECHNICAL COMPTENCY (continued)			
Server security	2	**Servers** are physically protected from access by unauthorized individuals	Can be in a cage or locked cabinet (with sufficient airflow) where only authorized users have access.
Access privilege controls are in place	2	1. Users with administrator rights are limited to those that need them 2. Users only have access only to those services they need 3. Access rights are removed when no longer needed or when employee separates from service 4. Access rights are periodically reviewed	
Technology -support	2	Staff or contractors are **available to support** its technology and respond to security incidents	
B. SOUND CYBER HYGIENE			
Training	**1**	All computer users receive **annual training** of at least one hour spread over two years. Training includes, but is not limited to malware identification (email and websites), password construction, identifying security incidents, and social engineering	The hour must be spread over the two years, not all at once.
Policies	2	The organization adopts sound government internet and email use **policies**	This includes the MEL standard Communications Media Policy.
Protect -Information	2	Files with personally identifiable and protected health information are **password protected or encrypted**	This has specific relevance to human resource and health information.
Password -strength	2	Employees are required to use **strong, unique passwords,** changed at least annually	**Passphrases** with at least 8 characters, with incidental upper- and lower-case letters and symbols are highly recommended.
C. TECHNOLOGY MANAGEMENT			
Leadership has expertise	2	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 as appropriate to the organization
Incident Response Plan	1	Management/Governing Body adopts a basic cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place	The MEL has developed a sample plan that is tied to the Cyber Insurance coverage program. Please see Appendix 2
Technology Practices Policy	1	Management/Governing Body adopts a basic Information Technology Practices Policy that outlines the entity's commitment to sound cyber security practices and technology management practices.	The MEL has developed a sample policy that is tied to the Cyber Insurance coverage program. Please see Appendix 1

Notes Concerning the MEL Model Information Technology Practices Policy

1) The attached Model Policy (Appendix 1) provides MEL members a policy template that implements the MEL's Minimum Technological Proficiency Standards. Successfully implementing and maintaining those standards will allow a MEL member who files a claim under the MEL Cyber Insurance Policy to receive a reimbursement of up to $7,500.

2) **Members are encouraged to amend the model policy to reflect their own practices**. Policies not consistent with, or which do not exceed the model policy will not meet the Minimum Standard and the member would not qualify for deductible reimbursement.

3) The policy includes several terms and phrases that need to be edited to reflect each member's specific organization and practices. They are all italicized and enclosed in <*brackets*>. The document should be carefully edited prior to adoption to replace those terms with ones appropriate to the member.

4) The backup policy (Section A-1 of the Minimum Standards) is highly technical in nature. Prior to adopting the policy, members should adjust it to reflect the member's specific backup practices; keep in mind, the practices describe a minimum. It is included in the policy document as its importance is critical in the event technology systems are compromised and warrants the attention of the member's leadership. It is recommended the advice of a technology expert be obtained to ensure the backup practice meets the member's needs.

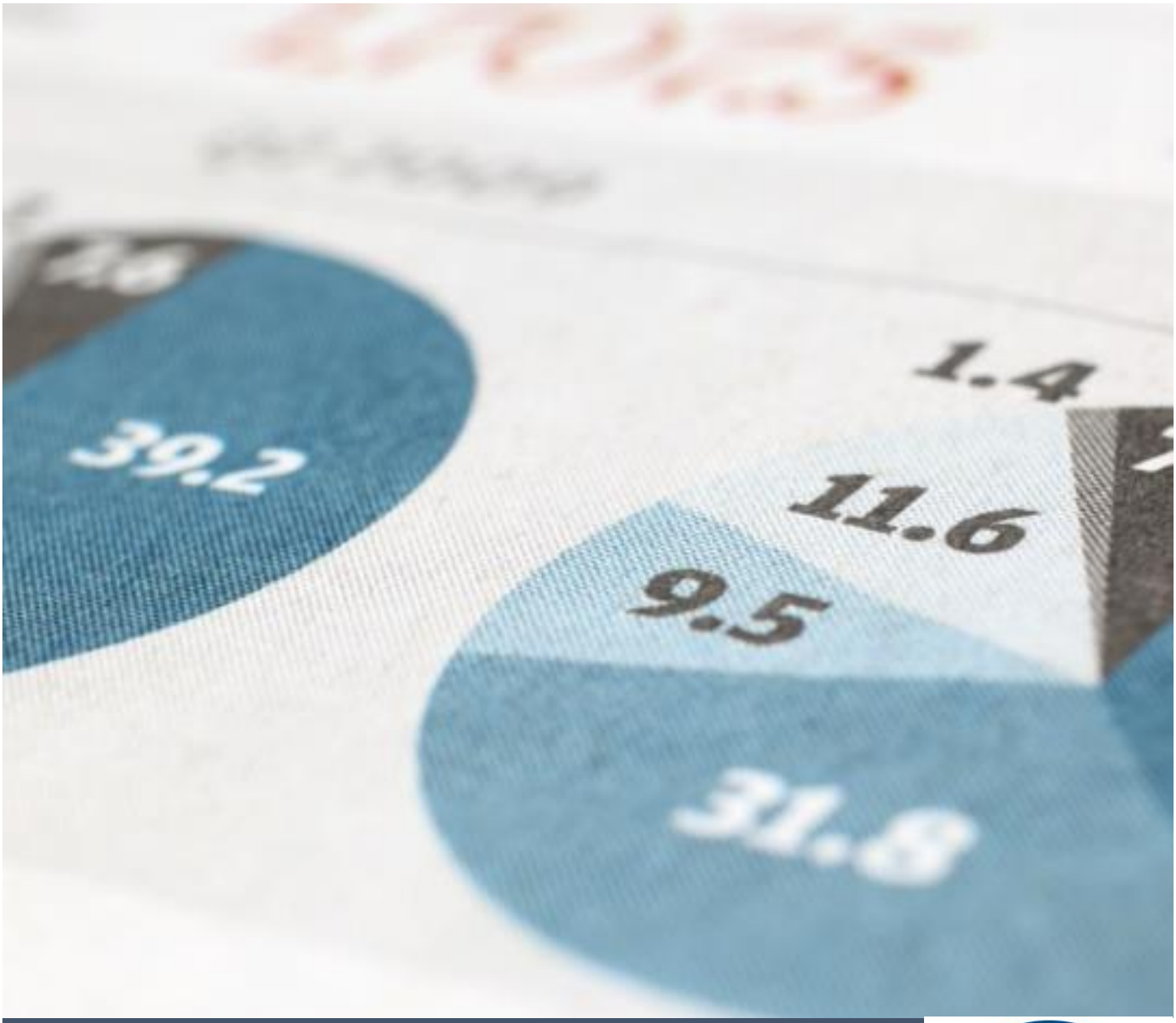
5) Elected officials and chief administrators should take careful note of the practices in Section C of the Minimum Standards, as they relate to the process used by the member to make technology decisions.

