Cyber Incident Response Plan
for the
[city or town] of [name of municipality]

[Date]

**PURPOSE**

This ***Cyber Incident Response Plan*** (“the Plan”) outlines the procedures that the [TOWN or CITY] of [NAME OF MUNICIPALITY] (“Municipality”) uses to detect and respond to unauthorized access or disclosure of private information from systems utilized, housed, maintained or serviced by [NAME OF MUNICIPALITY]. More specifically, this plan defines the roles and responsibilities of various staff with respect to the preparation, detection and analysis, containment, eradication and discovery and any post-incident activity.

[NAME OF MUNICIPALITY] seeks to prevent unauthorized access, use or disclosure of personal information (“PI”) electronically or otherwise, and to maintain privacy and security measures to protect the confidentiality of PI. “PI” is defined by applicable state law(s). [NAME OF MUNICIPALITY] has implemented reasonable and appropriate safeguards to protect the confidentiality, security and privacy of PI in its possession.

The Plan establishes the creation of the Cyber Incident Response Team (the “Team”), defines what constitutes a security incident or data breach, identifies areas of responsibility, and establishes documentation and assessment procedures.

**PREPARATION: THE INCIDENT RESPONSE TEAM**

Incident Response Coordinator or Chief Privacy Officer:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Technology Coordinator or Chief Security Officer:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Additional Technology Staff:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Communications Coordinator:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Internal Audit Coordinator:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Legal Counsel/Outside Legal Counsel:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Chief Financial Officer:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Human Resources:

|  |  |
| --- | --- |
| **Name** | **Email** |
| **Work Phone** | **Mobile Phone** |

Email list of the Entire Team with alternate email addresses:

|  |  |  |
| --- | --- | --- |
| **Name:** | **Primary Email:**  | **Secondary Email:**  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

List of Vendors, third parties and their contact information to aid in the notification requirements in accordance with state law(s):

|  |  |  |
| --- | --- | --- |
| **Vendor Name:** | **Email:**  | **Telephone:**  |
| Forensic Vendor |  |  |
| Outside Legal Counsel |  |  |
| Cyber Liability Insurance Broker and Insurance Company Contact Information |  |  |
| Credit monitoring/call center/identity theft mitigation services vendors |  |  |
| Law Enforcement Officials |  |  |
| Other Municipal Officials |  |  |
| Regulatory Officials  |  |  |

**DETECTION & ANALYSIS:**

During a Security Incident investigation, the Team will gather information from multiple computer systems and conduct interviews with key personnel based on the scope of the incident in question. All information gathered or discovered during a Security Incident will be strictly confidential throughout the investigative process. All members of the Cyber Incident Response Team agree to maintain this confidentiality throughout the process.

***Security Incident Definition***

There are many types of security incidents that may require activation of this Plan and participation by the Incident Response Team; however, some security incidents may be dealt with by IT personnel without further escalation. LOW risk level incidents typically can be carried out by appropriate IT personnel. HIGH risk level incidents typically require further escalation and the input of the Incident Response Team.

## LOW Risk Level Incidents

* Failed or failing equipment.
* Port scans.
* Virus outbreaks.
* Physical damage to IT assets (computers, printers, etc.).
* Spyware software found on desktop or laptop computers.
* Attempts at unauthorized access.
* Forwarding rules implemented by staff.
* Invalid logon attempts.

## Risk rating LOW incidents will be handled based on the information obtained during the analysis phase. Steps that may be taken will be determined based on the facts and usually can be handled by the Technology Coordinator. The Technology Coordinator should escalate any issues that arise to the full Incident Response Team.

## HIGH Risk Level Incidents

* Loss of information confidentiality—either paper or electronic (data theft).
* Compromise of data integrity (damage to data or unauthorized modification).
* Intrusion detection alarms.
* Loss or theft of IT assets or paper information (computers, storage media, removable media, mobile phones, USBs or paper records).
* Physical damage to IT assets (servers, routers, or other equipment in locked facilities).
* System compromise (system vulnerability exploits, defacing, denial of service, etc.).
* Unauthorized changes to system hardware or software.
* Unauthorized installation of software that could be used to exploit or circumvent security.
* Unauthorized access, use or disclosure of data.

## Most risk rating HIGH incidents should include involvement of the Cyber Incident Response Team. The analysis phase will help determine the next immediate course of action.

**CONTAINMENT, ERADICATION & DISCOVERY:**

***Investigation and Notification***

## If a system intrusion has occurred where data might have been compromised, the Team should determine:

* What are the symptoms?
* What may be the cause?
* What systems have been / are being / will be impacted?
* How wide spread is it?
* Which stakeholders are affected?

## The Team must document the Incident including information such as:

* Who reported the incident
* What are the characteristics of the activity
* Date and time the potential incident was detected
* Nature of the incident (Unauthorized access, DDoS, Malicious Code, Malware or Ransomware, Phishing Incident, No Incident Occurred, etc.)
* Potential scope of impact
* Whether the Team is required to perform incident remediation and the remediation to be employed

## Steps beyond these initial procedures will depend on the severity of the incident. Common steps for many incidents include:

* Disconnect the affected system(s).
* Change passwords.
* Block some ports or connections from some IP addresses.
* Disable services or applications being exploited.
* Implement multi-factor authentication.
* Implement remote monitoring services.
* User Awareness and Education.

