

Township of Florence

Resolution 2019-195

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 Township of Florence is a member of the BURLCO JIF which secures insurance protection through the New Jersey Municipal Excess Liability Joint Insurance Fund (NJ MEL); and

Whereas, through its membership in the BURLCO JIF, the Township of Florence enjoys cyber liability insurance coverage to protect the Township of Florence 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 Township of Florence; and

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

Now Therefore Be It Resolved, that the Township of Florence 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

I, NANCY L. ERLSTON, CLERK of the Township of Florence, County of Burlington, State of New Jersey, do hereby certify that the foregoing is a true copy of the Resolution approved by Township Council at their November 13, 2019 meeting.



Nancy L. Erlston, RMC
Township Clerk



Township of Florence

Information Technology Security
Practices Policy
For Tier 2 Compliance with the MEL
Cyber Risk Management Plan

Document Management

Document Owner:	Township of Florence
Document Name:	Information Security/Technology Practices Policy for Tier 2 Compliance
Version No:	Version: 1.0
Adoption Date:	10/14/2019
Distribution Date:	
Author (Source):	
Last Review Date:	10/14/2019
Next Review Date:	10/14/2020
Data Classification:	Sensitive

Table of Contents

<i>Document Management</i>	2
1. Policy Statement	4
2. Reason for the Policy	4
3. Scope	4
4. Tier 2 Technical Policies	4
4.1 <i>Server Physical Security Policy</i>	4
4.2 <i>Access Control Policy</i>	5
4.3 <i>Acceptable Use Policy</i>	5
4.4 <i>“Protected Data” Policy</i>	6
4.5 <i>Password Policy</i>	6
4.6 <i>Technology Support</i>	7
4.7 <i>Leadership Has Expertise</i>	7
4.8 <i>Governing Body Adopts Resolution for Technology Risk Management Standards in Compliance with the NJ MEL Cyber Risk Management Plan’s Tier 2 Requirements</i>	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 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 Support

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."



Township of Florence

Cyber Incident Response Plan

Document Management

Document Owner:	Township of Florence
Document Name:	Cyber Incident Response Plan
Version No:	Version: 1.0
Adoption Date:	10/14/2019
Distribution Date:	
Author (Source)	
Last Review Date:	10/14/2019
Next Review Date:	10/14/2020
Data Classification:	Sensitive

Table of Contents

<i>Document Management</i>	2
1. Policy Statement	4
2. Reason for the Policy	4
3. Scope	4
3.1 <i>Designation of an Incident Response Manager</i>	4
3.2 <i>Responsibilities</i>	4
4. Incident Response Phases	5
4.1 <i>Detection, Reporting, & Analysis</i>	5
4.2 <i>Forensics</i>	6
4.3 <i>Containment, Eradication, & Recovery</i>	6
4.4 <i>Post-Incident Review</i>	7
4.5 <i>Incident Response Team</i>	7
4.6 <i>Incident Response Notification Information</i>	7
5. Periodic Review	7
6. Special Situations/Exceptions	8
7. Related Information	8
8. Definitions Related to Cyber Liability Insurance	8

1. Policy Statement

The Incident Response Plan defines our methods for identifying, tracking, and responding to network, and computer-based security incidents.

2. Reason for the Policy

The Incident Response Plan is established to assist in protecting the integrity, availability, and confidentiality of employee and constituent data and assist in complying with statutory and regulatory/ contractual obligations including the Municipal Excess Liability Fund's Minimum Technology Proficiency Standards.

Responding quickly and effectively to an Incident is critical to minimizing the spread of the Incident and/or the business, financial, legal, and/or reputational impact. Incident Response generally includes the following phases:

- Detection, Reporting, and Analysis
- Forensics (optional, important if legal action is being considered)
- Containment, Eradication, and Recovery
- Post-Incident Review

3. Scope

This plan governs incidents that have a significant negative impact on information technology systems and/or sensitive information (hereinafter, "Incidents"). Incidents can include denial of service, malware, ransomware, and/or phishing attacks that can significantly impact operations and/or result in the unintended disclosure of sensitive data (e.g., constituent data, Protected Health Information, Personally Identifiable Information, credit card data, and law enforcement records).

Minor events (e.g., routine detection, and remediation of a virus, a minor infraction of a security policy, or other similar issues that have little impact on day-to-day business operations) are not considered an Incident under this policy.

3.1 Designation of an Incident Response Manager

The municipality shall designate an Incident Response Manager who is either a full or part time IT person working in your municipality on a daily basis or the highest-ranking administrative person in your municipality that employees would normally contact when having computer or IT problems. Ideally, this person should be readily available to employees in the case of a cyber security event.

3.2 Responsibilities

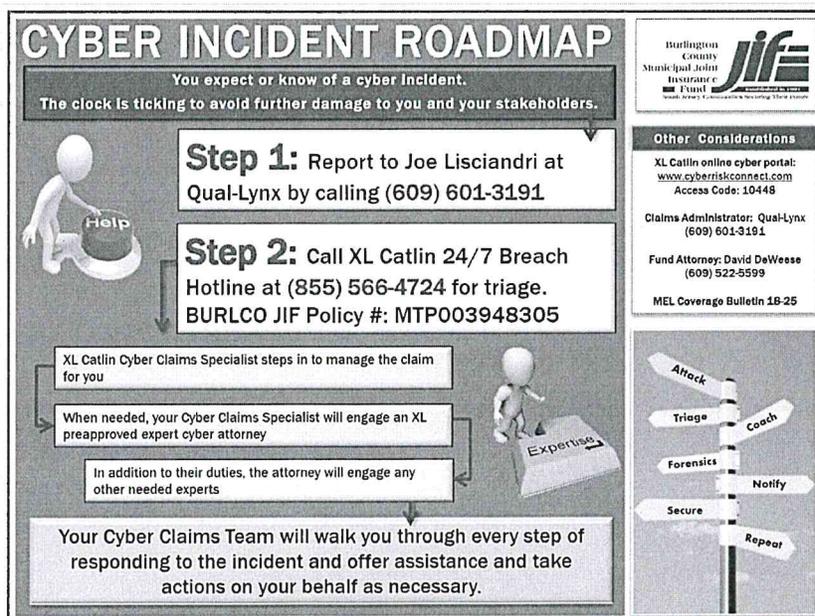
- The municipality has designated an Incident Response Manager that is responsible for determining whether an event, or a series of security events, is declared an Incident.
- The Incident Response Manager is responsible for ensuring that this policy is followed.
- The Incident Response Manager is responsible for establishing an Incident Response Team to support the execution of this plan.