6) With regard to item C-2 of the Minimum Standards, the MEL has prepared a **Cybersecurity Incident Response Plan (Appendix 2)**. This template should be the starting point for the adoption of a plan for the member. It can be adapted to reflect local practices, but must remain consistent with when and how the carrier is notified to ensure the engagement a breach coach and timely computer forensics engagement.

7) Underlying the policy is an assumption that individuals will be named to ensure the practices are implemented and maintained. While the term "information technology manager" is sometimes used, the member should carefully consider who, either employee(s), contactor(s), or a combination thereof, are given responsibilities to implement specific practices.

8) To the extent that some practices are not currently in place, the policy can include target dates for their implementation. A planned, but not implemented practice will not meet eligibility for the deductible reimbursement.

9) While the MEL Cyber Risk Management Program represents minimum cyber security practices for you to implement, we strongly recommend you consider the additional security practices listed in Appendix 5.



Appendix 1

Model Information Technology Practice Policy

NJ MEL Cyber Risk Management Program

Model Information Technology Practice Policy

<Member Organization Name>

Purpose: To establish as policy certain information technology practices. Further, compliance with various practices will enable <*member*> to claim a reimbursement of a paid insurance deductible in the event the member files a claim against <*member*>'s cyber insurance policy, administered through <*name of JIF*> and the Municipal Excess Liability Joint Insurance Fund.

A. Technical Operations

1. **System and data back-up practices:** <*Member*> will implement backup practices that meet the following as a minimum standard, or will implement recommendations of a qualified information technology advisor who, after consideration of <*member*>'s information technology needs, recommends an alternative, which shall be fully documented.
    a) Daily incremental backups or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files
    b) Weekly off-network full backups of all devices:
        a. Use of non-versioned, synchronized cloud-based drives are not acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files
        b. A full backup of non-networked/standalone desk and laptop computers must include all storage drives
    c) All backups are spot-checked monthly
    d) Consult with third party application providers to ensure their data files are part of a backup practice
2. **Security and system patching:** all operating and application software shall be updated on a timely basis with latest versions as released, particularly as related to security updates. Outdated or non-supported operating systems and software shall not be used unless there is no practical alternative available, in which case, appropriate steps shall be taken to mitigate potential security threats. System administrators shall coordinate patching with applications maintained or managed by third parties to ensure upgrades will not disable their applications. When upgrades cannot be applied, appropriate action shall be taken to prevent the system or application from security exploitation.
3. **Defensive software** shall be installed and operative on all computing devices as follows:
    a. For all desktops and laptops devices: antivirus and an enabled firewall
    b. Mail server: anti-spam and anti-virus filters
    c. For network servers that connect to the internet: an active firewall on all open ports, unused ports closed; and anti-virus, anti-malware software running
    d. All Microsoft Office applications are set to all downloaded files in "Protected Mode"
4. **Server security:** all servers are protected from unauthorized access by means of a secured cage, locked cabinet (with sufficient airflow) or other physically secure means to ensure that only authorized users have access to it.
5. **Access privilege controls and policies** are in place and maintained to ensure that: 1) users with administrator rights are limited to those that need them; 2) that other users only have access to those services they need for day-to-day activities; 3) that access is removed when it is no longer needed or when an employee separates from service; and 4) access rights are periodically reviewed to ensure compliance.

<*Human resources officer*> shall work with <*information technology manager*> to ensure that system access needed by new employees is provided on a timely basis, and that notice of termination of employees is provided and acted upon by <*information technology manager*> prior to notice provided to the employee.

6. **Security Incident response:** Appropriately trained staff or contractors are available to support <*member*>'s technology and to timely respond to security incidents.

B. Employee-based Cyber Security Practices

1. All computer users shall receive annual training of <*at least*> one hour, <*each year or spread o v e r two years*> in email and website malware identification, password construction, identifying security incidents, and social engineering attacks.

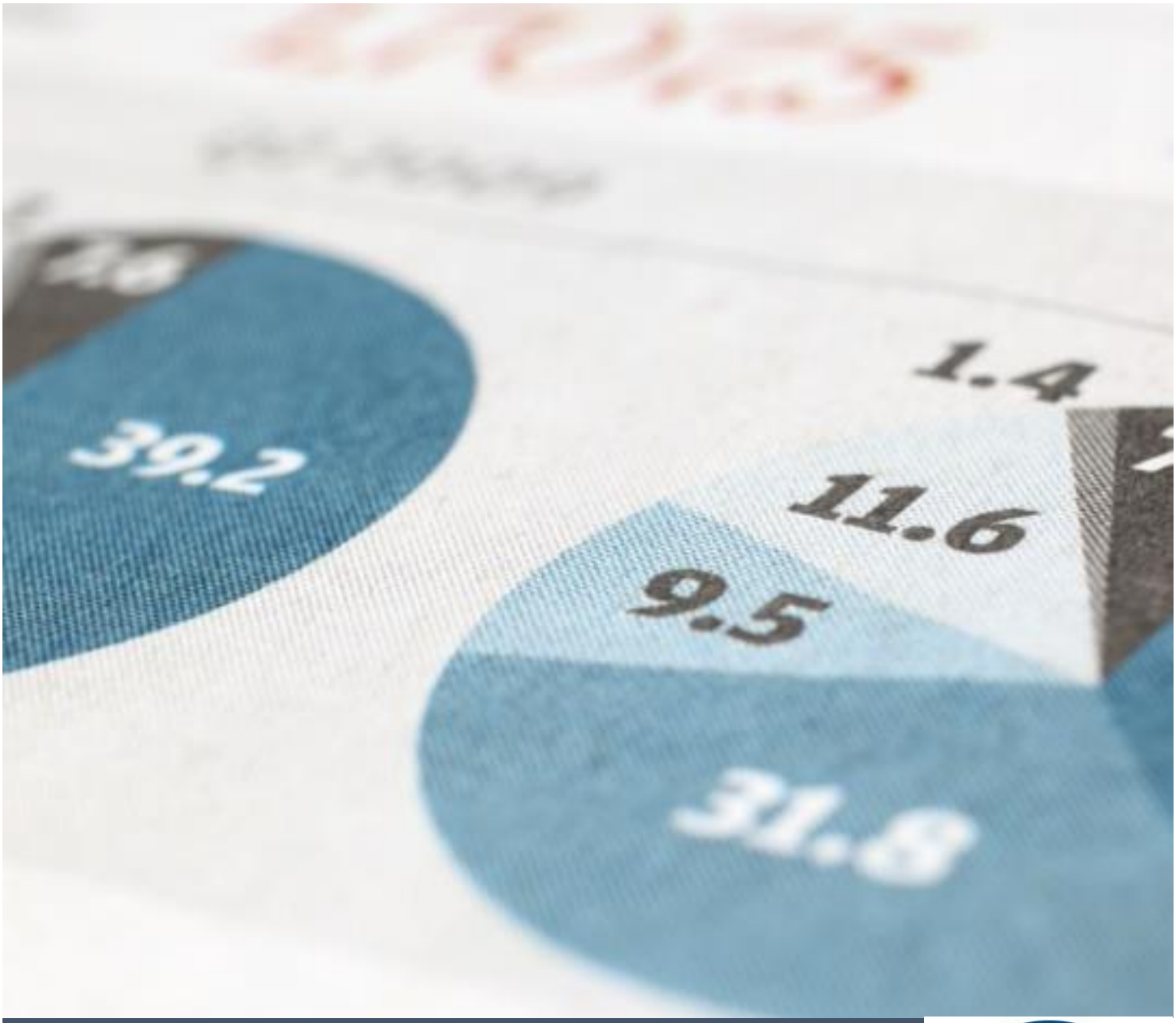
2. Employees are required to use unique passwords or passphrases made up of at least 8 characters, changed periodically, but at least annually. Passwords/phrases shall be at least 8 alpha-numeric characters, with incidental upper- and lower-case letters and symbols.

3. Files that contain protected data shall be password protection or be encrypted when the files are stored or transferred to others, regardless of the storage medium or means of transfer. Examples of protected data includes social security numbers, birthdates, driver's license number, health insurance numbers, etc. Practices shall include ensuring that more than one employee is aware of the password or passphrase used to encrypt these files.

C. Technology Management Practices

1. <*Mayor and Governing Body*> shall ensure that technology policy decisions (i.e., risk assessment, planning, and budgeting) are made with input from staff or advisors that possess appropriate technological expertise. This can be any combination of officials, employees, contractors/consultants, or citizen volunteers as they determine necessary.

2. <*Chief administrative officer or Governing Body*> shall approve and implement a cybersecurity incident response plan to direct staff and guide IT management decision making when a cybersecurity incident takes place.



Appendix 2

Member Minimum Security Response Plan for Cybersecurity Incidents

NJ MEL Cyber Risk Management Program

MEL Member Minimum Security Response Plan for Cybersecurity Incidents

If you suspect a cyber incident has taken place, call the hotline, notify your JIF claims administrator, and start your incident response plan.

This plan is a minimum. A member can modify it to reflect member-specific circumstances, but it must be consistent with the MEL cyber insurance policy, in that the member's Claims Administrator and the XL Catlin Data Breach Hotline are immediately notified of a security incident.

What is a Cybersecurity Incident?

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

What is a 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, and Trojan horses, spyware and adware, zero-day attacks, hacker attacks and denial of service attacks.

What is a 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; and
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.

What is a 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.

