Agenda Item No. F-4

DATE SUBMITTED	12/08/2021
SUBMITTED BY	R. Alejandro Estrada
DATE ACTION REQUIRED	12/15/2021

COUNCIL ACTION	(x)
PUBLIC HEARING REQUIRED	( )
RESOLUTION	( )
ORDINANCE 1ST READING	( )
ORDINANCE 2ND READING	( )
CITY CLERK'S INITIALS	RM

IMPERIAL CITY COUNCIL
AGENDA ITEM

SUBJECT: DISCUSSION/ACTION:

1. APPROVE AND ADOPTION OF THE CITY OF IMPERIAL CYBERSECURITY INCIDENT REPONSE PLAN POLICY.

DEPARTMENT INVOLVED: DEPARTMENT OF INFORMATION TECHNOLOGY

BACKGROUND/SUMMARY:

The City of Imperial staff is requesting the Council's consideration in adopting the Cybersecurity Incident Response Plan Policy to continue with the City Water Treatment Plant Risk and Resilience Assessment Emergency Response Plan Certification required by the United States Environmental Protection Agency (EPA).

A Cybersecurity Incident Response Plan (CIRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication and coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, a CIRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines.

FISCAL IMPACT:

FINANCE INITIALS

STAFF RECOMMENDATION:

It is staffs recommendation to approve the Cybersecurity Incident Response Plan Policy

DEPT. INITIALS

MANAGER'S RECOMMENDATION:

The City Manager agrees with staffs recommendation.

CITY MANAGER's INITIALS

MOTION:

SECONDED:
AYES:
NAYES:
ABSENT:

APPROVED ( ) REJECTED ( )
DISAPPROVED ( ) DEFERRED ( )

REFERRED TO:

1. Overview

A Cybersecurity Incident Response Plan (CIRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an CIRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an CIRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2. Purpose

This document describes the City of Imperial's overall plan for preparing and responding to both physical and electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this CIRP is to prepare for, detect, and respond to security incidents. It provides a framework by which the Incident Response Team (IRT) shall determine the scope and risk of an incident, respond appropriately to that incident, communicate the results and risk of an incident, communicate the results and risk to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

3. Scope

This policy applies to the physical location, the information systems, and networks of the City of Imperial and any person or device that gains access to these systems or data.

4. Policy

4.1 Incident

An incident is an event that, as assessed by the staff, violates the policies of the City of Imperial as related to Information Security, Physical Security, or Acceptable use, or code of conduct; or threatens the confidentiality, integrity or availability of information systems.
Incidents can include:

- Malware/viruses/Trojans.
- Ransomware.
- Phishing.
- Unauthorized electronic access.
- Breach of information.
- Unusual, unexplained or repeated loss of connectivity.
- Unauthorized physical access.
- Loss or destruction of physical files, etc.

4.2 Preparation

Preparation includes those activities that enable the City of Imperial to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans. The City of Imperial utilizes several mechanisms to prevent, and prepare to respond to, an incident.

- Security Awareness Training.
- Malware/ Antivirus/ Spyware Protections.
- Firewall and Intrusion prevention Devices (IPD).
- Personnel Security Measures.
- Physical Security Measures.
- Event Logs.
- Patching/ Updating.

4.3 Detection

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of the Cyber Emergency Switch (CES). The determination of an incident can arise from one or several circumstances simultaneously. Means by which detection can occur include.

- Trained personnel reviewing collected event data for evidence of compromise.
- Software applications analyzing, trends, and patterns of behavior.
- Intrusion Protection/ Intrusion Detection devices alerting to unusual network or port traffic.
- The observation of suspicious or anomalous activity within City of Imperial facility or on a computer system.

It is critical in this phase:

- To detect whether a security incident has occurred or not.
- To determine the method of attack.
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
- To obtain or create intelligence products regarding attack modes and methods.

It is crucial that after activation of the CES, system operators continuously control and monitor all of the processes manually.

4.4 Analysis

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weakness in either the physical security of the facility, its monitoring tools, or its training program to assess areas for process improvement or change. For an electronic incident, Department of Information Technology (DoIT) will perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These

analyses can be performed either manually or utilizing automated tools dependent upon the situation, timelines, and availability of resources.

4.5 Reporting
In the event an incident is suspected, employees are required to immediately contact the DoIT.

4.6 Containment
DoIT is responsible for containment and will document all containment activities during an incident. Containment activities for security incidents involve decision-making and application of strategies to help control attack and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of strategy is delayed.

4.7 Eradication
DoIT is responsible for the eradication and will document all eradication activities during incident. Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

4.8 Recovery
DoIT is responsible for recovery and will document all recovery activities during incident. Recovery efforts for incidents will involve the restoration of affected systems to normal operations. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems form agency approved baseline, replacing compromised files with clean visions, installing patches, changing passwords, and increasing network perimeter and host-based security.

4.9 Post-Incident Activity
DoIT is responsible for documenting and communicating post-incident activity.
Post-incident activities will occur after the detection, analysis, containment, eradication and recovery from a security incident. One of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered documentation are:

- Exactly what happened, and at what time?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What should be done differently the next time or similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

5. Policy Compliance

5.1 Compliance Measurement

The DoIT team will verify compliance with this policy through various methods, including but not limited to, business tools reports, internal and external audits, and feedback to the policy owner. This policy should be reviewed annually.

5.2 Exceptions

Any exception to the policy must be approved by the DoIT and City Manager's Office in advance.

5.3 Non-Compliance

An employee found to have violated this policy after having been provided a copy of this policy may be subject to disciplinary action, up to and including termination of employment.

EMPLOYEE ACKNOWLEDGMENT

If you have additional questions about this policy, please contact Human Resources and/or DoIT before signing the following agreement.

I have read the City of Imperial's Cybersecurity Incident Response Plan and agree to abide by it. I understand that violation of any of the above policies may result in discipline, up to and including termination.

User Name (Printed)	User Signature	Date