Cybersecurity Incident Response Plan (IRP)

Document Details

Document Title	**Cybersecurity Incident Response Plan**
Document Type	
Document ID	
Classification	Internal
Distribution	All
Effective Date	

Version Control

Version	Date	Author	Description
1.0	5/18/2023	Telecommunications Council	Original Document

1 Introduction

1.1 Policy Statement

The Information Security Incident Response Policy outlines the overall plan for responding to information security incidents at the Office of the City of Franklin. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. Moreover, it delineates roles within the Cyber Security Incident Response Team (CSIRT) and outlines which members of the organization should if feasible be involved in different types of security incidents. The Director of Technology is charged with executing this incident response plan.

1.2 Policy Revision

The Director of Technology and his/her designees are responsible for the maintenance and revision of this document. This policy shall be reviewed annually and approved by the Director of Technology.

1.3 Purpose

All security incidents should if feasible be managed in an efficient and time-effective manner to ensure that the impact of an incident is contained and the consequences for the City of Franklin and its stakeholders are limited. The goal of this policy is to detect and react to information security incidents, determine the scope and risk of the incident, respond appropriately to the incident, communicate the impact to all stakeholders, and reduce the likelihood of the incident reoccurring.

1.4 Scope

The policy applies to all information assets, processes, and services operated by and within the City of Franklin networks, including all employees, temporary employees, contractual third parties, and vendors. Additionally, it covers all systems operated by the City of Franklin or contracted with a third party, regardless of the platforms used or where they are located.

1.5 Incident response Process Overview (Quick Start Guide)

This Incident Response Plan follows the six-phase Incident Response planning methodology developed by the SANS Institute and illustrated in Figure 1.

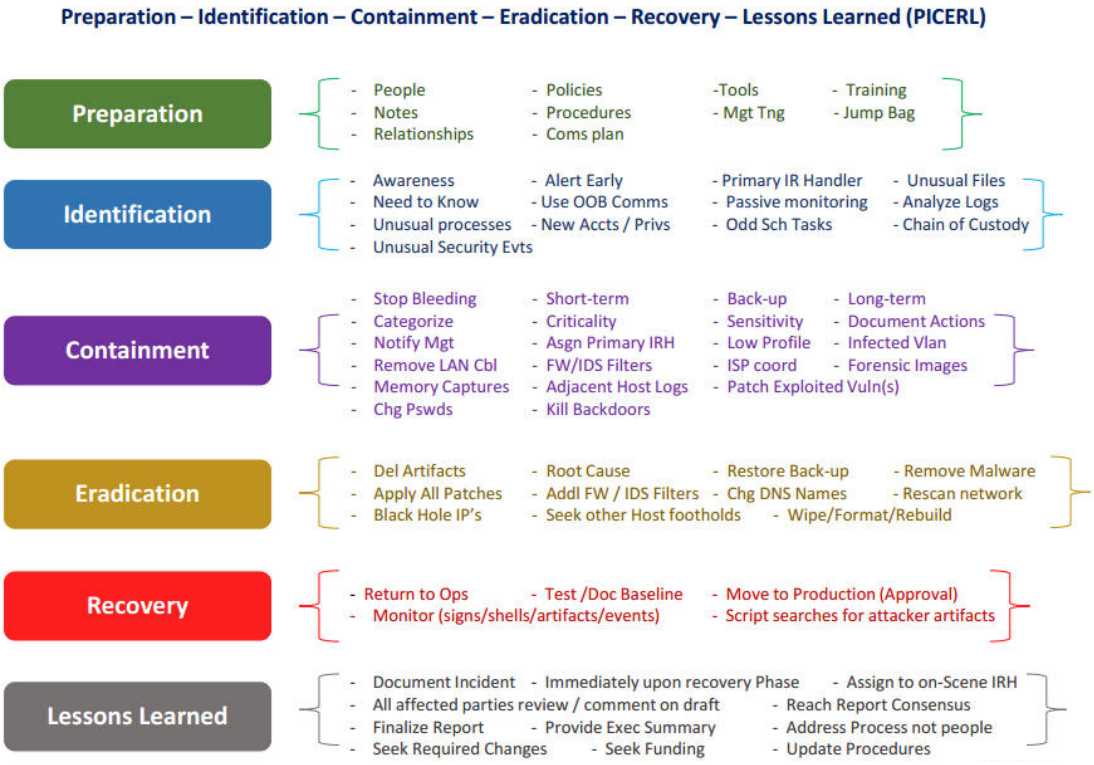

Figure 1 High Level Incident Response Process

2 Definitions

2.1 Event

An event is any observable occurrence in a system or network. Events include but are not limited to:

