**Name of Organization**

**Incident Response Tracking and Reporting**

December 2021

**Revision History**

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

Instructions

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

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc90305152)

[II. Incident Data 5](#_Toc90305153)

[III. IR Metrics 6](#_Toc90305154)

# Introduction and Purpose

In today’s always-on world, technology incidents and cyber breaches come with significant consequences. System downtime costs companies an average of $300,000 per hour in lost revenue, employee productivity, and maintenance charges. That does not include all the regulatory consequences, loss of reputation and clients because of an incident. With so much at stake, it’s more important than ever for teams to track incident management KPIs and use their findings to detect, diagnose, fix, and—ultimately—prevent incidents.

Besides KPI tracking, it is also key to track the actual cost of an incident (especially when it comes to cyber insurance, requesting reimbursement and/or support from state or federal agencies) for remediation and recovery.

Another main subject to consider is the storing all incident evidence in a secure and accessible way, available to authorized personnel only. Leakage of incident data, either accidentally or maliciously, can cause much damage to the organization.

# Incident Data

A secure centralized tracking system with ‘need to know' access leads to a more effective and methodical IR effort, as well as delivering an audit trail if the efforts result in legal prosecution of the perpetrator.

The following information should be included in the incident documentation system at a minimum:

* Date and time the event was reported
* Type of incident
* Source of incident reporting
* Summary of the incident
* Current state of the incident
* All actions taken in relation to the incident
* Contact information for all persons involved
* Evidence acquired during the investigation of the incident
* Relevant comments from IR team members
* Proposed future actions

For this purpose, the usage of Incident Report Intake Form, Chain of Custody and IR Log is recommended.

# IR Metrics

| IR Metrics |
| --- |
| Category | Measurement | Description |
| SLAs | # SLA adherence | Total percentage of incidents where SLAs were adhered to |
| Incidents | # Total Incidents / Year | Total amount of incidents responded to per year |
| # Incidents by Type / Year | Total number of incidents by category responded to per year |
| Time | # Personnel Hours / Incident | Total amount of labor spent resolving incident |
| # Days / Incident | Total amount of days spent resolving incident |
| # System Down-Time Hours / Incident | Total hours of system down-time until incident resolved |
| Cost | Estimated Monetary Cost / Incident | Estimated total monetary cost per incidence, including containment, eradication, and recovery, as well as data collecting and analysis (this may include labor costs, external entity assistance, tool procurements, travel, etc.) |
| Damage | # Systems Affected / Incident | Total number of systems affected per incident |
| # Records Compromised / Incident | Total number of records compromised per incident |
| Forensics | # Total Forensics Leveraged Incidents / Year | Total number of incidents requiring forensics (collection & analysis) per year |
| # System Images Analyzed / Incident | Total number of system images analyzed per incident |
| # System Memory Dumps Examined / Incident | Total number of system physical memory dumps examined per incident |

The following metrics will be useful to justify cybersecurity spend and insurance coverage: