NWC OT Cybersecurity Incident Response Procedure

Document Number:	A01001045-PRO-IR
Issue Date:	July 29, 2021
Revision Number:	00

Revision Details

Name	Title/Dept.	Signature	Date
Prepared by:			
Hafiz Muhammad Asad	Automation System & Security Engineer		July 06,2021
Reviewed by:			
Sameen Ullah Khan	OT Cybersecurity Lead		July 07,2021
Approved by:			
Farhan Rasheed	Operations Manager		July 07,2021

Issued by:			
Syed Ali Raza	Planning Engineer		July 29, 2021

History Page

Issue No.	Issue Date	Prepared By (Name)	Reviewed By (Name)	Owned By (Name)	Endorsed By (Name)	Approved By (Name)
Change Description						
Change Description						
Change Description						

Reference Documents

Document Number	Document Title
ECC-1:2018	National Cybersecurity Authority Essential Cybersecurity Controls (NCA ECC)

Document Roles and Responsibilities

	Prepare/ Update/ Amend	Review	Approve	Publish
Owner	YES	YES		
Cybersecurity Steering Committee		YES		YES
Corporate Strategy & Performance Management VP			YES	

Table of Contents

Glossary

Word or Phrase	Explanation
Asset	General support system, major application, resources, high impact program, physical plant, or a logically related group of systems
Asset Register	Location, condition, owner, status, procurement dates, depreciation or values of the assets
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
BU	Business Unit- Represents a specific line to the business and is a part of firm's value chain of activities including operations, accounting, HR, marketing and sales.
Central Management Console	(CMC) appliances deliver centralized edge or public cloud-based monitoring of Guardian sensors–no matter how distributed your business is.
Compliance	Ensuring that a Standard or set of Guidelines is followed. A means of conforming to a rule, such as a specification, policy, standard or law.
Firmware	Tangible computing device providing low level of controls, held in non-volatile memory devices such as ROM, EPROM, Flash memory

Word or Phrase	Explanation
Integrity	The property of safeguarding the accuracy and completeness of assets.
Network Management system	NMS, responsible for collecting, storing and presenting data
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Test Environment	A controlled Environment used to test Configuration Items, Software Builds, OT/IT Services, Processes, etc.
IR Team	Incident Response Team

1. Introduction

The role of this incident response procedure is to provide NWC staff, how to perform consistent and comprehensive incident response. This procedure provides information on how to detect, identify, contain, eradicate the incident and recover the OT system. This procedure is applicable to all NWC OT infrastructure.

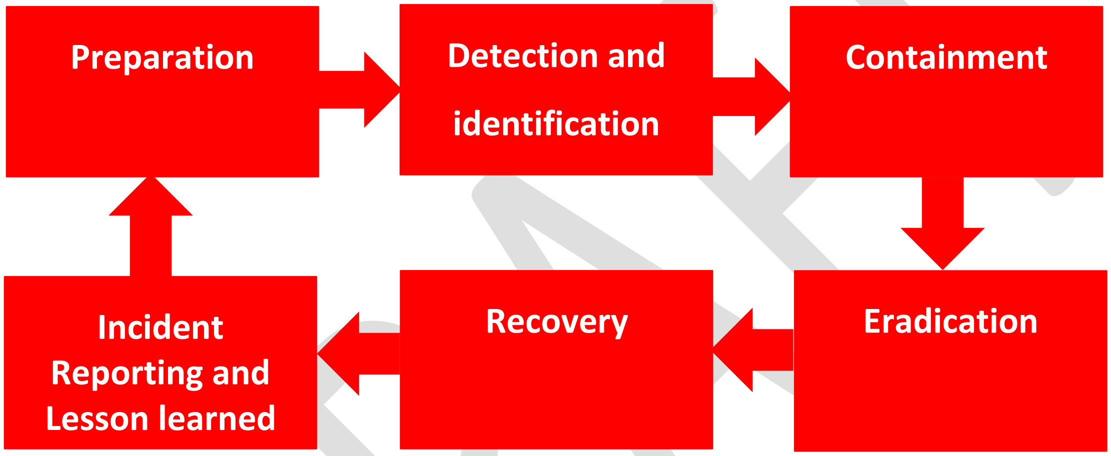
2. Roles and Responsibilities

Roles	NWC Representative	Responsibilities
Incident Reporter	Any OT Asset Owner, NWC Information Security, NWC Leadership/Management	Report the incident
NWC Information Security	Information security officer	Coordinates with Line Managers for incident detection and identification
Incident Response Team	All NWC representative who are in any way involve with OT asset and information security	Perform incident response and recovery process

