Re: CT11.11

ATTACHMENT 1

Cyber Security
Incident Response Plan

January 2020

Table of Contents

The Cyber Security Incident Response Plan is used to support the organized response to security incidents. It documents the roles and responsibilities and steps that will be followed to identify, contain, eradicate, and recover from security incidents.

Steps include Identification, Containment, Eradication, Recovery, and Lessons Learned.

TO Live should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. TO Live needs a plan that meets its unique requirements, which relate to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support.

1. Purpose and Scope

Purpose

This Cyber Security Incident Response Plan exists to ensure TO Live is prepared to manage Cyber Security Incidents in an effective, efficient and organized manner. Cyber Security Incidents are more frequent and sophisticated than ever and TO Live is not immune to these incidents. TO Live must ensure they are prepared to respond to incidents as well as prevent and detect. By having a plan, a team, and conducting exercises, TO Live will be better prepared for inevitable incidents and will be able to contain and mitigate further risk to the organization.

This document describes the overall plan for responding to Cyber Security Incidents at TO Live. It identifies the structure, roles and responsibilities, types of common incidents, and the approach at identifying, containing, eradicating, recovering, and conducting lessons learned in order to minimize impact of such incidents.

The goal of the Cyber Security Incident Response Plan is to ensure TO Live is able to respond to security incidents effectively and efficiently.

Scope

This Cyber Security Incident Response Plan applies to all networks, systems, and data as well as members of the organization including employees and contractors as well as vendors that access the networks, systems, and data. Members of the organization who may be called upon to lead or participate as part of the Cyber Security Incident Response Team must familiarize themselves with this plan and be prepared to collaborate with the goal of minimizing adverse impact to the organization.

This document assists TO Live with establishing incident handling and incident response capabilities and determining the appropriate response for common security incidents that will arise. This document is not intended to provide a detailed list of all activities that should be performed in combatting security incidents.

2. Authority

Responsibility for the security of information resides with the Director of Information Technology. During times when a high or critical security incident is underway this responsibility is entrusted to the Directory of Information Technology.

3. Definitions

Event - an observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, or a user sending email.

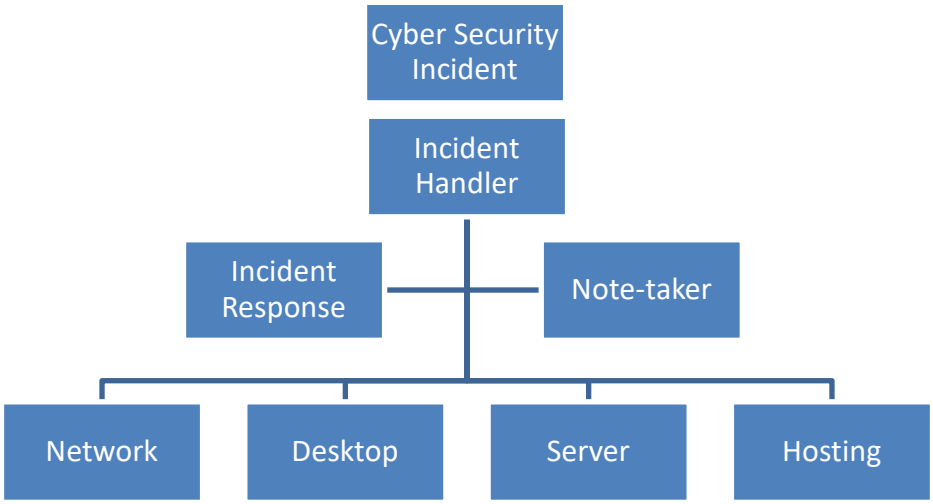
Incident - an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. An *incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It implies harm or the attempt to harm.

4. Roles & Responsibilities

Incident Handler (lead)	Support Technician
Incident Handler (backup)	Applications Analyst
Incident Response (lead)	Director of Information Technology
Incident Response(backup)	Applications Analyst
Note-taker	Archives/Records
Human Resources	Director of Human Resources
Finance & Administration	Vice President of Finance & Administration

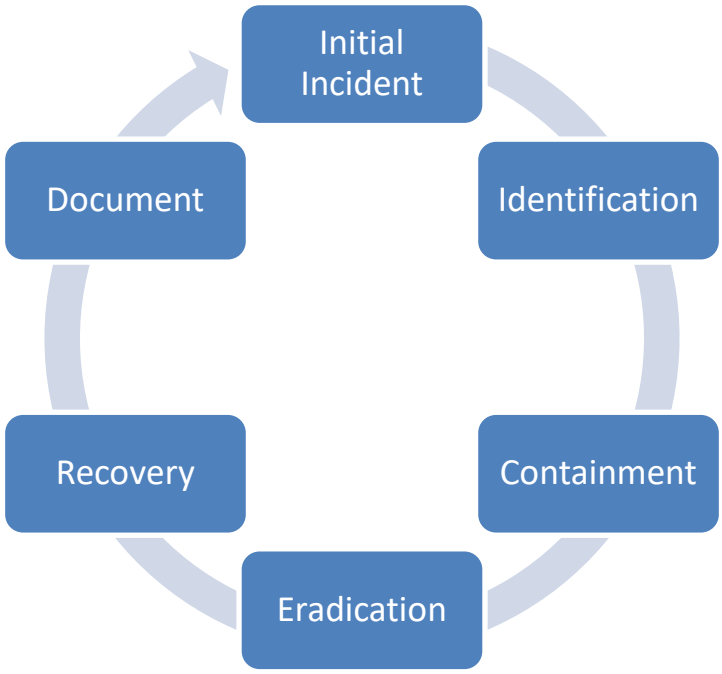
All of the roles identified above will review the Cyber Security Incident Response Plan and be delegated with the responsibility for mitigating harm to the organization.

5. Cyber Security Incidence Response Structure



6. Incident Handling Process

In the event of a Cyber Security Incident the Cyber Security Incident Response Team will adhere to the process as follows:



Preparation

- ☐ Build an incident response plan
  - o Establish mandate, delegate authority decision making process and chain of command
  - o Review/update annually
- ☐ Ensure you have an incident response team
  - o Dedicated, virtual, or on-retainer
  - o Provide training as necessary
- ☐ Document roles and responsibilities
  - o Delegate authority
  - o Provide training as necessary
- ☐ Understand the environment
  - o Diagrams, location of critical systems and data
  - o Ensure adequate visibility into networks and systems to respond to an incident
  - o Understand dependencies
- ☐ Understand what controls are in place
  - o Are they sufficient to mitigate risk to an acceptable level?

- ☐ Understand impacts
    - o Determine Maximum Tolerable Downtime (MTD) and Acceptable Interruption Window (AIW)?
    - o Prioritized list of assets and downtime
- ☐ Prepare Confidential Meeting Locations
    - o Require a location physically or logically to convene
    - o Ensure location is secure and appropriately equipped
- ☐ Establish communications plan in advance
- ☐ Establish agreements in advance
    - o Established SLA's, response times

Notification

- ☐ Ensure a central point of contact exists for employees to report real or suspected security incidents
- ☐ Ensure all employees are required to report security incidents
- ☐ Ensure all employees know they are required to report security incidents and how
- ☐ Ensure all employees do report security incidents in a timely fashion

Convene

- ☐ Bring together those who are aware of the incident
- ☐ Engage Incident Response Team members
- ☐ Remind all of responsibility to maintain need-to-know
    - o Otherwise leads to managing misinformation
- ☐ Communicate effectively and efficiently
- ☐ Convene in Meeting Location
    - o Ensure location is secure and appropriately equipped

Identification

- ☐ Determine whether an incident has occurred
    - o Is it an event or an incident?
    - o Search for correlating information to increase confidence there is a real incident
- ☐ Perform Identification and ensure common understanding of how it was detected and who is aware
- ☐ Analyze
- ☐ Perform research (eg. search engines, knowledge base)
- ☐ Document investigation and evidence gathering
- ☐ Prioritize handling of incident based on relevant factors (functional impact, information impact, recoverability effort, etc)
- ☐ Determine severity, urgency and initial impact
- ☐ Review information and actions taken to date
- ☐ Report incident to appropriate internal personnel and external organizations

Communication

- ☐ Invoke communications plan respecting need-to-know
- ☐ Develop stakeholder relationship map, to determine the level of stakeholder involvement
- ☐ Ensure reported information is factual based on evidence available at the time
- ☐ Ensure a point of contact knows the current status at all times

Containment

- ☐ Implement incident response
- ☐ Prevent further damage and problem from getting worse by containing the incident
- ☐ Determine the source, what vulnerability was exploited and patch accordingly
- ☐ Continue impact/damage assessment and confirm the scope of the incident
- ☐ Determine what was changed (eg. files, connections, processes, accounts, access)
- ☐ Acquire, preserve, secure and document evidence and preserve chain of custody
- ☐ Continue taking notes, ensuring a detailed log about what was found and what was done

