**Name of Organization**

**Incident Response**

**Lessons Learned**

December 2021

**Revision History**

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

Instructions

The (Name of Organization) Incident Response Checklist 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. The document is unclassified but contains sensitive information.

|  |
| --- |
| **INCIDENT IDENTIFICATION INFORMATION** |
| Date and Time of Notification: |
| Incident Detector’s Information: |
| Name: | Date and Time Detected: |
| Title: | Location: |
| Phone/Contact Info: | System or Application: |
| **INCIDENT SUMMARY** |
| **Type of Incident Detected:** |   |   |
| **☐ Denial of Service** | **☐ Malicious Code**  | **☐ Unauthorized Use** |
| **☐ Unauthorized Access** | **☐ Unplanned Downtime**  | **☐ Other** |
| Description of Incident: |
|  |
|  |
| **Names and Contact Information of All Other Parties Involved:** |
|  |
|  |
| **INCIDENT NOTIFICATION – OTHERS** |
| **☐ Incident Commander** | **☐ System or App Owner** | **☐ System or App Vendor** |
| **☐ CIRT** | **☐ Corp. Communications** | **☐ Legal Counsel** |
| **☐ IHT**  | **☐ Human Resources** |  |
| **☐ Other:** |  |  |
| **ACTIONS** |
| **Identification Measures (Incident Verified, Assessed, Options Evaluated):** |
|  |
|  |
| **Containment Measures (quarantine, shut down, network change):** |
|  |
|  |
| **Evidence Collected (Systems Logs, etc.):** |
|  |
|  |
| **Eradication Measures (locate hash, isolate):** |
|  |
| **Recovery Measures (restore to safe backup, DR invocation):** |
|  |
| **Other Mitigation Actions:** |
|  |
| This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only |
| **EVALUATION** |
| **How Well Did Incident Response Team Members Respond?** |
|  |
| **Were the Documented Procedures Followed? Were They Adequate?** |
|  |
| **What Information Was Needed Sooner?** |
|  |
| **Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?** |
|  |
| **What Could Work Force Members Do Differently the Next Time an Incident Occurs?** |
|  |
| **What Corrective Actions Can Prevent Similar Incidents in the Future?** |
|  |
|  |
| **What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?** |
|  |
|  |
| **Other Conclusions or Recommendations:** |
|  |
|  |
| **FOLLOW-UP** |
| **Reviewed By:** |  |
| **☐ Security/Risk Officer** | **☐ Incident Commander** |
| **☐ Privacy Officer** | **☐ Other** |
| **Recommended Actions Carried Out:** |
|  |
|  |
| **Initial Report Completed By:** |
|  |
| **Follow-Up Completed By:** |
|  |

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.