3. OT Incident Response Procedure

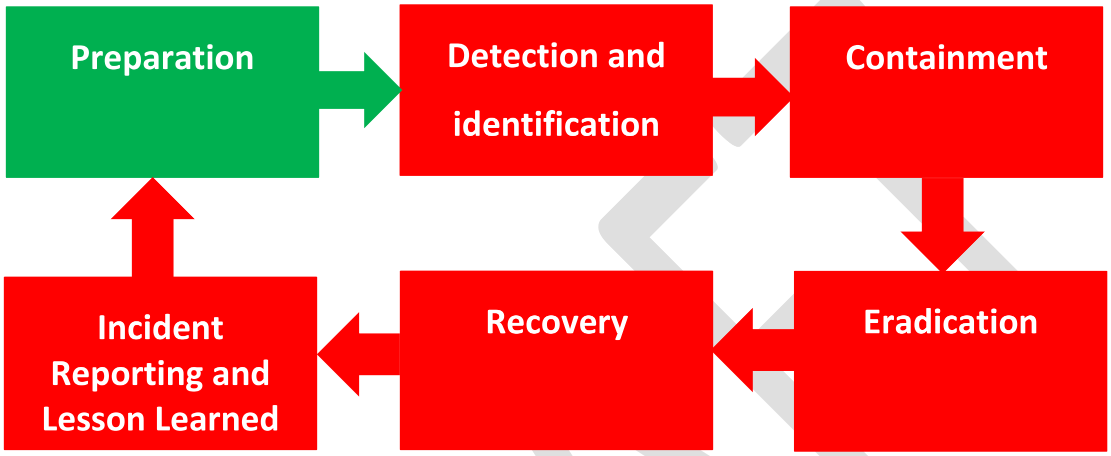
Incident response procedure requires the following steps to be identified.

1. Preparation
2. Detection and identification
3. Containment
4. Eradication
5. Recovery
6. Incident Reporting and Lesson learned


Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson learned

3.1 Preparation

Preparation is the first and most critical step of the Incident response procedure. Tasks associated with preparation should be performed prior to an incident.

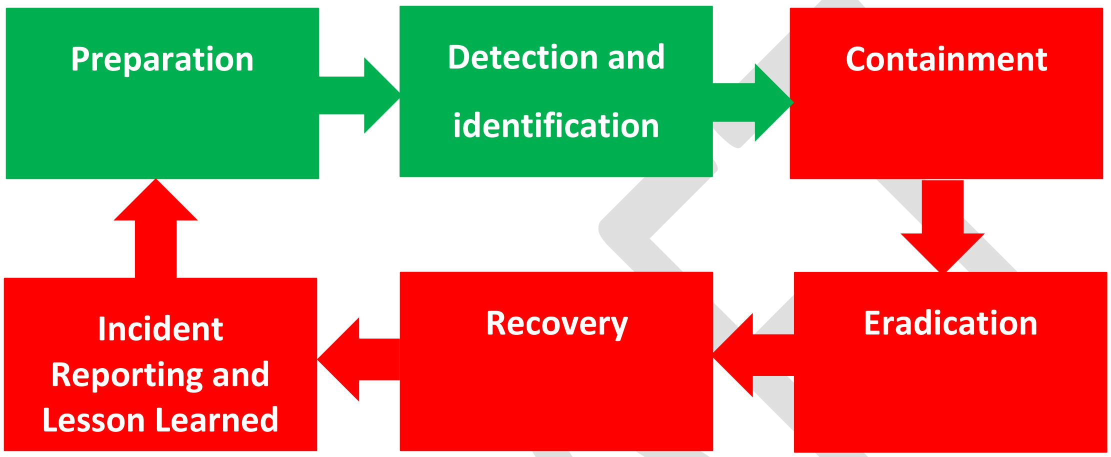

Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

Prepare Incident Plan:

- NWC Information Security Team will organize the Incident Response Teams
- Incident handling policies are created
- Building incident response plan
  1. Overview, goals and objectives
  2. Incident description
  3. Incident detection
  4. Incident notification
  5. Incident analysis
  6. Response actions
- Exercising the incident plan
- System state and status reporting and lesson learned

3.2 Detection, Identification

Detecting an incident early stage helps to limit or even prevent possible damage to the ICS and reduce downstream efforts to contain, eradicate, recover, and restore the affected systems.


Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

3.2.1 Incident Detection:

1. Detection by Observation - User observation will be used for the detection of abnormal system or component behavior. An observation will come from any member of the organization, including operators, process engineers, or system administrators.
2. Automated Detection Methods - Automated detection via applications, IDSs and antivirus programs will be used to detect and flag malware, intrusion attempts, policy violations, and exploits, as well as component failure.

Report the incident to the NWC Information Security Team and other internal and external stakeholders as needed. IR team will be formed by NWC Information Security and activated by the IR Lead to investigate the situation.

3.2.2 Incident Identification:

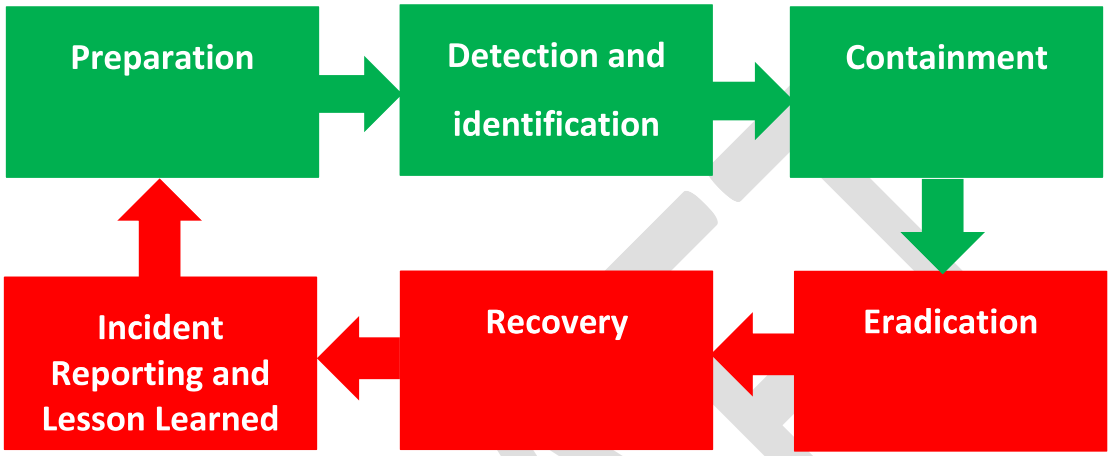
Logs from SIEM will be used in identifying threat from different sources and to investigate path vector of attack. These automated approaches still require human interaction for configuration, review, analysis and action.

The following list of symptoms will be considered as possible indicators of an attack:

- Unusually heavy network traffic
- Out of disk space or significantly reduced free disk space
- Unusually high CPU usage
- Creation of new user accounts
- Attempted or actual use of administrator-level accounts
- Locked-out accounts
- Accounts in use when the user is not at work
- Cleared log files
- Full log files with an unusually large number of events
- Antivirus or IDS alerts
- Disabled antivirus software and other security controls
- Unexpected patch changes
- Machines or intelligent field devices connecting to outside Internet Protocol (IP) addresses
- Requests for information about the system (social engineering attempts)
- Unexpected changes in configuration settings
- Unexpected system shutdown
- Unusually slow access to hosts on the network
- Filenames containing unusual characters or new or unexpected files and directories
- Auditing configuration changes logged on the host records, especially disabling of auditing functionality
- A large number of bounced e-mails with suspicious content
- Unusual deviation from typical network traffic flows
- Erratic ICS equipment behavior, especially when more than one device exhibits the same behavior
- Any apparent override of safety, backup, or failover systems
- Equipment, servers, or network traffic that has bursts of temporary high usage when the operational process itself is steady and predictable.
- Unknown or unusual traffic from corporate or other network external to control systems network
- Unknown or unexpected firmware pulls or pushes.

3.3 Containment

While performing containment, source of the incident should be isolated. Containment focuses on preventing the spread and effects of incident.

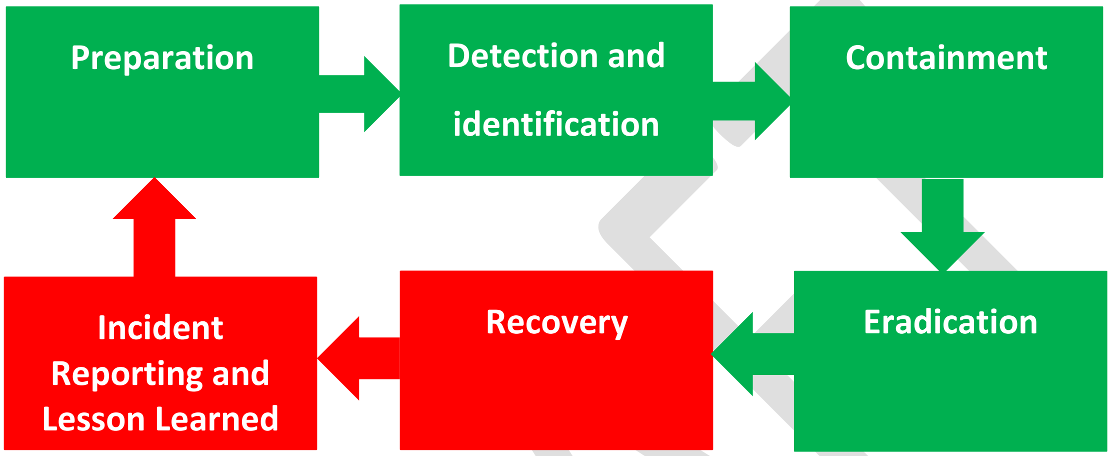

Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

Use the list of strategies below to choose most appropriate for the situation.

- Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks
- Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed
- If DOS/DDOS - control OT/APN Cloud
- Virus outbreak – contain LAN/system

3.4 Eradication

Prior to perform full system recovery and restoration, remediation efforts should be performed to fix the source of the incident.

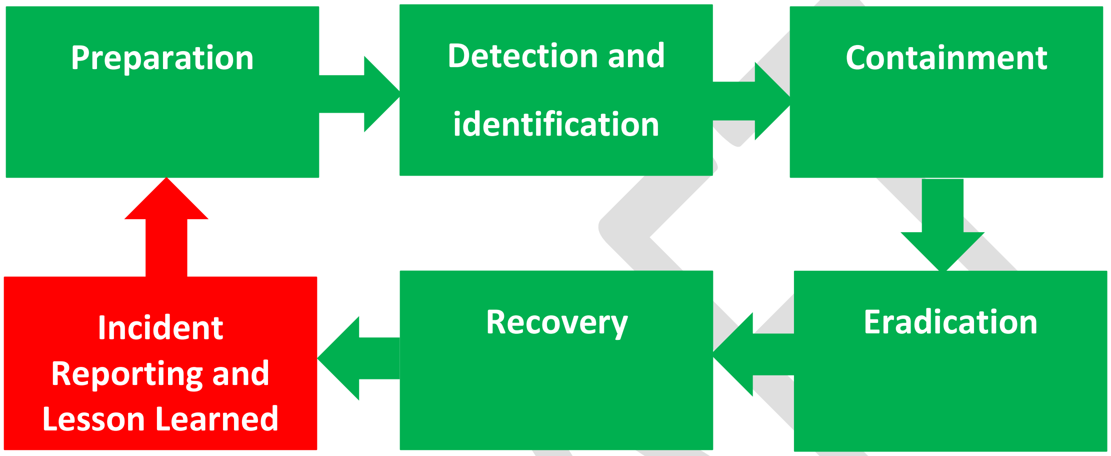

Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

Steps to eradicate components of the incident may include:

- Eradication of any malware found on the system
- Removal or replacement of vulnerable equipment
- Reconfiguration and patching of equipment or software
- Access cancellation for certain personal
- Access blocking from identified IP addresses
- Changing port configuration on firewall
- Increase security logging, alerting, and monitoring
- Clean installation of affected operating systems and applications

3.5 Recovery

Prior to restoring systems to normal operation, it is critical that the Team validate the system(s) to determine that eradication was successful, and the network is secure.


Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

If feasible, the system should be installed in a test environment to determine functionality prior to reintroduction into a production environment.

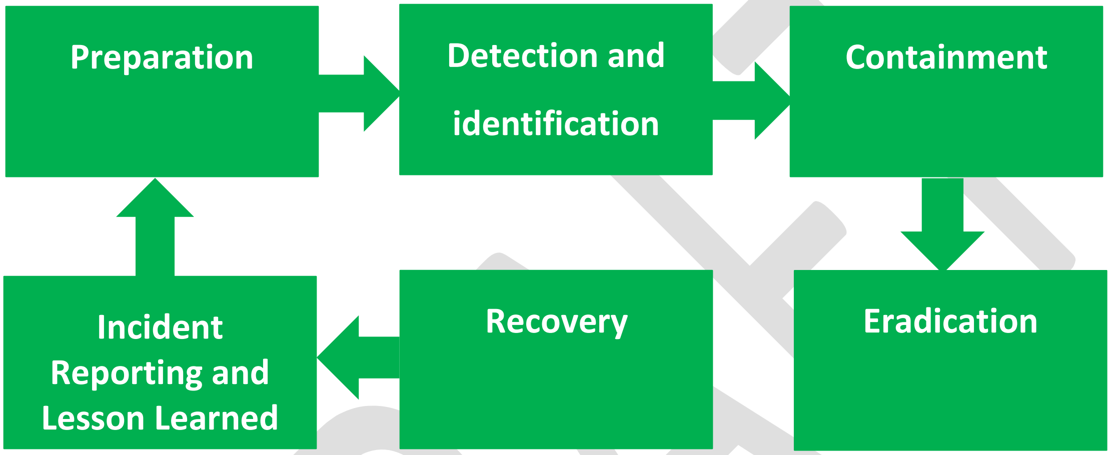
Recovery steps may include:

- Restoring systems from a clean backup and refer to RPO and RTO.
- Replacing corrupted data from a clean backup.
- Restoring network connections and access rules.
- Communicating with interested parties about changes related to increased security.
- Increasing network and system monitoring activities.
- Increasing internal communication/reporting related to monitoring.
- Engaging a third party for support in detecting or preventing future attacks.

3.6 Incident Reporting and Lesson Learned

3.6.1 Incident Reporting

In the final step, the organization identifies areas that could have been improved in the incident handling process, and then initiates steps to implement required changes.


Preparation
Detection and identification
Containment
Eradication
Recovery
Incident Reporting and Lesson Learned

- All OT incidents in the ICS environment shall be documented and kept in archival files for a minimum of 1 year.
- Report OT incidents that result in significant loss of data, system availability, or control of systems.
- Report OT incidents that impact operations of the NWC infrastructure to one of the government regulations.
- Report OT incidents that impact national security or public health and safety to one of government regulations.

3.6.2 Lesson Learned:

A lesson learned session should take place after the resolution of the incident for future incident plan.

It involves:

- getting to the root of how and why it happened

- evaluating how well your incident response plan worked to resolve the issue
- identifying improvements that need to be made by updating your incident response plan

3.7 Process

Activity		Responsible	Description
Incident Detection			
1.1	Report the incident	Any OT Asset Owner NWC Information Security Team NWC Leadership/Management	Responsible person reports the incident to Line Manager
Incident Response Team formation			
1.2	Incident Response Team formation	NWC Information Security representative	NWC Information Security representative identifies the team according to defined incident scenario document
Incident Response			
1.3	Identify of incident	Incident Response Team	Collects the information from responsible person for incident
1.4	Analyze the Incident	Incident Response Team	Analyzes the incident
1.5	Contain the incident	Incident Response Team	Performs the activities to contain the incident to avoid further disruption
1.6	Eradicate the incident	Incident Response Team	Performs the activities to eradicate the incident
1.7	Recover the system	Incident Response Team	Incident related recovery steps will be followed to recover the system