- A user connecting to a file share
- A server receiving a request for a web page
- A user sending email
- A firewall blocking a connection attempt.
- A user receiving an email

2.2 Event of Interest (EOI)

An Event of Interest (EOI) is an event that looks suspicious, and requires further investigation, but has not yet been classified as something of serious concern. EOIs may turn out to be inconsequential after further investigation, and no further action is required. On the other hand, EOI investigations may lead to the identification of an Adverse Event. EOI examples Include, but are not limited to:

- A user lockout
- A security system alert
- Uncharacteristic behavior of a user or system
- User receiving a suspicious email
- Multiple reports of similar unexpected events

2.3 Adverse Event

Adverse Events (AE) are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. There are generally three types of AE:

a. **Operational AE**: Operational Adverse Events are the result of a system failure or misconfiguration and do not appear to be a violation or imminent threat of a breach of computer security policies, standard security practices, system integrity or an actual or possible unauthorized release of information. Operational Adverse Events are usually referred to the Operations Team for further review and resolution. If, in the course of the Operational Team investigation, the event does not appear to meet the criteria specified above, then the results of the review are referred back to the Security Lead as a suspected security-related AE. The remainder of this document addresses only security-related AE, not those that are operational or caused by natural disasters, power failures, etc.

b. **Security AE**: Security Adverse Events are events that appear to be a violation or imminent threat of a breach of computer security policies, standard security practices, system integrity or an actual or possible unauthorized release of information. All security-related AE needs to be reported initially to the Director of Technology. Security AE may or may not constitute a security incident depending on further analysis. The Director of Technology has the authority to declare an Incident and make emergency changes or disconnections of the affected system.

c. **Insignificant AE**: Some Adverse Events have irrelevant or inconsequential implications. These AE are either thwarted by an automated process or can be handled within minutes by City of Franklin staff, and therefore may not rise to the level of needing the full execution of the IR Plan. In these scenarios, the Director of Technology chooses not to declare the AE as an Incident, and abbreviated response and reporting procedures are followed. Upon remediation, all actions are documented and presented to senior leaders for review and possible reporting by following this plan.

2.4 Security Incident

A Security Incident is an Adverse Event that has significant implications for the organization and requires the full implementation of this IR Plan. Examples of Security Incidents include, but are not limited to:

- Denial of Service
- Web Site defacement
- Widespread Malware infection
- Network Penetration
- Unauthorized access, manipulation, destruction or loss of data
- Ransomware

2.5 Executive Leadership

The term, *executive leadership,* is used throughout this document. Depending on the incident, *executive leadership* may also include the Mayor, Clerk Treasurer, Director of Technology, and City Attorney..

3 Roles & Responsibilities

To properly prepare for and address security incidents across the organization, a centralized Cybersecurity Incident Response Team (CIRT) shall be formed. This team is responsible for analyzing security breaches and taking any necessary responsive measures to minimize an adverse impact.

4 Preparation

4.1 Applicable Policies and Procedures

Incident response team members may access applicable security policies and procedures (including this IR plan) by downloading.

Additionally, the Director of Technology is responsible for maintaining current hard copies and offline copies of these policies to access during an incident (if the primary storage location is not accessible).

4.2 Communications Plan

Communications within and outside the team occur every day, but in the middle of an incident, conventional means of communicating may not be advisable or possible. For this reason, the City of Franklin has designated primary and alternate communications systems to be used during an Incident. Confidentiality is paramount during an Incident response, so the team should if feasible avoid communications methods that may not be secure and have not been included in the playbook

4.2.1 Designated Communication Platforms

During an incident, City of Franklin team members should if feasible use designated official communication platforms to securely communicate during an incident. Designated official communication platforms are identified in the playbook.

4.2.2 Notification of Affected City of Franklin Personnel

During an incident, City of Franklin employees may experience service disruptions or adverse impacts. In some instances, it may be necessary to notify City of Franklin employees about issues such as service disruptions, threat awareness, precautionary advice, or potential employee data leakage. In such cases, the Director of Technology is authorized to immediately establish contact with City of Franklin employees if it is necessary to facilitate immediate containment or mitigation actions.

4.2.3 External Incident Communications

All incident-related communications with external parties (e.g., press, suppliers, law enforcement, users) should if feasible be coordinated through and authorized by the Director of Technology in coordination with legal counsel, executive leadership, and Communications.

4.3 Secure Incident Response Workspaces

During an Incident that occurs during daily work hours, the incident response team may need a safe location or additional space to work the Incident other than their regular offices. If standard workspaces do not provide adequate privacy or security, the Director of Technology may need to repurpose conference rooms or private offices as needed to support incident response activities. This should if feasible be performed only at the direction of the Director of Technology.

4.4 Incident Response Evidence Storage and Collection

Although the primary reason for gathering evidence during an incident is to analyze and resolve the incident, digital evidence may also be needed for legal proceedings. Therefore, it is essential to document how all evidence, including compromised systems, has been preserved. The City of Franklin is likely to utilize a third-party service to assist in the collection and preservation of digital evidence on severe incidents. However, in some instances, the City of Franklin may need to gather evidence and securely store it before providing it to law enforcement or third-party forensics services.

To ensure the integrity of digital evidence the following procedures should if feasible be followed if the incident is likely to result in legal or regulatory proceedings:

- The Incident Manager should if feasible take custody of relevant physical items such as workstations, laptops, tablets, or mobile phones involved in the incident.
- The Incident Manager should if feasible use Chain of Custody and Final Disposal Action forms to provide details about the devices and document the chain of custody.

- The devices should if feasible be stored in a restricted area with strong physical controls that prevent unrestricted access to the stored evidence.

5 Identification

5.1 Initial Reporting Channels

Table 5 lists the contact mechanisms available for initial incident reports.

Table 5 Initial Incident Reporting Mechanisms

Reporting Mechanism	Description	Availability	Communication
IT Support	User support for IT Issues	24/7	Email or direct phone call, text

5.2 Event Analysis

The Incident Response Handler doing the analysis will follow a disciplined approach to gather and analyze the data to provide the Director of Technology with the best information possible to make an Incident determination.

5.2.1 Event Analysis Guidance

Specific guidance for event analysis may be provided per incident type in future City of Franklin incident response playbooks. Event analysis guidance in playbooks will include, where applicable, criteria for determining if an Event of Interest should if feasible be considered a security incident.

5.3 Incident Classification

5.3.1 Criticality

The criticality of impacted Systems/Services and Users/Accounts should if feasible be categorized according to the categories defined in Table 6.

- **System/Service criticality** will have a direct bearing on the extent of damage that could be caused by an adverse event. If multiple systems are affected, it is crucial to prioritize the critical systems over those that are not as critical.
- **User Criticality** also plays a part in prioritizing response efforts. Events affecting customers, executives, or key functional personnel in the City of Franklin should if feasible typically be prioritized over those affecting only standard users.

Table 6 Systems and Service Criticality

Systems and Service Criticality	Definition
Mission Critical	Systems or services that will result in near-immediate detrimental losses to the City of Franklin's critical operations and missions.
Business Critical	Systems or services that are heavily relied upon for daily tasks, reports, or services, but can sustain slight downtime without a major impact on the City of Franklin's operations and mission.
Business Essential	Systems or services that are essential to the operation of the business, such as payroll or human resources
Non-Essential	Systems or services that can be down for an extended period without having a large impact on the business, such as a single user endpoint, development systems, or quality assurance systems.

5.3.2 Impacts

Each incident should if feasible be classified according to its corresponding Functional/Business Impact and its Information Impact according to the categories defined in Table 7 and Table 8.

- **Functional Impact**: Adverse events targeting IT systems typically impact the business functionality that those systems provide, resulting in some negative impact on the users of those systems. Analysis should if feasible consider how the event will impact the existing functionality of the affected systems. They should if feasible consider not only the current functional impact of the incident but also the likely future operational impact of the incident if it is not immediately contained.
- **Information Impact**: Adverse events targeting data may affect the confidentiality, integrity, and availability of the organization's critical or sensitive information. For example, a Director of Technology agent may exfiltrate confidential information. Analysis should if feasible consider how this information exfiltration will impact the City of Franklin's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data is about a partner organization.

