Borough of Clayton

Resolution 212-19

A RESOLUTION ADOPTING TECHNOLOGY RISK MANAGEMENT STANDARDS IN COMPLIANCE WITH THE NEW JERSEY MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND'S CYBER RISK MANAGEMENT PLAN'S TIER ONE REQUIREMENTS

Whereas, the Borough of Clayton is a member of the TRICO JIF which secures insurance protection through the New Jersey Municipal Excess Liability Joint Insurance Fund (NJ MEL); and

Whereas, through its membership in the TRICO JIF, the Borough of Clayton enjoys cyber liability insurance coverage to protect the Borough of Clayton from the potential devastating costs associated with a cyber related claim; and

Whereas, in an attempt to prevent as many cyber related claims as possible, the NJ MEL developed and released to its members the NJ MEL Cyber Risk Management Plan; and

Whereas, the NJ MEL Cyber Risk Management Plan outlines a set of best practices and standards broken out into Tier 1 & Tier 2 standards that if adopted and followed will reduce many of the risks associated with the use of technology by the Borough of Clayton; and

Whereas, in addition to the reduction of potential claims, implementing the following best practices and standards will enable the Borough of Clayton to claim a reimbursement of a paid insurance deductible in the event the member files a claim against Borough of Clayton's cyber insurance policy, administered through the TRICO JIF and the Municipal Excess Liability Joint Insurance Fund;

Now Therefore Be It Resolved, that the Borough of Clayton does hereby adopt the following best practices and standards, a copy of which is attached hereto and incorporated herein by reference, in accordance with Tier 1 of the NJ MEL Cyber Risk Management Plan;

- **System and data back-up**
- **Security and system patching**
- **Defensive software**
- **Security Awareness Training**
- **Incident Response Plan**

And, Be It Further Resolved, that a copy of this resolution along with all required checklists and correspondence be provided to the NJ MEL Underwriter for their consideration and approval

This Resolution was duly adopted by the Borough of Clayton at a public meeting held on October 10, 2019.

Christine Newcomb

Christine Newcomb, Municipal Clerk

Tom Bianco, Mayor

Borough of Clayton

Information Technology Security Practices Policy For Tier 1 Compliance with the MEL Cyber Risk Management Plan

Document Management

Document Owner:	**Borough of Clayton**
Document Name:	Information Security/Technology Practices Policy for Tier 1 Compliance
Version No:	Version: 1.0
Adoption Date:	9/4/2019
Distribution Date:	
Author (Source):	
Last Review Date:	9/4/2019
Next Review Date:	9/4/2020
Data Classification:	**Sensitive**

Table of Contents

Document Management 2

1. Policy Statement **4**

2. Reason for the Policy **4**

3. Scope **4**

4. Tier 1 Technical Policies **4**

4.1 Information Backup Policy 4

4.2 Patch Management Policy 5

4.3 Defensive Software Policy 6

4.4 Security Awareness Training 6

4.5 Incident Response Policy (SEE SEPARATE DOCUMENT: CYBER INCIDENT REPSONSE PLAN POLICY) 6

4.6 Governing Body Adopts Resolution Adopting Technology Risk Management Standards in Compliance with the NJ MEL Cyber Risk Management Plan's Tier 1 Standards 7

1. Policy Statement

The Information Security/Technology Practices Policy defines the information security practices necessary to ensure the security of our information systems and the information that they store, process, and/or transmit.

2. Reason for the Policy

Our municipality acts as the custodian of a wealth of sensitive information relating to the services we provide and the constituents we serve. 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 information systems that store, process, or transit it.

This policy affirms our commitment to information security by specifying the policies and standards necessary to achieve our security objectives, including compliance with all Federal and State requirements, and Tier 1 of the **Municipal Excess Liability Fund's Minimum Technology Proficiency Standards.**

3. Scope

All information systems, including those operated by a third party, are expected to comply with this policy. In addition, all personnel, contractors, and vendors are expected to comply with this policy.

Non-compliance with this policy can result in disciplinary actions in accordance with your municipality's disciplinary policy.

4. Tier 1 Technical Policies

4.1 Information Backup Policy

Ensuring that all important data is regularly "backed up" is critical to ensuring the availability of the information that we need to provide services to our constituents. The objective of the Information Backup Policy is to ensure that we can fully recover all of the municipality's data in an incident (e.g., ransomware, flood). If desktops are virtualized, meaning no local data is stored on them, the requirement to backup desktops does not apply.

