**Name of Organization**

**Incident Response**

**Times and SLAs**

December 2021

**Revision History**

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

Instructions

The (Name of Organization) Incident Response Times and SLAs 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](#_Toc85689982)

[II. Response Times 1](#_Toc85689983)

[Table 1: Response Times 1](#_Toc85689984)

# Introduction and Purpose

The (Name of Organization), Incident Response Times and SLAs document defines objectives for establishing specific standards on the agreed response times to incidents based on their priority. The Incident Response Times and SLAs document builds on the objectives established in the Incident Response Plan (IR Plan) and provides appropriate response and communication times for different types of incidents.

# Response Times

The table provides guidelines on the agreed-upon service response times. These response times are based on incident criticality and provide each involved party a clear set of expectations. For each categorization, the scope of the incident also has to be taken into consideration when determining the overall risk, which includes evaluation of affected users, asset criticality and locations (e.g., a virus outbreak in entire test environment, completely isolated from production will have a lower categorization that the same virus outbreak in production with customer data and critical business assets).

Table 1: Response Times

The SLA and Response Times Table defines the minimal response time and ongoing communication requirements for a case.

| **Criticality Level** | **Initial Response Time** | **Ongoing Response (Critical Phase)** | **Ongoing Response (Resolution Phase)** | **Ongoing Communication Requirement** |
| --- | --- | --- | --- | --- |
| 1 | 60 Minutes | Cybersecurity Incident Response Team (CIRT) Incident Commander assigned to work case on 24x7 basis. | Incident Commander assigned to work on case during normal business hours. | Case update sent to appropriate parties on a daily basis during critical phase. If CIRT involvement is necessary to restore critical systems to service then case update will be sent a minimum of every 2 hours. Case update sent to appropriate parties on a weekly basis during resolution phase. |
| 2 | 4 Hours | CIRT Incident Commander assigned to work case on 24x7 basis. | CIRT Incident Commander assigned to work on case during normal business hours. | Case update sent to appropriate parties on a daily basis during critical phase.  Case update sent to appropriate parties on a weekly basis during resolution phase. |
| 3 | 48 Hours | Case is worked as CIRT time/resources are available. | Case is worked as CIRT time/resources are available. | Case update sent to appropriate parties on a weekly basis. |
| 4 | 72 Hours | Case is worked as CIRT time/resources are available. | Case is worked as CIRT time/resources are available. | Case update sent to appropriate parties on a weekly basis. |

Initial Response Time:

This specifies the maximum amount of elapsed time between incident identification and initial action taken by the CIRT team.

At a minimum, the following should occur within this initial response time:

1. Initial assessment and triage.
2. Case classification is determined.
3. The case ownership is established, and Incident Commander is assigned.
4. An email will be sent to the customer. This is the initial “we have your case” email. This email will include various information such as the date/time of the request, case number, the name, phone, and email of the Incident Commander, a CIRT escalation contact, the criticality and sensitivity level of the case, and an indication of when the customer will receive case updates.