Table 7 Functional Business Impacts

Functional / Business Impact	Definition
High	The organization is no longer able to provide some critical services to any users
Medium	The organization has lost the ability to provide a critical service to a subset of system users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Informational	No effect on the organization's ability to provide all services to all users

Table 8 Information Impacts

Information Impact	Definition
Confidentiality Loss - Proprietary / Business Confidential	Sensitive proprietary or confidential information was accessed and possibly exfiltrated
Confidentiality Loss - Personal Data	Sensitive personally identifiable information (PII) or personal health information (PHI) of employees, customers, business partners, etc. was accessed and possibly exfiltrated
Integrity Loss	Company Information has been accessed and manipulated possibly affecting the *Integrity* of the data
Availability Loss	Company Information has been encrypted, destroyed, or otherwise made *unavailable* (i.e., Denial of Service, System Outage, etc.)
Informational	Failed Attempt or No apparent loss of Confidentiality, Integrity, or Availability

5.3.3 Recoverability

Each incident should if feasible be categorized according to the estimated effort required to recover from the incident according to the categories defined in Table 9. If it is not possible to estimate recovery effort during the Identification phase, then *Unknown* should if feasible be selected, and the Director of Technology or Incident Manager should if feasible ensure that the Recoverability category is updated when it is possible to provide a recoverability estimate.

The size of the event and the type of resources it affects will determine the amount of time and resources that should if feasible be spent on recovering from it. In some instances, it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. The analyst should if feasible consider the effort necessary to recover from an incident and carefully weigh that against the value the recovery effort will create, and any requirements related to incident handling.

Table 9 Recoverability Categories

Recoverability Effort	Definition
Unknown	The effort required and Time to recover is unknown and may not be entirely possible (e.g., sensitive data exfiltrated and posted publicly)
Extended	The effort required and Time to recover is unpredictable and may be extended for a long duration; additional resources and outside help are needed
Supplemented	The effort required and Time to recover is predictable with additional resources
Regular	The effort required and Time to recover is predictable with existing resources
None	EOI Thwarted. No further effort is required.

5.4 Cybersecurity Incident Declaration

The Director of Technology reviews the analysis and determines if Events of Interest (EOI) and resulting security-related Adverse Events (AE) are significant enough to be designated as a Cybersecurity Incident.

- If the EOI is not determined to be a Cybersecurity Incident, the Director of Technology should if feasible still ensure that analysis is documented using the Event/Incident Analysis & Reporting Form at Appendix D and file it accordingly.
- If the EOI is an actual incident, the Director of Technology should if feasible immediately declare the incident, activate the CIRT, and begin notifications and adherence to the full requirements of this plan.
- The Director of Technology should if feasible work with the executive leadership and legal counsel to determine if the Cybersecurity Incident meets criteria that require notification of external parties, legal, or compliance issues.

Prioritizing the handling of the incident is a critical decision point in the incident handling process. Incidents cannot be handled on a first-come, first-served basis as a result of resource limitations. Instead, handling should if feasible be prioritized based on the relevant factors identified in the Incident Classification (see Section 5.3).

5.5 Incident Response Team Formation

Once an incident is declared, the Director of Technology activates the CIRT and designates other Technical Leads as needed. The Director of Technology will also appoint an Incident Scribe to manage documentation and notes throughout the incident.

5.6 Informal Reporting to Executives and Senior Leaders

Informal reporting to executive leadership should if feasible happen as soon as possible after Incident Declaration; this does not mean that further investigating and containment should if feasible wait until the initial report is done.

5.7 Confidentiality

Confidentiality should if feasible be stressed during any formal incident investigation. Depending on the sensitivity of the incident or the data involved, the discussions of the incident may have to be significantly restricted to just a couple of key individuals, and not the entire team. Any communication related to an incident should if feasible be provided only to the appropriate parties involved. Specifically, individuals should if feasible not be added or removed from the original email associated with the incident. When replying to an email about an incident, ensure that the "reply all" function is selected so that all of the original recipients receive all of the communications related to the incident. If a member of the original recipient's group would like to add or remove members from the email communications, they should if feasible first discuss that with the Director of Technology.