Eradication

- ☐ Eradicate the incident
- ☐ Remove all traces of the infection or other incident
    - o Identify and mitigate all vulnerabilities that were exploited
    - o Remove malware, inappropriate materials, and other components
- ☐ If more affected hosts are discovered (e.g., new malware infections), ensure to perform the identification steps on the newly identified examples, then contain
- ☐ Ensure the incident cannot re-occur
- ☐ Continue taking notes, ensuring a detailed log
- ☐ Ensure any compromised machines are removed or formatted before placing back into service

Recovery

- ☐ Return affected systems to an operationally ready state one by one
- ☐ Monitor closely to ensure incident does not re-occur or is not still ongoing
- ☐ Ensure systems are restored from a trusted source
- ☐ Confirm the affected systems are functioning normally
- ☐ Implement additional monitoring to look for future related activity if necessary

Lessons Learned

- ☐ Hold lessons learned meeting within 2 weeks
- ☐ Create a follow up report

- ☐ Walk through and review play-by-play of incident report
    - o How was the incident detected, by whom, and when
    - o Scope and severity of incident
    - o Methods used in containment and eradication
- ☐ Identify opportunities for improvement to better prepare for next time
- ☐ Ensure accountability to follow up on identified opportunities

7. Incident Types

Type	Description
Unauthorized Access or Usage	Individual gains physical or logical access to network, system, or data without permission.
Service Interruption or Denial of Service	Attack that prevents access to the service or otherwise impairs normal operation
Malicious Code	Installation of malicious software (eg. virus, worm, Trojan, or other code)
Network System Failures (widespread)	An incident affecting the confidentiality, integrity, or availability of networks
Application System Failures	An incident affecting the confidentiality, integrity, or availability of applications or systems
Unauthorized Disclosure or Loss of Information	An incident affecting the confidentiality, integrity, or availability of data
Privacy Breach	Incident that involves real or suspected loss of personal information
Information Security/Data Breach	Incident that involves real or suspected loss of sensitive information
Other	Any other incident that affects networks, systems, or data

8. Severity Matrix

The Cyber Security Incident Response Team will determine the severity of the incident taking into consideration whether a single system is affected or multiple, the criticality of the system(s) affected, whether impacting a single person or multiple, whether impacting a single team or multiple, or impacting the entire organization. The Team will consider whether a single business area or multiple areas and the impact of the incident. The Incident Handler must consider the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remediation.

The Cyber Security Incident Response Team will consider the available information to determine the known magnitude of impact compared with the estimated size along with likelihood and rapidness of spread. The Cyber Security Incident Response Team will determine the potential impacts to the organization whether financial damage or brand and reputational damage or other harms.

The incident may be the result of a sophisticated or unsophisticated threat, automated or manual attack, or may be nuisance/vandalism.

The Cyber Security Incident Response Team will determine whether there is a vulnerability, whether there is an exploit, whether there is evidence of the vulnerability being exploited, and whether there is a known patch. Finally, the Team will determine if this is a new threat (eg. zero day) or a known threat and the estimated effort to contain the problem.

Category	Indicators	Scope	Action
Critical	Data loss, Malware	Widespread and/or with critical servers or data exfiltration	Incident Response Plan, create Security Incident, Organization-wide
High	Theoretical threat becomes active	Widespread and/or with critical servers or data exfiltration	Incident Response Plan, create Security Incident, Organization-wide
Medium	Email phishing or active spreading infection	Widespread	Incident Response Plan, create Security Incident, Organization-wide
Low	Malware or phishing	Individual host or person	Create Security Incident Report Short Form

Appendix 1

TO LIVE - CYBER SECURITY INCIDENT RESPONSE (**SHORT FORM**)

Contact Information and Incident

Last Name: _____ **First Name:** _____

Job Title: _____ _____

Phone: _____ **Alt Phone:** _____

Mobile: _____ **Notes:** _____

Email: _____ _____

Incident General Information

Incident #: _____ **Source of Incident:** ☐ External ☐ Internal **Type of Incident:** _____

Date/Time of Incident Occurred: _____ **Date/Time of Incident Detected:** _____

Location: _____ **Severity Level:** Low

Impact Category: _____ **Confidential/Personal Identifiable Information Affected?** ☐ Yes ☐ No

Systems and Services Impacted: _____

Incident Summary

Comments:

Incident Mitigation

Comments:

Recommendation

Comments:

Additional Comments/Notes

Comments: