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