RESOLUTION NO. 19-118

RESOLUTION OF THE CITY COUNCIL OF THE CITY OF WOODBURY 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 City of Woodbury is a member of the Gloucester, Salem and Cumberland Counties Municipal Joint Insurance Fund (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 City of Woodbury enjoys cyber liability insurance coverage to protect the City of Woodbury 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 City of Woodbury; and

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

NOW THEREFORE BE IT RESOLVED, that the City of Woodbury 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

ADOPTED at a regular meeting of the Mayor and City Council of the City of Woodbury held on July 9, 2019.

CITY OF WOODBURY

By: **TRACEY PARKER**

President of Council

ATTEST:

DANEEN D. FUSS, City Clerk

Council Member	Ayes	Nays	Abstain	Absent
Councilwoman Carter	✓			
Councilman Fleming	✓			
Councilman Hagerty	✓			
Councilman Johnson	✓			
Councilman McIlvaine	✓			
Councilwoman Miller	✓			
Councilwoman O'Connor	✓			
Councilwoman Tierney	✓			
Council President Parker	✓			
Mayor Floyd				

CERTIFICATION

I, Daneen D. Fuss hereby certify that the foregoing Resolution was adopted by the City Council, of the City of Woodbury, in the County of Gloucester and State of New Jersey at a meeting held on **July 9, 2019** at the Municipal Building, 33 Delaware Street, Woodbury, New Jersey 08096.

Daneen D. Fuss
City Clerk

Res 18

Gloucester, Salem, Cumberland Counties Municipal Joint Insurance Fund

Established in 1991

South Jersey Communities Securing Their Future

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

Document Management

Document Owner:	**City of Woodbury**
Document Name:	Information Security/Technology Practices Policy for Tier 1 Compliance
Version No:	Version: 1.0
Adoption Date:	July 9, 2019
Distribution Date:	July 10, 2019
Author (Source):	TRICO JIF; Reviewed by Robert Law, Fund Commissioner 7/2/19
Last Review Date:	07/1/19
Next Review Date:	07/1/20
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 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 from our servers using Barracuda software on a daily basis. The data is cross-stored at City Hall and the Department of Public Works. We maintain 14 versions (or days) of this data.
    a. We perform a full backup weekly and an incremental backup daily.
- We achieve the "off-network" requirement by storing the data in at the City Hall server for Public Works, and at Public Works server for City Hall.
- 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 the City Hall server.
    a. Edmunds & Associates
    b. Paychex Payroll software

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:

- 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 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 VIPRE antivirus and Fortinet Firewall which provides antivirus, firewall, and anti-malware capabilities.
- All mail servers are protected by VIPRE antivirus and Fortinet Firewall which provides anti-spam, and antivirus capabilities.
- All servers that are reachable from the Internet are protected by a VIPRE antivirus and Fortinet Firewall. Only those ports required to be reachable are reachable from the Internet.
- All servers are protected by VIPRE antivirus and Fortinet Firewall 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 ensuring that 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

Gloucester, Salem, Cumberland Counties Municipal Joint Insurance Fund

Established in 1991

South Jersey Communities Securing Their Future

Cyber Incident Response Plan

Document Management

Document Owner:	**Member Municipality**
Document Name:	Cyber Incident Response Plan
Version No:	Version: 1.0
Adoption Date:	July 9, 2019
Distribution Date:	July 10, 2019
Author (Source)	TRICO JIF; Reviewed by Robert Law, Fund Commissioner 7/2/19
Last Review Date:	7/1/19
Next Review Date:	7/1/20
Data Classification:	**Sensitive**

Table of Contents

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

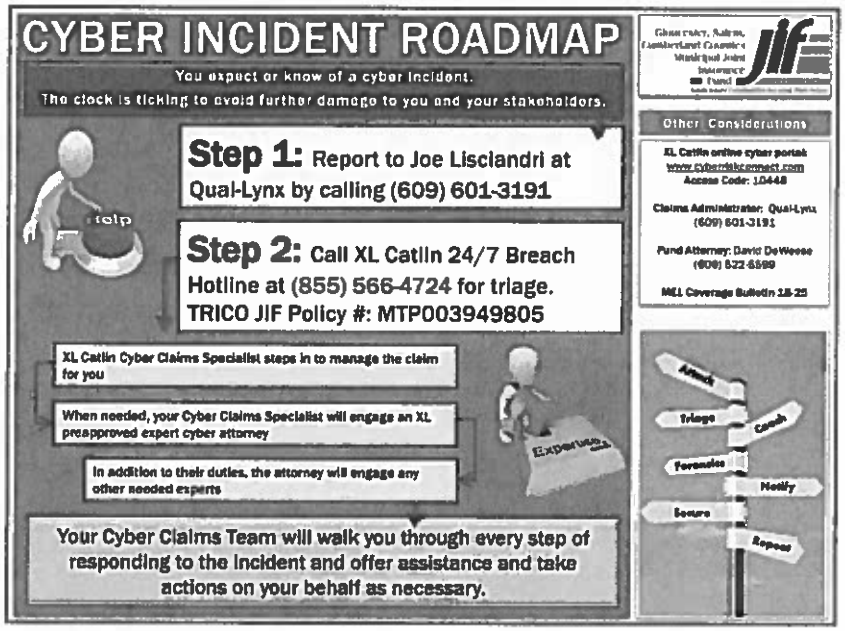
- The municipality has designated an Incident Response Manager that is responsible for determining whether an event, or a series of security events, is declared an Incident.
- The Incident Response Manager is responsible for ensuring that this policy is followed.
- The Incident Response Manager is responsible 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	Franklin Brown, City Administrator Tel: 856-845-1300 x120
Chief of Police	Thomas R. Ryan, Chief of Police Tel: 856-845-0065
Incident Response Manager	Robert Law, Fund Commissioner Tel: 609-352-5853
JIF Claims Administrator	Name: Joe Liscandri Tel: 609-601-3191
TRICO JIF Technology Risk Services Director	Name: Lou Romero Tel: 732-690-4057
XL Catlin Data Breach Hotline 24/7	 Tel: 855-566-4724
JIF Risk Management Consultant	Christopher J. Powell, Hardenbergh Insurance Group Tel: 856-890-7106

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