**Name of Organization**

**Incident Response Management Log**

December 2021

**Revision History**

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

Instructions

This Incident Response Management Log serves to document all security incident-related activities for a given incident. This document should be updated throughout the Incident Response episode. Furthermore, each Cybersecurity Incident Response Team (CIRT) member must maintain a log of response team activities, findings, and interactions in support of the Information Security Incident Response.

Communication between third parties (e.g., cyber insurance, vendors, etc.) and escalations and information sharing with relevant or affected parties (e.g., other organizations must be logged in this document.

All incident response logs will become a part of the Incident Response Report.

Incident Response Management Log

|  |  |
| --- | --- |
| Incident Title: |  |
| Incident Opened Date: |  |
| Incident Commander: |  |
| Incident Description:  |  |

|  |
| --- |
| Incident Response Management Log  |
| Date/Time | Action/Event | Reporter/ Performed by | Details |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |   |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |