**Name of Organization**

**Incident Response**

**Where to start**

December 2021

**Revision History**

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

Instructions

The (Name of Organization) Incident Response Where to start 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. Introduction and Purpose 1](#_Toc90900644)

[II. Incident Response: Administration (Pre-Preparation Phase) 2](#_Toc90900645)

[III. Incident Response – Preparation Phase 2](#_Toc90900646)

[IV. Incident Response – Detection and Analysis Phase 3](#_Toc90900647)

[V. Incident Response – Containment Phase 3](#_Toc90900648)

[VI. Incident Response – Eradication Phase 4](#_Toc90900649)

[VII. Incident Response – Recovery Phase 4](#_Toc90900650)

[VIII. Incident Response – Post Incident Activities (Lessons Learned) 5](#_Toc90900651)

# Introduction and Purpose

The (Name of Organization), Where to Start document provides clear instructions on high level Incident Response Processes and when to use what documents and forms during the complete lifecycle of an incident.

The entire process for Incident Response Life Cycle includes the following phases:



The rest of this document is centered on using swimlane process diagrams that visually represent the actors (people/teams responsible) and process for each of the IR phases. These are supported by a list of relevant IR documents (the bottom lane in each diagram). The diagrams are self-explanatory so no further narrative for each was deemed necessary here. Further details are available in Sessions 3 and 5 of the training videos.

# Incident Response: Administration (Pre-Preparation Phase)



# Incident Response – Preparation Phase



# Incident Response – Detection and Analysis Phase



# Incident Response – Containment Phase



# Incident Response – Eradication Phase



# Incident Response – Recovery Phase

For this phase, each company and each system will have its own recovery processes and runbooks which should be part of Disaster Recovery, backup, and system documentation. For this phase each unique recovery and restoration/backup procedures for each system need to be followed.

# Incident Response – Post Incident Activities (Lessons Learned)