Employees need training to understand what a security incident is, what they might observe if one is happening, and how to report it. For example, a security incident could include appearance of a ransomware attack screen, the mouse or computer screen acting on its own, an unauthorized user accessing a computer, not being able to access routine services, device theft, or finding a damaged or non-operating computer.

Other security incidents that would be noticed by system administrators 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
- A denial of service condition against data, network or computer

Responding to a Security Incident

Prerequisites to managing a security incident:

a) The member has access to technology (tech) support personnel (employee or contractor) that understands how to recognize and respond to security incidents.
b) Management knows how to contact tech support when a security incident occurs.
c) Staff has received instruction on how to identify a potential security incident and how to contact tech support when one happens.
d) Management establishes a chain of command for staff to report a potential security incident.
e) It is strongly advised that tech support develops a detailed security incident response plan tied to the member's technology risks.

What to Do When a Possible Security Incident Takes Place

1. The user aware of a possible security incident should identify the affected device(s) (individual machines or network equipment) and:
    a. Immediately contact tech support to report the event and follow their instructions. It is now the responsibility of tech support to notify management of the incident and to execute the security incident response plan.
    b. Continue with Step 2 if tech support is not immediately available.
2. 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. Turn the equipment off if tech support is not immediately available or isolation is not possible. If the machine will not let you do that, unplug the power supply.
3. User reports the incident to management.
    a. If technology support has not been contacted management by this time, management must communicate with support, advise them of the situation, and engage them in the matter.
4. Management or tech support assesses if the incident is a **cyber security breach**, **cyber extortion threat,** or **data breach**. **If it is, or if there is any question that the incident may or may not be one**, management contacts their JIF Claims Administrator to advise them of the incident and management (or tech support) will call the XL Catlin Data Breach Hotline (855-566-4724). If not answered, leave a message naming the member's contact person. 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 reach out to the named contact person. Provide Breach Counsel with all information about the incident and work with them to determine the next steps. Engage technology support as much as practical.
5. Advise the member's risk manager, JIF Executive Director, member legal counsel, chief operating officer, and chief executive officer (i.e., Mayor, Commission Chair, etc.) of the event and actions taken.
6. Follow advice from Breach Counsel and your technology personnel until the issue is resolved.
7. Document all actions as they are taken.

CYBER INCIDENT ROADMAP

You expect or know of a cyber incident.
The clock is ticking to avoid further damage to you and your stakeholders.

Step 1

Report to Claims Administrator

Call XL Catlin 24/7 Breach Hotline at (855) 566-4724 and they will triage your incident.

XL Catlin Cyber Claims Specialist steps in to manage the claim for you

When needed, your Cyber Claims Specialist will engage an XL preapproved expert cyber attorney

In addition to their duties, the attorney will engage any other needed experts

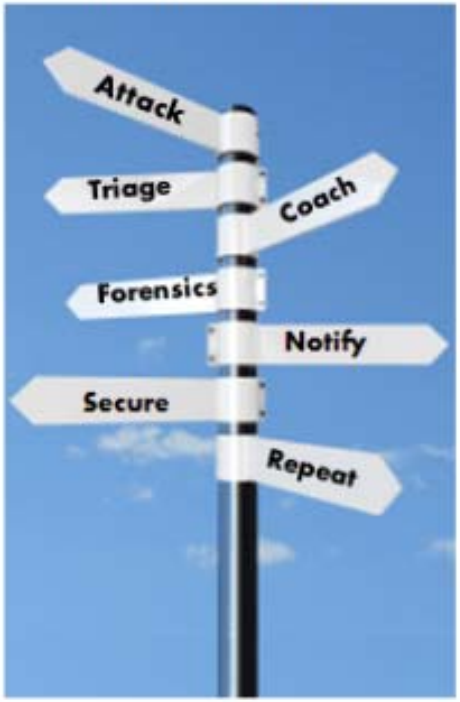
Your Cyber Claims Team will walk you through every step of responding to the incident and offer assistance and take actions on your behalf as necessary.

