**Name of Organization**

**Incident Response Responsibilities and Positions**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Incident Response Responsibilities and Positions document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Team Composition 5](#_Toc90302821)

[II. Team Structure 5](#_Toc90302822)

[III. Team Composition 6](#_Toc90302823)

[Incident Handling Team (IHT) 6](#_Toc90302824)

[Incident Response Team Members 6](#_Toc90302825)

[Chief Information Security /Technology Officer (CISO/CIO/CTO) 7](#_Toc90302826)

[Incident Commander 7](#_Toc90302827)

[Command Staff 7](#_Toc90302828)

[General Staff 8](#_Toc90302829)

[200-Level ICS 8](#_Toc90302830)

[300-Level ICS 8](#_Toc90302831)

[400-Level ICS 8](#_Toc90302832)

# Team Composition

This Incident Response Responsibilities and Positions document is aligned with National Institute of Standards and Technology (NIST) Incident Response (IR) and National Incident Management System (NIMS) Incident Command System (ICS) frameworks.

# Team Structure



# Team Composition

## Incident Handling Team (IHT)

The IHT consists of Legal experts, Risk Managers, the Data Privacy Officer (DPO), the Public Information Officer (PIO) and other department managers that may be consulted or notified during incident response. Expert responsibilities include:

* Advise on incident response activities pertaining to their area of expertise.
* Maintain a general understanding of the Incident Response Plan (“the Plan”) and policies of the organization.
* Ensure incident response activities are in accordance with legal, contractual, and regulatory requirements.
* Participate in tests of the Plan and procedures.
* The team is responsible for internal and external communications pertaining to cyber security incidents.

## Cybersecurity Incident Response Team Members (CIRT)

The Incident Commander (IC) is supported by a Cybersecurity Incident Response Team (CIRT) of technical staff that work directly with the affected information systems and owners to research the time, location, and details of an incident. CIRT members are typically comprised of subject matter experts (SMEs), senior level IT staff, third parties, and outsourced security or forensic investigation partners.

Further responsibilities:

* Assist in incident response as requested by IC and organizational leadership. CIRT responsibilities should take priority over normal duties, depending on the level of incident.
* Understand the Plan and procedures to appropriately respond to an incident.
* Ensure tools are properly configured and managed to alert on security incidents/events.
* Analyze network traffic for signs of denial of service, distributed denial of service, or other external attacks.
* Review log files of critical systems for unusual activity.
* Monitor business applications and services for signs of attack.
* Collect pertinent information regarding incidents at the request of the Incident Commander.
* Consult with qualified information security staff for advice when needed.
* Ensure evidence gathering, chain of custody and preservation is appropriate.
* Participate in tests of the incident response plan and procedures.
* Be knowledgeable of service level agreements with service providers in relation to incident response.
* Continue to develop skills for incident response management.

## Chief Information Security /Technology Officer (CISO/CIO/CTO)

* Seek approval from Executive Management for the administration of the Plan.
* Coordinate response activities with auxiliary departments and external resources as needed to minimize damage to information resources.
* Provide updates on response activities to Incident Handling Team (IHT) and other stakeholders during an incident.
* Ensure service level agreements (SLAs) with service providers clearly define expectations of the organization and deliverables of the service provider in relation to incident response.
* Ensure policies related to incident management accurately represent the goals of the organization, and are regularly reviewed for such.
* Review the Plan to ensure that it meets policy objectives and accurately reflects the goals of the organization. Seek Plan approval from IHT.
* Work with the Incident Commander (IC) to periodically evaluate the effectiveness of the Plan and CIRT.
* Ensure CIRT managers are given the necessary authority to seize assets and stop services quickly to contain an incident.
* Approve close of moderate or critical-severity incidents.
* Ensure Cyber Insurance is maintained as necessary and appropriate stakeholders are informed.

## Incident Commander

* Single Incident Commander – Most incidents involve a single [Incident Commander](https://en.wikipedia.org/wiki/Incident_commander). In these incidents, a single person commands the incident response and is the decision-making final authority.
* Unified command – A [unified command](https://en.wikipedia.org/wiki/Unified_command_%28ICS%29) involves two or more individuals sharing the authority normally held by a single Incident Commander. Unified command is used on larger incidents usually when multiple agencies or multiple jurisdictions are involved. A Unified Command typically includes a command representative from major involved agencies and/or jurisdictions with one from that group to act as the spokesman, though not designated as an Incident Commander. A Unified Command acts as a single entity. It is important to note, that in Unified Command the command representatives will appoint a single operations section chief.
* Area command – During multiple-incident situations, an area command may be established to provide for Incident Commanders at separate locations. Generally, an Area Commander will be assigned – a single person – and the area command will operate as a logistical and administrative support. Area commands usually do not include an operations function.

## Command Staff

* Safety Officer – The safety officer monitors safety conditions and develops measures for assuring the safety of all assigned personnel.
* Public Information Officer (PIO or IO) serves as the conduit for information to and from internal and external stakeholders, including the media or other organizations seeking information directly from the incident or event. While less often discussed, the public information officer is also responsible for ensuring that an incident's command staff are kept apprised as to what is being said or reported about an incident. This allows public questions to be addressed, rumors to be managed, and ensures that other such public relations issues are not overlooked.
* Liaison Officer serves as the primary contact for supporting agencies assisting at an incident.

## General Staff

* Operations Section Chief: Tasked with directing all actions to meet the incident objectives.
* Planning Section Chief: Tasked with the collection and display of incident information, primarily consisting of the status of all resources and overall status of the incident.
* Finance/administration Section Chief: Tasked with tracking incident related costs, personnel records, requisitions, and administrating procurement contracts required by Logistics. E.g., Cost unit Leader, Documentation Unit Leader.
* Logistics Section Chief: Tasked with providing all resources, services, and support required by the incident.

## 200-Level ICS

At the ICS 200 level, the function of Information and Intelligence is added to the standard ICS staff as an option. This role is unique in ICS as it can be arranged in multiple ways based on the judgement of the Incident Commander and needs of the incident. The three possible arrangements are:

* Information & intelligence officer, a position on the command staff.
* Information & intelligence section, a section headed by an information & intelligence section chief, a general staff position.
* Information & intelligence branch, headed by an information & intelligence branch director, this branch is a part of the planning section.

## 300-Level ICS

At the ICS 300 level, the focus is on entry-level management of small-scale, all-hazards incidents with emphasis on the scalability of ICS. It acts as an introduction to the utilization of more than one agency and the possibility of numerous operational periods. It also involves an introduction to the emergency operations center.

## 400-Level ICS

At the ICS 400 level, the focus is on large, complex incidents. Topics covered include the characteristics of incident complexity, the approaches to dividing an incident into manageable components, the establishment of an "area command", and the multi-agency coordination system (MACS).