6 Containment

6.1 Containment Authority

During the Containment Phase, the Director of Technology has authority to make decisions to isolate or disconnect an impacted/offending device or system from the network to contain it.

6.2 Containment Strategies and Playbooks

Containment strategies vary based on the type of incident. For example, the plan for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. For this reason, the City of Franklin may maintain separate playbooks to address containment and eradication strategies for major incident types, with criteria documented clearly to facilitate decision-making.

6.3 Evidence Preservation

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. Therefore, it is essential to document how all evidence, including compromised systems, have been preserved. City of Franklin does not have in-house expertise to independently perform digital forensics, and incidents that require significant forensics expertise will likely be supported by a third-party.

Regardless of who performs forensics, evidence preservation requirements should if feasible be met according to the details provided in this Section.

Incident evidence will be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. Additionally, a detailed log will be kept for all evidence, including the following:

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Name, title, and phone number of each who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored

7 Eradication

7.1 Host Remediation or Replacement

After the incident has been contained, eradication will be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, all affected hosts within the organization will be identified so that they can be remediated. For some incidents, eradication may not be necessary or may be performed during recovery. Like containment, eradication strategies vary based on the type of incident.

7.2 Phased Approach

Eradication and recovery will be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; therefore, the intent of the early phases will be to increase the overall security quickly (days to weeks) to implement high-value changes that will prevent future incidents. The later phases will focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

8 Recovery

The Director of Technology will authorize a return to normal operations once the satisfactory resolution is confirmed.

The Director of Technology will notify the city that normal business operations can resume. Normal operations should if feasible adopt any updated processes, technologies, or security measures identified and implemented during incident resolution.

8.1 Restore systems to regular operations

In recovery, administrators will restore systems to regular operation, remediate any remaining vulnerabilities, confirm that the systems are functioning normally, monitor for any additional events or evidence of re-compromise, and closeout documentation and reporting requirements. Some business-critical systems may also require extensive functional testing before being returned to production.

8.2 Determining Cause

After removing all artifacts, it is necessary to identify what vulnerabilities allowed the objects to get on the system or to the data in the first place. Specifically, what controls were either ignored, bypassed, failed, or missing. These vulnerabilities should if feasible be mitigated as soon as possible to prevent reinfection. In some cases, existing security controls may need to be modified or new ones developed.

8.3 Final Incident Report

The initial investigation and Incident Report should if feasible be completed within a reasonable amount of time. The Director of Technology will establish an extended investigation timeline based on this initial report.

9 POST-INCIDENT Activities (Lessons Learned)

The goal of the Post-Incident Activity Phase is to document what went right, what went wrong, and to implement changes as needed to improve our capabilities for future incidents. Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lesson-learned meeting. This meeting provides a chance to achieve closure concerning an incident by reviewing what occurred, what was done, and how well the intervention worked.

9.1 Lessons Learned

As soon as possible after the incident closeout, the Director of Technology, executive leadership, and other selected stakeholders will hold lessons learned meeting to discuss the incident and response actions. This meeting will address areas of improvement to the CIRT, security controls, and the response procedures so that they can more effectively handle similar incidents in the future. Questions to be answered in the meeting include:

- Precisely what happened, and at what times?
- How well did staff and management perform in dealing with the Incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should if feasible be watched for in the future to detect similar incidents?

- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

9.2 Notification of Affected Personnel

The organization will provide notice to personnel and affected parties about the Incident following regulatory and legal requirements.

10 Forms

CHAIN OF CUSTODY				
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE FOR CHANGE OF CUSTODY
		NAME	NAME	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		SIGNATURE	SIGNATURE	

FINAL DISPOSAL ACTION

RELEASED TO ☐ OWNER, OR ☐ OTHER (*Name)*:

DESTROYED

OTHER DISPOSITION (*Specify)*

FINAL DISPOSAL AUTHORITY

ITEM(S) _____ ON THIS DOCUMENT, PERTAINING TO INVESTIGATION

No. _____ INVOLVING _____

(IS) (ARE) NO LONGER REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE.

_____

Printed Name, Title *Signature* *Date*

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S) _____ (WAS) (WERE) DESTROYED IN MY PRESENCE ON THE DATE INDICATED ABOVE.

_____

Printed Name, Title *Signature* *Date*