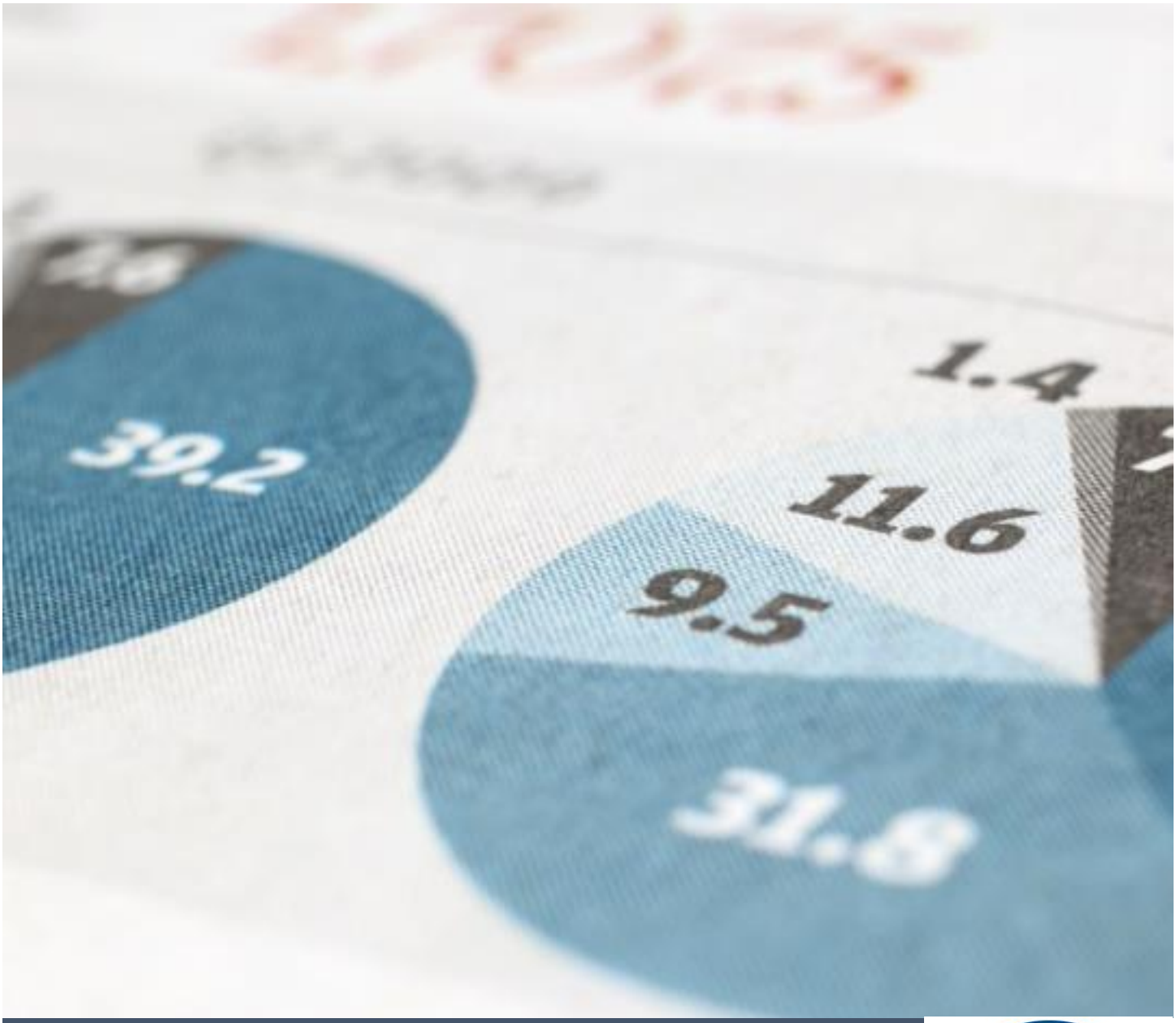
MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL ·

Other Considerations

XL Catlin online cyber portal:
www.cyberriskconnect.com
Access Code: 10448

MEL Coverage Bulletin 17-26





Appendix 3

Minimum Technological Standards Certification

NJ MEL Cyber Risk Management Program

MEL Cyber Insurance Reimbursement Plan

Minimum Technological Standards Certification

Entity Name: _____

JIF Name: _____

Tier 1 — Completed

Technical Competency

Minimum Back-Up Practices

1. Daily incremental backups with at least 14 days of versioning on off-network device for data files _____
2. Weekly off-network full backups of all devices _____
3. All backups are spot-checked monthly _____
4. Data files of third party application providers are part of their backup practice _____
5. Cybersecurity practices are formalized as a policy and implemented _____

Patch

1. All operating and application software with latest versions _____

Defensive Software

1. All desktops and laptops: antivirus, firewall enabled _____
2. Mail server: anti-spam and anti-virus filters _____
3. Internet connected network servers: firewall on all active ports, unused ports closed, anti-virus, anti-malware _____
4. If applicable, Microsoft Office applications open all downloaded files in "Protected Mode" _____

Cyber Hygiene

Training

1. All network users receive annual training of at least one hour, spread over two years, in:
    a. malware identification (email and websites) _____
    b. password construction _____
    c. identifying security incidents _____
    d. social engineering attacks _____

Technology Management

Incident Response Plan

1. Adopted basic cybersecurity incident response plan _____
2. Adopted basic technology practices policy _____

Minimum Technological Standards Certification

Tier 2

Completed

Technical Competency

Physical Server Access

1. Servers are physically protected from unauthorized access _____

Access Privilege Controls

1. Users with administrator rights are limited _____
2. Users only have access to those services they need _____
3. Access is removed when no longer needed or separated from service _____
4. Access rights are periodically reviewed _____

Technology Support

1. Staff or contractors are available to support technology and respond to security incidents _____

Cyber Hygiene

Policies

1. Adopted sound and periodically reviewed government internet and email use policies _____

Protect Information

1. Files containing PII and PHI are password protected or encrypted _____

Password Strength

1. Employees are required to use strong, unique passwords, changed at least annually _____

Technology Management

Leadership Expertise

1. Leadership has access to expertise that supports technology decision making, such as risk assessment, planning and budgeting (check all that apply)
    a. Officials _____
    b. Employees _____
    c. Contractors/consultants _____
    d. Citizen volunteers _____

Signature

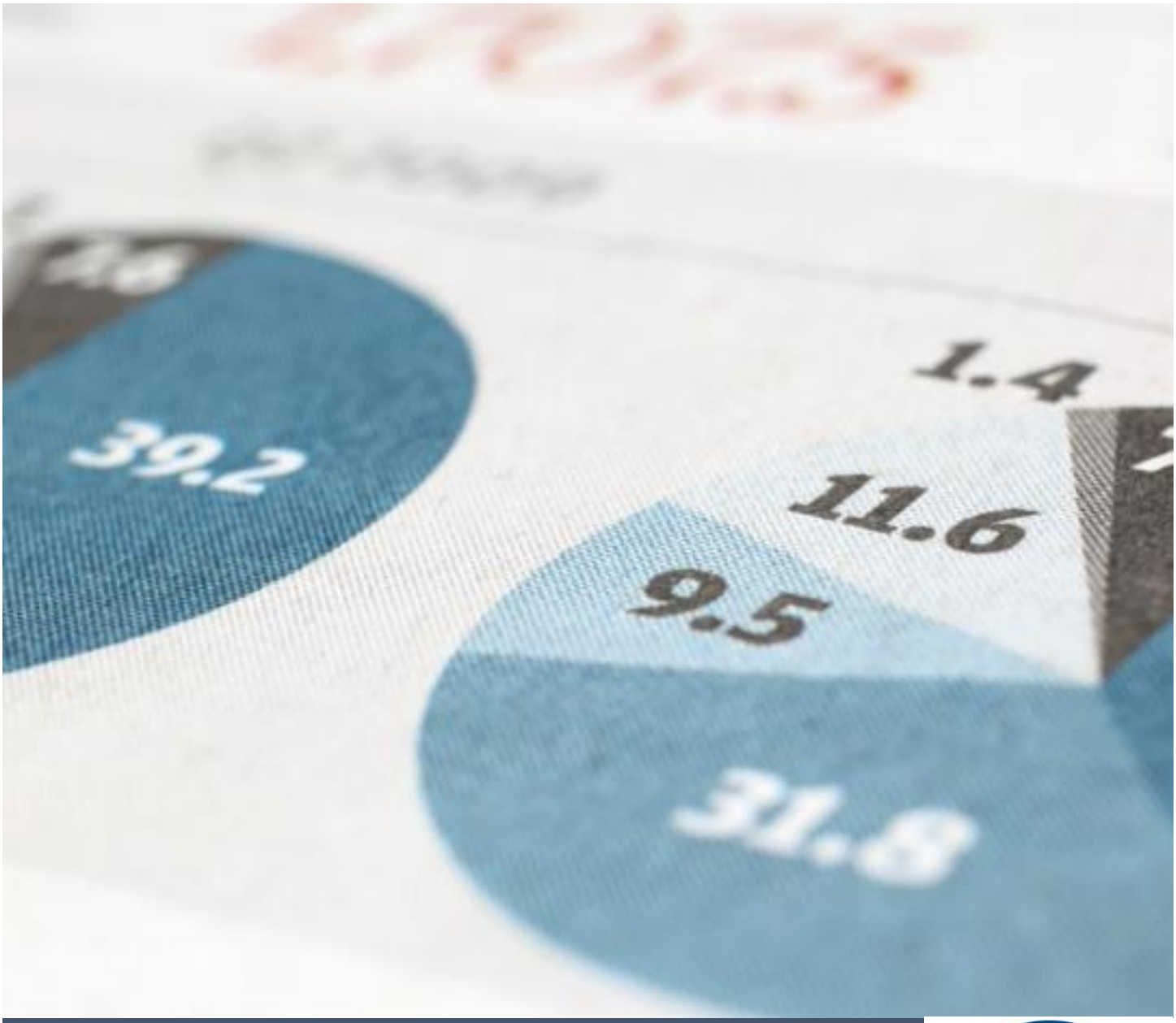
This document must be signed by the mayor, municipal administrator or municipal clerk (or director of entity if not a municipality) AND your technology expert.

MEMBER ENTITY

Print Name	Title
Signature	Date

TECHNOLOGY EXPERT

Print Name	Title
Signature	Date



Appendix 4

Deductible Reimbursement Application

MEL Cyber Risk Management Program

Deductible Reimbursement Application

Entity Name: _____

JIF Name: _____

Claim #: _____

Tier 1 — Completed

Technical Competency

Minimum Back-Up Practices*

1. Daily incremental backups with at least 14 days of versioning on off-network device for data files _____
2. Weekly off-network full backups of all devices _____
3. All backups are spot-checked monthly _____
4. Data files of third party application providers are part of their backup practice _____
5. Cybersecurity practices are formalized as a policy and implemented _____

Patch*

1. All operating and application software with latest versions _____

Defensive Software*

1. All desktops and laptops: antivirus, firewall enabled _____
2. Mail server: anti-spam and anti-virus filters _____
3. Internet connected network servers: firewall on all active ports, unused ports closed, anti-virus, anti-malware _____
4. If applicable, Microsoft Office applications open all downloaded files in "Protected Mode" _____

Cyber Hygiene

Training*

1. All network users receive annual training of at least one hour, spread over two years, in:
    a. malware identification (email and websites) _____
    b. password construction _____
    c. identifying security incidents _____
    d. social engineering attacks _____

Technology Management

Incident Response Plan & Technology Practices Policy*

1. Adopted basic cybersecurity incident response plan (Appendix 2) _____
2. Adopted basic technology practices policy (Appendix 1) _____

Notes

1. All items marked with an asterisk require documented support, outlined later in this application.

2. All appendices referenced are included in the MEL Cyber Risk Management Program packet.

MEL Cyber Risk Management Program

Deductible Reimbursement Application

Tier 2 — Completed

Technical Competency

Physical Server Access

1. Servers are physical protected from unauthorized access _____

Access Privilege Controls

1. Users with administrator rights are limited _____
2. Users only have access to those services they need _____
3. Access is removed when no longer needed or separated from service _____
4. Access rights are periodically reviewed _____

Technology Support*

1. Staff or contractors are available to support technology and respond to security incidents _____

Cyber Hygiene

Policies*

1. Adopted sound and periodically reviewed government internet and email use policies _____

Protect Information

1. Files containing PII and PHI are password protected or encrypted _____

Password Strength*

1. Employees are required to use strong, unique passwords, changed at least annually _____

Technology Management

Leadership Expertise

1. Leadership has access to expertise that supports technology decision making, such as risk assessment, planning and budgeting (check all that apply)
    a. Officials _____
    b. Employees _____
    c. Contractors/consultants _____
    d. Citizen volunteers _____

Notes

1. All items marked with an asterisk require documented support, outlined later in this application.

2. All appendices referenced are included in the MEL Cyber Risk Management Program packet.

MEL Cyber Risk Management Program

Deductible Reimbursement Application

Supporting Documentation Required

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

Tier 1

1. Cyber hygiene training certificates
2. Screen shots of antivirus coverage
3. Screen shots of patches
4. Backup reports showing offsite backups
5. Copies of Incident Response Plan & Technology Practices Policy (appendices 1 and 2)

Tier 2

1. List of staff or contractors that support technology
2. Copies of adopted policies
    a. Access, use, & control policy (appendix 1)
    b. Acceptable use policy (MEL standard communications email policy)
    c. PII & PHI encryption policy (appendix 1)
    d. Password policy (appendix 1)

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

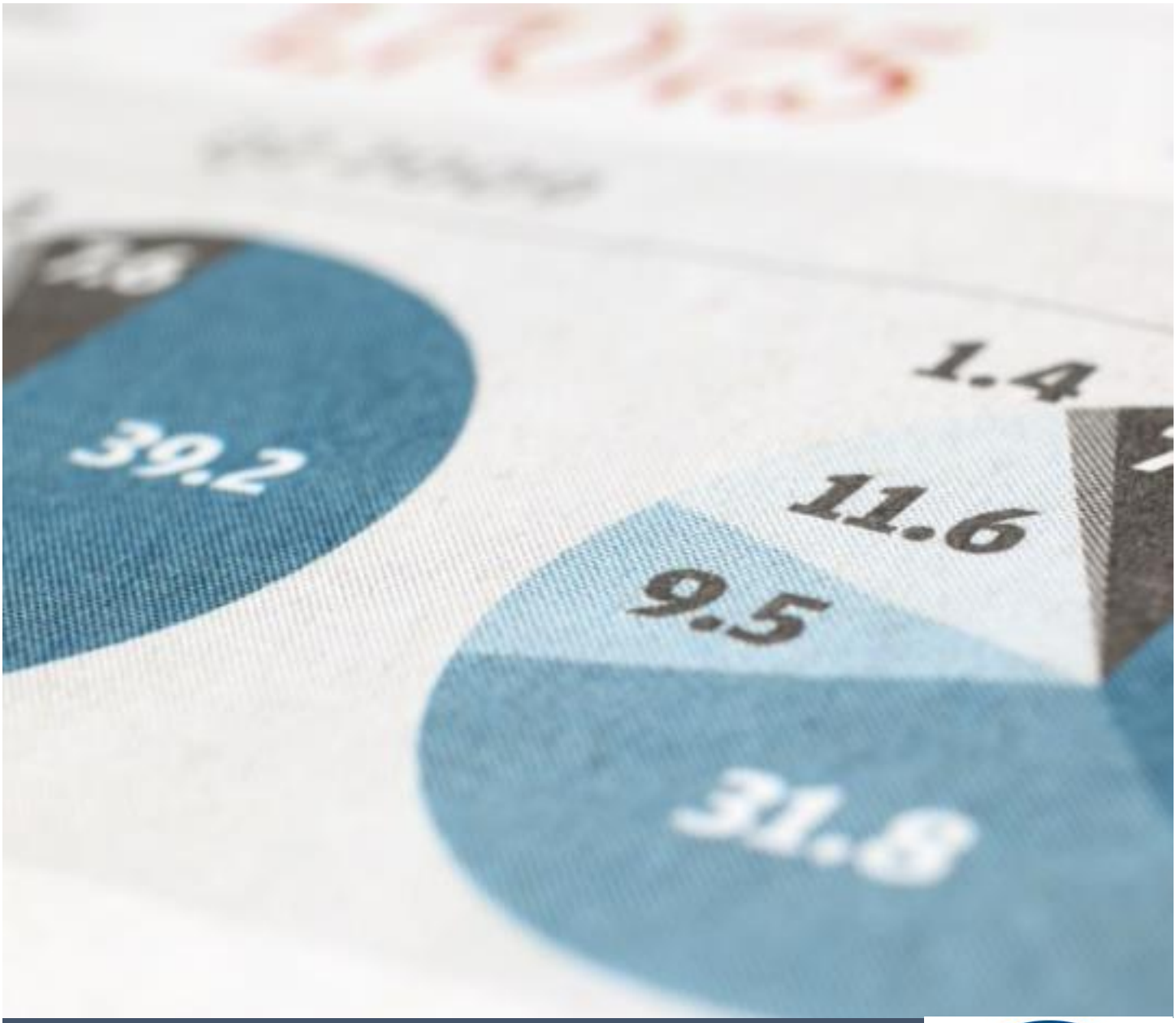
Print Name _____ Title _____

Signature _____ Date _____

TECHNOLOGY EXPERT

Print Name _____ Title _____

Signature _____ Date _____



Appendix 5

Additional Security Practices

ADDITIONAL SECURITY PRACTICES TO CONSIDER

Subject to adequate budgeting and staffing resources, there are additional technological enhancements that members can implement to help manage their risk in using technology. These practices include the following suggested actions:

