

Cyber Incident Response Plan

## Document Management

|  |  |
| --- | --- |
| Document Owner: | **Member Municipality** |
| Document Name: | Cyber Incident Response Plan |
| Version No: | Version: 1.0 |
| Adoption Date: |  |
| Distribution Date: |  |
| Author (Source) |  |
| Last Review Date: | 6/1/19 |
| Next Review Date: | 6/1/20 |
| Data Classification: | **Sensitive** |

Table of Contents

[Document Management 2](#_Toc10796931)

[1. Policy Statement 4](#_Toc10796932)

[2. Reason for the Policy 4](#_Toc10796933)

[3. Scope 4](#_Toc10796934)

[3.1 Designation of an Incident Response Manager 4](#_Toc10796935)

[3.2 Responsibilities 4](#_Toc10796936)

[4. Incident Response Phases 5](#_Toc10796937)

[4.1 Detection, Reporting, & Analysis 5](#_Toc10796938)

[4.2 Forensics 6](#_Toc10796939)

[4.3 Containment, Eradication, & Recovery 6](#_Toc10796940)

[4.4 Post-Incident Review 7](#_Toc10796941)

[4.5 Incident Response Team 7](#_Toc10796942)

[4.6 Incident Response Notification Information 7](#_Toc10796943)

[5. Periodic Review 7](#_Toc10796944)

[6. Special Situations/Exceptions 8](#_Toc10796945)

[7. Related Information 8](#_Toc10796946)

[8. Definitions Related to Cyber Liability Insurance 8](#_Toc10796947)

# Policy Statement

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

# 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**.](https://burlcojif.org/wp-content/uploads/2017/12/MEL-Cyber-Risk-Management-Program-Standards-to-Qualify.pdf)

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

# 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.

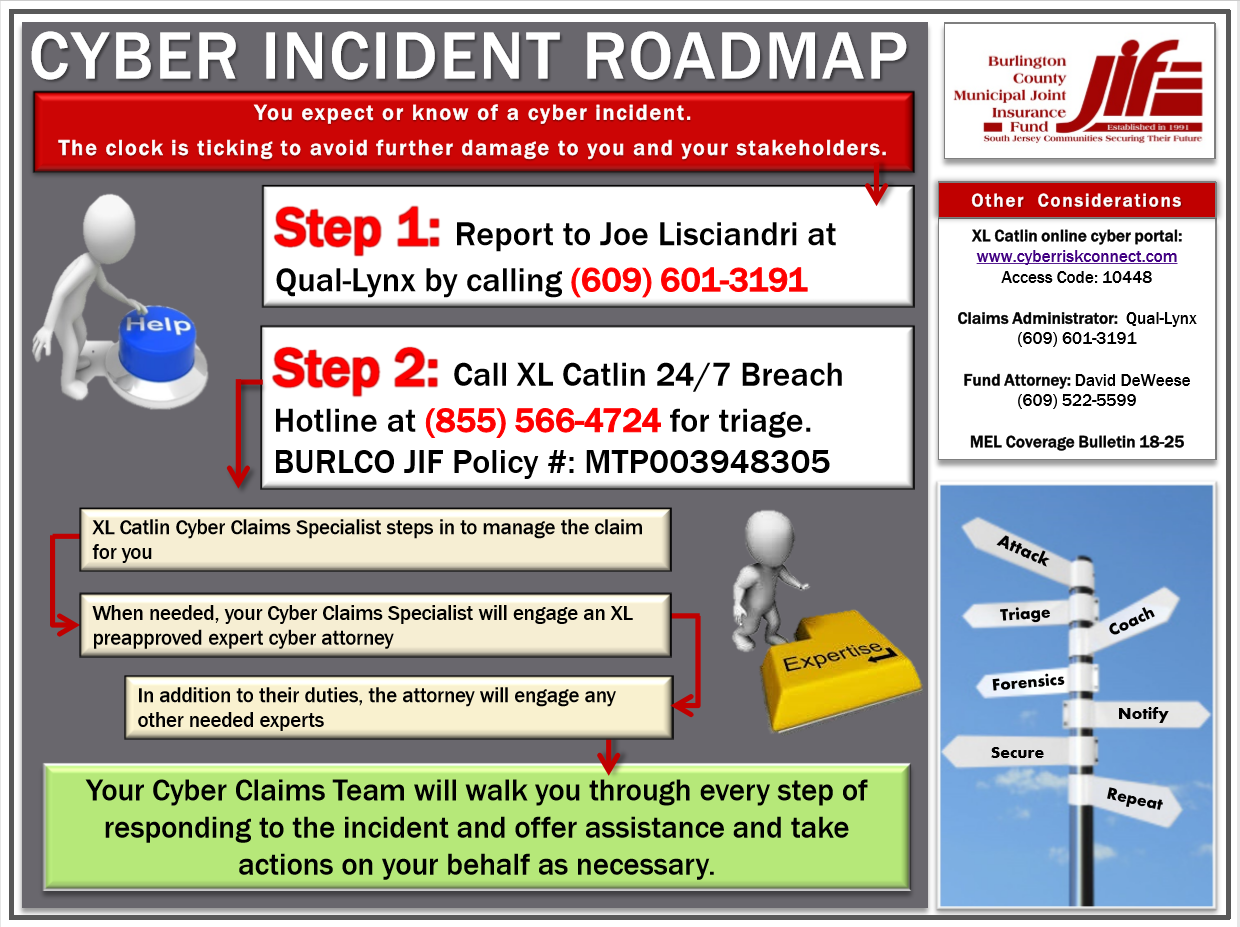
## 3.2 Responsibilities

* 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.

# Incident Response Phases

## 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.**

1. *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.
2. 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.

## 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.

## 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

## 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

## Incident Response Team

|  |  |
| --- | --- |
| Highest Ranking Administrative Official | Name  Tel: XXX-XXX-XXXX |
| Chief of Police | Name  Tel: XXX-XXX-XXXX |
| Incident Response Manager | Name  Tel: XXX-XXX-XXXX |
| JIF Claims Administrator | Name: Joe Liscandri  Tel: 609-601-3191 |
| BURLCO 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 | Name  Tel: XXX-XXX-XXXX |

## 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>   * + 1. 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.

# 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.

# Related Information

[**Municipal Excess Liability Fund’s Minimum Technology Proficiency Standards**](https://burlcojif.org/wp-content/uploads/2017/12/MEL-Cyber-Risk-Management-Program-Standards-to-Qualify.pdf)

# 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