1.8	Incident Reporting and Lesson Learned	Incident Response Team	Incident will be reported and lesson learned will be logged for future incident plan

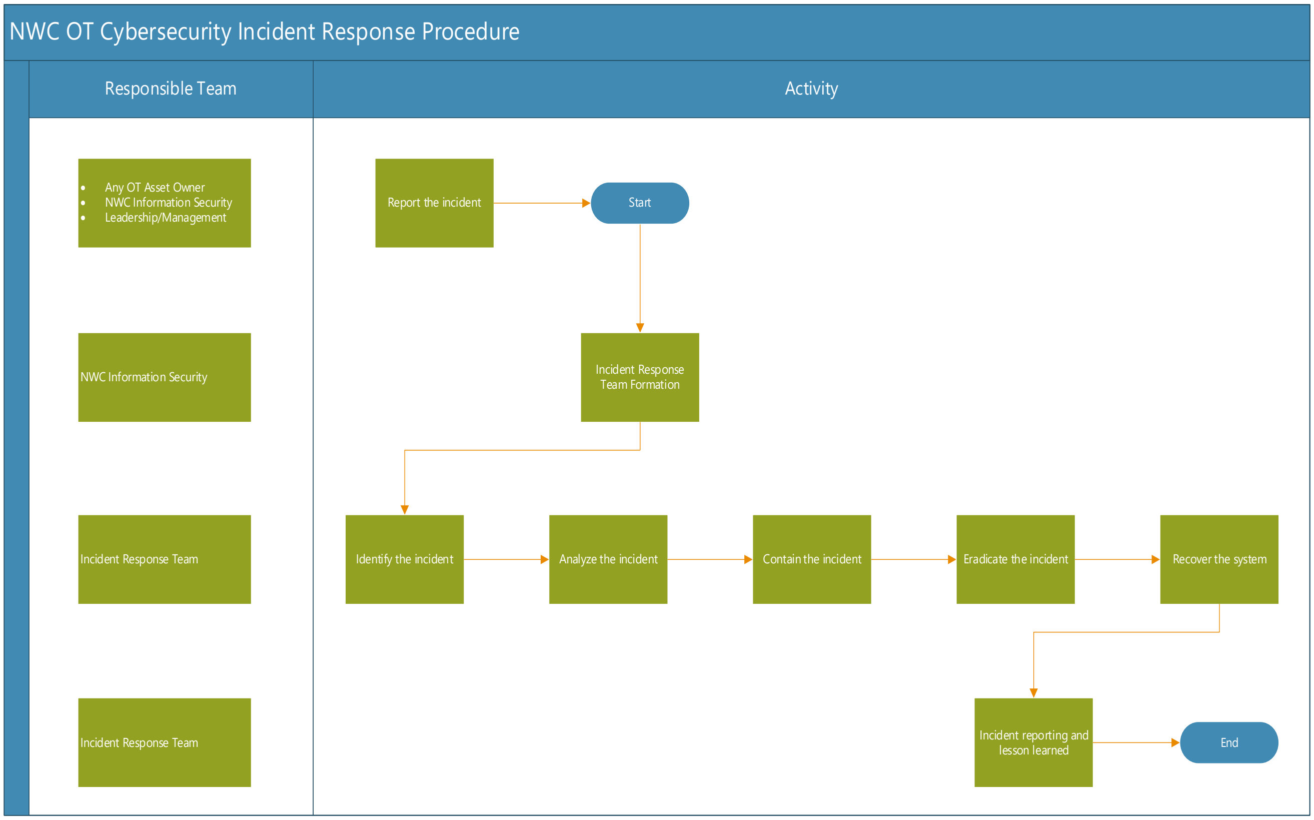
4. Exceptions

Exceptions shall be noted while performing incident response and recovery.

5. Compliance

All the activities performed during incident response must be complied with policies and standards.

6. Process Flow Chart


NWC OT Cybersecurity Incident Response Procedure
Responsible Team
Activity
Any OT Asset Owner
NWC Information Security
Leadership/Management
Report the incident
Start
NWC Information Security
Incident Response Team Formation
Incident Response Team
Identify the incident
Analyze the incident
Contain the incident
Eradicate the incident
Recover the system
Incident Response Team
Incident reporting and lesson learned
End