Our Approach:

- All data is backed up twice per day from the server to a removable storage drive.
- Full server backups are performed nightly.
- Monthly backups are stored off site
- We spot check backups monthly by restoring a random file, or the use of backup software to perform a nightly validation and provide a report to our IT Director/vendor for review.
- We run the following critical applications and have ensured that the required backups are being performed. Documentation of this information is kept on XXX.
    a. Ex: Edmunds & Associates

b. *List others here*

4.2 Patch Management Policy

Ensuring that all systems are patched on a regular basis is critical to ensuring the availability of the information that we need to provide services to our constituents. The objective of the Patch Management Policy is to ensure that we have a plan to keep systems patched so that they are not vulnerable to exploit by malware or a malicious individual. Outdated and/or unsupported operating systems/applications should not be used.

Our Approach:

- Your IT Director or IT vendor will oversee the patch management process. They will review the patches before applying them.
- All desktop operating systems are configured to use the Windows Update Service which ensures patches are deployed weekly. Emergency patches are deployed within 48 hours.
- Microsoft Office products, Chrome, Firefox, and Adobe Reader are patched within 2 days of important patches being released using ManageEngine.
- All server operating systems are patched monthly using SCCM (System Center Configuration Manager) unless testing shows the patch will create application problems. A patch exception can be granted by the highest ranking administrative official in the municipality upon review and approval of the exception and the compensating controls that will be deployed to protect the server/application until the patch can be deployed.
- Microsoft SQL Server, and XXX are patched manually as important patches are released. A patch exception can be granted by the highest ranking administrative official in the municipality upon review and approval of the exception and the compensating controls that will be deployed to protect the server/application until the patch can be deployed. A compensating control for an unapplied patch might include:
    1. Updating a firewall to limit access to that server and/or that port
    2. Turning off a service on that system
    3. Adding alerts for an event that might indicate an attempt to exploit the vulnerability the patch mitigates
- System administrators coordinate patch upgrades with applications residing on non-Microsoft systems and third party systems/applications to ensure upgrades will not disable their applications. When upgrades cannot be applied, an exception can be granted by the highest ranking administrative official in the municipality upon review and approval of the exception and the compensating controls that will be deployed to protect the application until the patch can be deployed.

4.3 Defensive Software Policy

Ensuring that all computing systems are resilient to attack is critical to ensuring the confidentiality, integrity, and availability of the information that we need to provide services to our residents. The objective of this Defensive Software Policy is to ensure that all systems are protected by software that minimizes the likelihood that an attack by malicious individuals and/or malware will result in the compromise of that system.

Our Approach:

- All desktops are protected by Windows Defender (or appropriate program) which provides antivirus, firewall, and anti-malware capabilities.
- All mail servers are protected by Symantec (or appropriate software) which provides anti-spam, and antivirus capabilities.
- All servers that are reachable from the Internet are protected by a Cisco ASA firewall (or appropriate program.) Only those ports required to be reachable are reachable from the Internet.
- All servers are protected by McAfee (or appropriate software) which provides anti-virus and anti-malware capabilities.
- All Microsoft Office applications are set to download all files in "Protected Mode."

4.4 Security Awareness Training

All employees need to receive appropriate awareness education and training on our security policies and procedures, as relevant for their job function. The objective of the Security Awareness Policy is to ensure that all employees have the information security knowledge necessary to achieve their information security responsibilities.

Our Approach:

- All employees and contractors with access to the municipality's information assets receive annual training of at least 30 minutes that includes (but may not be limited to) malware identification (email and websites), password construction, identifying security incidents, and social engineering.
- All employees are made aware of their responsibilities outlined in the Information Security/Technology Practices Policy by being provided a copy and/or training when they are hired.
- Changes to this policy are communicated to all employees via email.

4.5 Incident Response Policy (SEE SEPARATE DOCUMENT: CYBER INCIDENT REPSONSE PLAN POLICY)

The municipality needs an Incident Response Plan to ensure that we can detect and respond to incidents in a timely manner to minimize the potential impact to our municipality. The objective of the policy is to ensure an appropriate Incident Response Plan is maintained and that responsibilities relating to security incidents are clearly communicated.

Our Approach:

- We publish an Incident Response Plan, which is reviewed/updated at least annually.
- We communicate the Incident Response Plan and responsibilities to all employees.
- Our Incident Response Plan outlines the staff or contractors necessary to support the secure operations of our municipality and respond to incidents effectively.

4.6 Governing Body Adopts Resolution for Technology Risk Management Standards in Compliance with the NJ MEL Cyber Risk Management Plan's Tier 1 Requirements

See separate Resolution titled: "Sample Tier 1 Information Technology Standards Policy Resolution.docx."