



## Tier 1

### Minimum Back-Up Practices

1. Use of standardized system images or virtualized desktops. \_\_\_\_\_
2. Back-up copy of all application 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 application data must also be backed-up to the same standards. \_\_\_\_\_

### Patching Practices

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. Firewall rules and policies are reviewed or reassessed at least twice per year. \_\_\_\_\_
5. Microsoft Office applications open all downloaded files in "Protected Mode". \_\_\_\_\_

### Security Awareness Training

1. All computer users receive annual training of at least one hour on at least the following topics: \_\_\_\_\_
  - a. Password Construction
  - b. Identifying security incidents
  - c. Social Engineering attacks
  - d. Business email compromise



## 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 Technology Policy Ver 2.2. \_\_\_\_\_

### Email Warning

1. The municipality has implemented an automatic warning label to all emails coming from outside of your organization. \_\_\_\_\_

### Cybersecurity Incident Response Plan

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

### Technology Practices Policy

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

### Government Cyber Memberships

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



## Tier 2

### Server Security

1. The 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 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

2. 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 Technology Policy Ver 2.2). \_\_\_\_\_

### 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. \_\_\_\_\_



## *MEL Cyber Risk Management Deductible Reimbursement*

---

### **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

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

## Remote Access

- 3. 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 Technology Policy Ver 2.2. \_\_\_\_\_

## 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. \_\_\_\_\_

## 3rd Party Risk Management

- 1. The municipality has access to the MEL’s 3<sup>rd</sup> Party Risk Assessment Tool to assess a vendor’s risk when issuing new or renewing contracts. \_\_\_\_\_



## Required Documentation

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

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



## MEL Cyber Risk Management Deductible Reimbursement

# Signature

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

### **MEMBER ENTITY**

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

### **TECHNOLOGY EXPERT**

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date