- The Incident Response Team is tasked with executing this plan in accordance with and at the direction of the Incident Response Manager.
- The highest-ranking administrative official in the municipality is responsible for ensuring that end-users have sufficient knowledge to recognize a potential security Incident and report it in accordance with this plan.
- Employees are responsible to report potential security incidents in a timely manner and provide any requires support during plan execution.

4. Incident Response Phases

4.1 Detection, Reporting, & Analysis

1. If a user, employee, contractor, or vendor observes a potential security event they should notify the Incident Response Manager immediately. If the Incident Response Manager is not available, the events should be immediately reported to the highest-ranking administrative official.
2. The Incident Response Manager is responsible for communicating the Incident, its severity, and the action plan to the highest-ranking administrative official.
3. If the Incident Response Manager or the highest-ranking administrative official are not available, a user should 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. If isolating the machine from the network is not possible then unplug the machine from its power source.
4. If you have determined or suspect that the Incident is a cyber security breach, cyber extortion threat, or data breach (*see Definitions Related to Cyber Liability Insurance – Section 8 of this document*) proceed to Step 5. If not, proceed to Step 6.
5. For a cyber security breach, please follow this process:



If the XL Catlin Data Breach Hotline does not answer, leave a message with your contact information. 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 gather information about the Incident and work with you to determine an action plan.

The Incident Response Manager should follow the advice from the Breach Counsel until the issue is resolved.

6. *If the Incident is determined not to be a cyber security breach, cyber extortion threat, or data breach, the Incident Response Manager should work with the Incident Response Team to assess the Incident, develop a plan to contain the Incident, and ensure the plan is communicated to and approved by the highest ranking administrative official.*
7. The Incident Response Manager should ensure that all actions are documented as they are taken and that the highest-ranking administrative official, Incident Response Team, and outside support are regularly updated.

4.2 Forensics

Security incidents of a significant magnitude that may require legal action post-Incident may require that a forensics investigation take place. Once that need has been established all additional investigation/containment activities need to be directed and/or performed by a forensics specialist to ensure that the evidence and chain of custody is maintained. The highest-ranking administrative official, in consultation with the Incident Response Manager and/or XL Caitlin will advise if engaging a forensics firm is required.

4.3 Containment, Eradication, & Recovery

Containment is the act of limiting the scope and magnitude of the attack as quickly as possible. Containment has two goals: preventing data of note from being exfiltrated and preventing the attacker from causing further damage.

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the OS and applications is preferred.

Recovery allows business processes affected by the Incident to recover and resume operations. It generally includes:

- Reinstall and patch the OS and applications
- Change all user and system credentials
- Restore data to the system
- Return affected systems to an operationally ready state
- Confirm that the affected systems are functioning normally

4.4 Post-Incident Review

To improve the Incident Response processes and identify recurring issues each Incident should be reviewed and formally reported on. The report should include:

- Information about the Incident type
- A description of how the Incident was discovered
- Information about the systems that were affected
- Information about who was responsible for the system and its data
- A description of what caused the Incident
- A description of the response to the Incident and whether it was effective
- A timeline of events, from detection to Incident closure
- Recommendations to prevent future Incidents
- A discussion of lessons learned that will improve future responses

4.5 Incident Response Team

Highest Ranking Administrative Official	Richard Brook – Administrator (609) 499-2525
Chief of Police	Chief Brian Boldizar (609) 267-8300 X 130
Incident Response Manager	Richard Brook – Administrator (609) 499-2525
JIF Claims Administrator	Joe Liscandri Tel: (609) 601-3191
BURLCO JIF Technology Risk Services Director	Lou Romero Tel: (732) 690-4057
XL Catlin Data Breach Hotline 24/7	Tel: (855) 566-4724
JIF Risk Management Consultant	No RMC Designated

4.6 Incident Response Notification Information

Please verify with your breach advisor/counsel that their firm will be handling the required breach notifications including, but potentially not limited to, those agencies listed below.

IC3	FBI Internet Crime Complaint Center: https://www.ic3.gov/
NJ Cybersecurity and Communications Integration Cell (NJCCIC)	Incident Reporting: https://www.cyber.nj.gov/report 609-963-6900 x7865

5. Periodic Review

This policy and associated subordinate procedures will be reviewed at least annually by the Incident Response Manager to adjust processes considering new risks and security best practices. Material

changes in this policy should be approved by the highest ranking administrative official and/or governing body of the municipality.

6. Special Situations/Exceptions

Any personally owned devices, such as PDAs, phones, wireless devices, or other electronic devices which have been used to access organizational data and are determined to be relevant to an Incident, may be subject to retention until the Incident has been eradicated.

7. Related Information

Municipal Excess Liability Fund's Minimum Technology Proficiency Standards

8. Definitions Related to Cyber Liability Insurance

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
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

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, Trojan horses, spyware, adware, zero-day attack, hacker attack, or denial of service attack.

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.

Other cyber security incidents 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