Borough of Clayton

Resolution 213-19

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 TWO 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 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 2 of the NJ MEL Cyber Risk Management Plan;

- **Server Security**
- **Limiting Access Privileges**
- **Acceptable Use of Internet and Email**
- **Protection of Data**
- **Passwords Policy**
- **Appropriate level of Technology Support**
- **Leadership has Expertise to Support Technology Decision Making**

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 2 Compliance with the MEL Cyber Risk Management Plan

Document Management

Document Owner:	**Borough of Clayton**
Document Name:	Information Security/Technology Practices Policy for Tier 2 Compliance
Version No:	Version: 1.0
Adoption Date:	10/4/2019
Distribution Date:	
Author (Source):	
Last Review Date:	10/4/2019
Next Review Date:	10/4/2020
Data Classification:	**Sensitive**

Table of Contents

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 transmit 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 2 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.

Our municipality has access to the expertise necessary to support critical technology decision making, including the following examples:

- IT Support
- Legal Support
- Risk Management Supopoort

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

4. Tier 2 Technical Policies

4.1 Server Physical Security Policy

Ensuring that access to servers is restricted to a "need to access" basis reduces the likelihood that those systems or the data they contain will be compromised. The objective of the Server Physical Security Policy is to ensure that sufficient controls are in place to prevent unauthorized access to our servers.

Our Approach:

- Our servers are housed in a locked server rack or room to prevent unauthorized access.
- Gaining access to our servers requires a physical key, access badge and/or combination door lock.

- Access to the server room is approved by the highest ranking administrative official in the municipality and/or the IT Director, and is restricted to a "need to access" basis.
- Each quarter the server access list is reviewed by the highest ranking administrative official in the municipality and/or the IT Director to ensure that only those with a current need to access, have access.
- When access card or key is secured from the individual, the list is updated and the means of access is disabled or collected.

4.2 Access Control Policy

Ensuring that the level of system and information access is appropriately restricted is critical to ensuring information security. The objective of the Access Control Policy is to provide guidance on restricting access to a "need to access" basis.

Our Approach:

- Administrator rights on desktops are only granted when approved by the highest ranking administrative official in the municipality and/or the IT Director.
- Access to key applications and network resources, including file shares, is access controlled.
- Employee access is granted when a new person is hired, and the hiring manager consults with the highest ranking administrative official in the municipality and/or the IT Director to determine the level of access and equipment that the new employee needs to perform their job function (e.g., key cards, Office 365, network, key applications, etc.)
- Employee access is removed when an employee is terminated/leaves the municipality. The employee's manager submits written notification to the highest ranking administrative official in the municipality and/or the IT Director. Where possible, the request should proceed the person's termination/leave by 48 hours to ensure that IT has the time to disable access.
- Conduct employee access rights reviews for key systems on a periodic basis per the following schedule:
    a. Active Directory/Quarterly/Director of IT
    b. Server Room/ Quarterly /Director of IT
    c. 3rd Party Contractors (e.g. Edmunds)/Quarterly/CFO
- The number of "administrators" for key systems including any 3rd Party Contractors (e.g. Edmunds) are kept to the minimum number required to ensure effective and secure operation. The number of personnel with administrative level access to these systems is reviewed quarterly by the highest ranking administrative official in the municipality and/or the IT Director. Records for this review are kept in the Cloud.

4.3 Acceptable Use Policy

All employees need to receive appropriate guidance to the acceptable use of our computing assets including appropriate use of the Internet and email. The objective of the **Acceptable Use Policy** is to ensure that all employees have the information security knowledge necessary to minimize risk to themselves and our municipality when using computing assets.

Our Approach:

- We publish an Acceptable Use Policy. (See page 24 of the MEL Model Personnel Policies and Procedures Manual.)
- Employees formally acknowledge their receipt and understanding of the Acceptable Use Policy when hired and annually thereafter.

4.4 "Protected Data" Policy

The security applied to "Protected Data" when stored in files and/or transmitted needs to be adequate to meet any legal, regulatory, or contractual obligations relating to the data. The objective of the "Protected Data" Protection Policy is to outline user responsibilities when working with "Protected Data."

Our Approach:

- "Protected Data" is defined as:
    a. Personally Identifiable Information (PII) including: Social Security numbers, checking account numbers, birthdate, driver's license number, passport number, and xxx.
    b. Protected Health Information (PHI) including: health insurance numbers, medical diagnostic codes, medical records, and xxx.
    c. Payment Card Industry (PCI) information including: credit card numbers (includes payer account number and sensitive authentication data). See PCI DSS (Payment Card Industry Data Security Standard) regulation for additional guidance.
- All files stored or transmitted that contain protected data are required to be encrypted (AES - Advanced Encryption Standard-256 or stronger, which is the norm used worldwide to encrypt data) using a password that conforms with our Password Policy. Acceptable file protection includes the following examples:
    a., Microsoft Word password protection
    b. Microsoft Excel password protection
    c. Adobe Acrobat password protection
    d. WinZip password protection
- Passwords used for encrypted files should be stored in a safe and secured location.

4.5 Password Policy

All information and computing assets should be protected by passwords whose "strength" is proportional to the value of the asset. The objective of the Password Policy is to ensure that users construct passwords that minimize the likelihood that the assets they protect will be accessed by unauthorized individuals.

Our Approach:

- Employees are required to use strong, unique passwords comprised of at least 8 characters and include upper and lower-case letters, symbols, and numbers.
    a. Longer passwords (10 or more characters) are preferable and encouraged.
    b. Administrator passwords should be 12 characters or more in length.
    c. Passwords are changed at least annually and/or when known to be compromised.

4.6 Technology Support

Municipal staff or IT contractors are available to support all municipal employee's technology usage and respond to security incidents.

Our Approach:

- Distribute IT contact information to municipal employees annually and update contact lists when a change occurs.

4.7 Leadership Has 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 as appropriate to the municipality.

Our Approach:

- Meet with IT Professionals at least annually to discuss the contents of this document to ensure that your Municipality can adhere to the standards outlined in this policy.

4.8 Governing Body Adopts Resolution for Technology Risk Management Standards in Compliance with the NJ MEL Cyber Risk Management Plan's Tier 2 Requirements

See separate Resolution "Sample Tier 2 Information Technology Standards Policy Resolution.docx."