a) Conduct a security review of third party vendors

b) Conduct and maintain an inventory of authorized and unauthorized devices

c) Servers are protected from environmental hazards

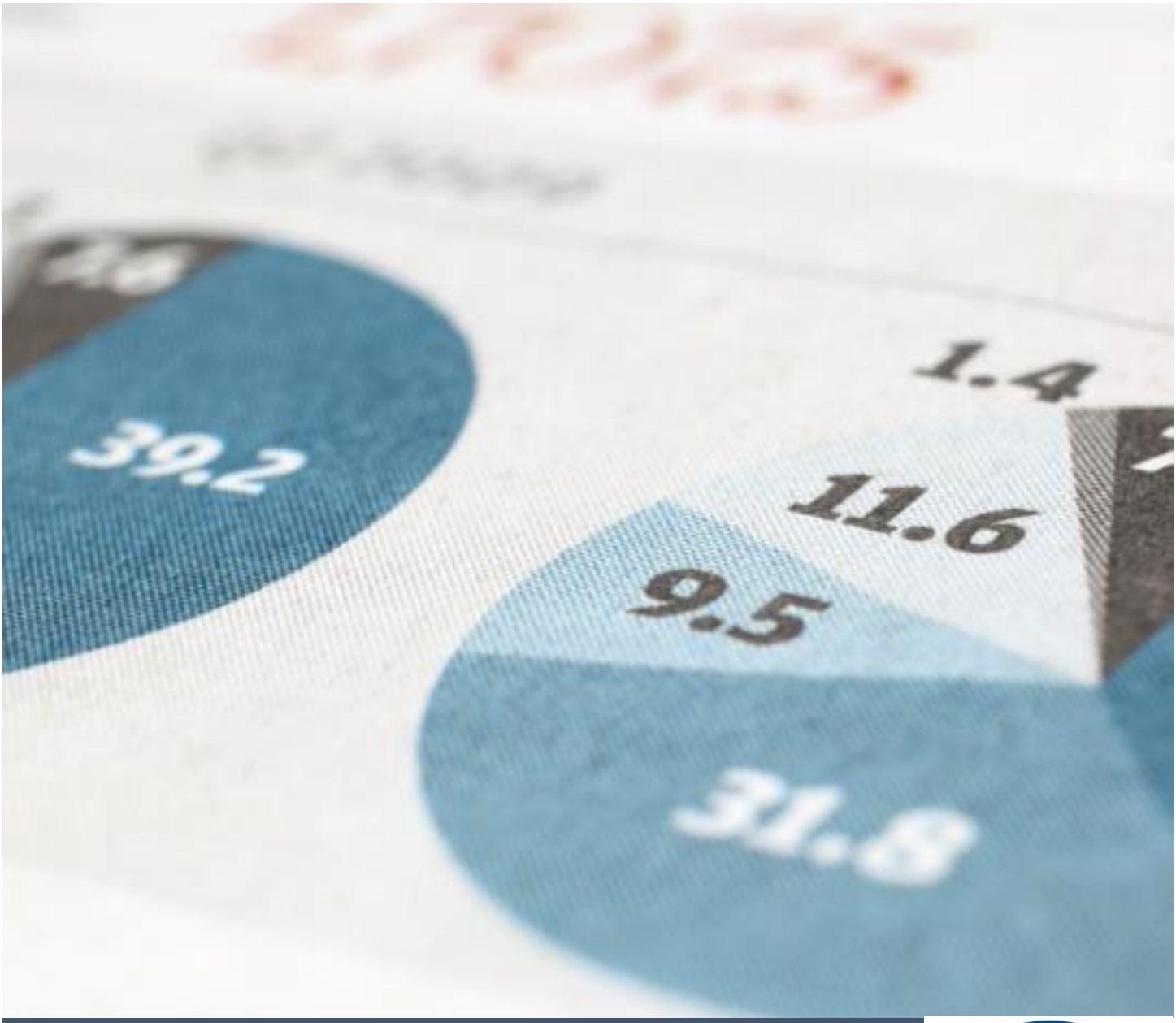
d) Conduct and maintain an inventory of authorized and unauthorized software and whitelisting of approved software

e) Implement basic internet content filtering

f) Ensure that a firewall protects the *<member>*'s Wi-Fi network from any public Wi-Fi network

g) Employees receive a total of one hour of annual cyber hygiene training

h) *<Primarily for members with managed or sophisticated technology profiles (e.g. with several full time IT staff members):* Implement and maintain the CIS Critical Security Controls and the NIST Cybersecurity Framework as part of the technology planning practices



Appendix 6

Cyber Insurance Reimbursement Plan Infographic

NJ MEL Cyber Risk Management Program

MEL Cyber Insurance Reimbursement Plan

- **$10,000 standard claim deductible**
- **$5,000 reimbursement if TIER 1 requirements are met**
- **$7,500 reimbursement if TIER 1 & 2 requirements are met**

Tier	Technical Competency	Cyber Hygiene	Tech Management
1	Minimum back-up practices Patch Defensive software	Training Tech practices policy	Incident response plan
2	Controlled server access Access privilege controls Technology support	Policies Protect information Password strength	Leadership has expertise

Plus +

Improve Your Technical Competency With...

- Safe and secure servers
- Third party risk assessments
- Device inventory
- Software inventory
- Secure internet usage
- Wi-Fi controls
- Additional training

Brought to You By

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL ·

RUTGERS
Edward J. Bloustein School of Planning and Public Policy

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND • MEL •

MEL

Protecting You and
Your Hometown

AGAINST CYBER ATTACKS