## Once the incident has been contained, the Technology Coordinator should communicate to the Cyber Incident Response Team the following information:

* + - The extent of the damage (if any);
		- The current status of the incident;
		- Which systems are affected;
		- Affected systems - Have they already, or can they be patched, hardened or reconfigured to prevent re-infection or re-exploitation?
		- The expected time of resolution (if known).

Confirmed breaches of the security or privacy of PI will invoke certain actions to determine whether the PI has been compromised according to applicable state law(s), and whether, under those state law(s), notification of the breach will be made to the affected individual(s) and/or regulatory authorities.

When a security incident has been reported that may involve the unauthorized access, use or disclosure of PI, an investigation will be conducted under the supervision of legal counsel. The Cyber Incident Response Team and legal counsel will determine whether outside vendors are appropriate or necessary to assist in the investigation. The Cyber Incident Response Team and legal counsel will coordinate notifying any applicable insurance broker/company regarding the incident and obtaining approval for the use of any approved vendors.

* The investigation and steps taken will be thoroughly documented. If at the conclusion of the investigation it is determined that no unauthorized access, use or disclosure of PI occurred, no further action is necessary, but the investigation and conclusion will be thoroughly documented.
* If it is confirmed that a breach of security or confidentiality has occurred and has resulted in the unauthorized access, use or disclosure of PI, legal counsel will assess applicable state breach notification law(s) to determine if the incident falls within the definition of a reportable data breach. The investigation and assessment will be documented thoroughly, including the actions taken, the conclusions of the assessment and the basis for the determination that there was or was not a breach of PI in accordance with the applicable state law(s).
* If it is determined that the PI was breached, and notification is required, an analysis of the requirements for notification of the state(s) in which the affected individual(s) reside will be conducted and documented.
* If notification to law enforcement or another regulatory body or agency is required under state law(s), such notification will be made to the regulatory body or agency in accordance with state law(s).
* If state law(s) requires notification to the individual(s), notification will be made in accordance with state law(s). The notification will include any information required by applicable state law(s).
* The Cyber Incident Response Team, in coordination with legal counsel, will determine whether information about the incident will be provided to any other state or federal governmental entities on a case by case basis.

***Restoration***

After the prevention procedures are completed, the Technology Coordinator and/or Chief Security Officer should work toward bringing the system(s) affected back to functional state. Care should be taken to preserve any evidence of an intruder by backing up logs or the entire system(s) affected. If the incident did not involve the Municipality’s electronic systems, the Team should utilize appropriate physical safeguards and/or take appropriate action related to the third-party’s acts or omissions related to the incident.

***Documentation***

The Technology Coordinator should collate all technical documentation (logs, system events, exploit descriptions and other information) regarding the incident, the effects of the incident and any damage incurred from the incident, preservation of all evidence and the steps taken to restore functionality. This documentation should be given to the Cyber Incident Response Coordinator. The Cyber Incident Response Coordinator should document any processes and procedures, and investigative notes, regarding all other security incidents not involving electronic data.

Under the supervision of legal counsel, the Incident Response Coordinator should prepare a written summary of the incident and corrective action taken steps taken to restore functionality. When finalized, a copy of this documentation should be included with the documentation obtained during the final assessment of the incident. As applicable, the Incident Response Coordinator will maintain copies of all notifications sent to individual(s) and/or regulatory bodies and/or agencies.

The Communications Coordinator should obtain a copy of the final assessment of the incident from the Incident Response Coordinator. The final assessment documentation should comprise the written summary of the incident from the Incident Response Coordinator, and, as applicable, the technical documentation, data files and other literature from the Technology Coordinator.

As applicable, the Communications Coordinator is responsible for all communications during an incident and retaining such documentation as part of the incident response file.

**POST-INCIDENT ACTIVITY**

***Responsibilities of the Team – Post Incident:***

* Assess damage and cost; assess the damage and estimate both the damage cost and the cost of the containment efforts;
* Review response and update policies, procedures and guidelines; plan and take preventative steps so the intrusion will not recur;
* Consider implementation of additional staff education, as applicable;
* Consider whether a procedure or policy was not followed which may have led to the intrusion;
* Was the incident response appropriate? How could it be improved?
* Was every appropriate party informed in a timely manner?
* Were the incident response procedures followed? How can they be improved?
* Are all systems patched, systems locked down, passwords changed, anti-virus updated, and appropriate procedures, guidelines and policies in place, etc.?
* Have changes been made to prevent a new and similar incident?
* Should any security measures be changed or updated?
* What lessons have been learned from this experience?

***Maintenance and Going Forward***

* Determine who in the organization has responsibility for maintaining the Plan;
* Make sure the Plan is distributed as appropriate, within the organization;
* Review Plan at least annually;
* Review security measures and technology annually;
* Conduct tabletop exercises at least annually;
* Conduct regular staff and employee education and training in privacy and security;
* Provide regular updates and recommendations to appropriate Municipal governance personnel on security risks, recommended mitigation measures, budgeting requests and education.