**Name of Organization**

**Incident Response Documents Overview**

December 2021

**Revision History**

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

# IR & DR Documents Overview

All documents here can be downloaded on NCTCOG website located here:

<https://nctcog.org/ep/resources/cyber-security-incident-response-planning-system>

|  |  |
| --- | --- |
| **Document Name** | **Details**  |
| **Incident Response Framework** | Provides structure to support incident operations and supporting documents. |
| **Incident Response Plan (“the Plan”)** | Outlines an organization's procedures, steps, and responsibilities of its incident response. |
| **Incident Response Operations Checklist**  | Checklist for meet all key IR Plan requirements.  |
| **Incident Response Standard** | Provides the standard definitions and overview on which the Incident Repose Plan (“the Plan”) is based on. |
| **IR Consolidated List of Standards** | Overview of all applicable standards for incident response and threat management. Used as guidance for more detailed information to develop an IR Plan, organization, and service delivery. |
| **IR Organization Structure** | Provides the best practice organizational structure and chain of command for an IR organization (CIRT). |
| **DR Initial Planning Agenda** | Pre-planning for the disaster recovery exercise. |
| **Regulatory Notification Requirements** | Regulatory reporting requirements in case of a breach and disclosure of data. |
| **IR Customer and Media Communications** | Guidance on protocol for media communication and notifications following an incident. |
| **IR Standard Operating Procedures** | Provides guidance on key steps to perform full Life Cycle Incident management for key threats. |
| **DR Facilitator Guide Tabletop Exercises** | A guidebook for the facilitator to follow when conducting training exercises related to Disaster Recovery. |
| **DR Initial Planning Minutes** | Documentation and accountability of time and personnel. |
| **DR Final Planning Agenda** | Finial agenda concerning the training objectives and goals for the DR exercise. |
| **DR Exercise Evaluation**  | Observer form to use to evaluate the DR training.  |
| **IR Lesson Learned Form** | Formed to log any Lessons Learned following an incident which are then taken to create an Improvement Plan. |
| **DR After Action Agenda** | Identifies what needs to be addressed in After Action Meeting. |
| **DR Report and Improvement Plan** | Disaster recovery report outlining all actions taken during DR as well as lessons learned and Improvements to be taken. |
| **IR Responsibilities and Positions** | Lists IR Handling Team and Team Members, along with their roles and responsibilities. |
| **Incident Categorization** | Provides description, priority level, and category guidelines for Incidents. |
| **Tech Incident Response Requirements** | Lists the minimum baseline configuration requirements for various devices to be able to support efficient and rapid responses to incidents and forensic investigations. |
| **IR Report Template** | Template to create IR Reports. To be used as soon as an incident has been identified, updated during the incident, and closed when incident has been resolved. Document to capture all relevant IR information. |
| **Incident Management Log** | Form to record Date/Time, Action/Event, Reported/Performed by, and Details of IR as the incident progresses. An electronic ticket system can be used as well, if available. |
| **Incident Response Toolkit** | List of IR Tools and open-source tools for incident responses, network monitoring, SIEM and forensic analysis. Tools can be downloaded from the Internet. |
| **Third Party Risk Management** | Defines requirements for establishing Third-Party Risk Management program to minimize risk for cyber security incidents and breaches related to subcontractors, vendors and other entities providing services. |
| **Incident Response Organizations** | Provides a list of organizations that handle IR and how to contact them. |
| **Incident Response Times and SLAs** | Provides guidance on agreed upon service response times based on their priority. |
| **IR Forensic Intake Form** | Details on media (HDD) materials / chain of custody. |
| **IR Chain of Custody**  | Control of received and/or released items for an investigation. |
| **DR Requirements Industries** | Highlights the requirements for all key industries related to IT Disaster Recovery. |
| **Risk Management Plan** | Details the organization's risk management process, risk analysis, scoring and management. |
| **IT Disaster Recovery Plan Template** | Provides guidance on how the business will recover after an IT disaster. |
| **Business Impact Analysis Template** | Template to create a Business Impact Analysis for Risk Management and Disaster Recovery for each IT System, assets, and business processes. |
| **Risk Register and Acceptance** | Register to contain all identified and assessed risks and status updates. A living document to be updated as risks are identified and/or closed. |
| **IR - Where to start** | IR cheat sheet providing process overview and lists which documents to use when, and at what stage of the Incident Response Life Cycle. |
| **IR Tabletop Exercise Full** | A detailed, full-blown incident response tabletop exercise. |
| **IR Tabletop Exercise Examples** | Incident response exercises to test and enforce incident repones, test staff and existing processes. Document provides guidelines on how to set up Tabletop exercises with examples. |
| **Incident Notification Form - Version 1** | Long and more detailed incident intake form to be used when incident has been identified and needs to be reported to CIRT team for investigation. If electronic ticket system is used, this document should serve as a guideline as to what information is to be collected and passed to CIRT team. |
| **Incident Notification Form - Version 2** | Simple incident intake form to be used when incident has been identified and needs to be reported to CIRT team for investigation. If electronic ticket system is used, this document should serve as guideline what information is to be collected and passed to CIRT team. |
| **IR Operations Checklist** | Checklist to be used by IR Ops. |
| **IR Tracking and Reporting** | Provides guidelines on what IR data is to be tracked for improvement, cost, trending, and reporting. |
| **IR Acronyms** | List of commonly used acronyms. |
| **IR Financial Tracker** | Form to help track finances deployed during an incident. |
| **IR Document usage list** | Overview of all documents created for this project that outlines their purpose and links to SharePoint for download. |
| **Virus outbreak** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Unauthorized Access** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Root Access** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Phishing** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Improper Computer Usage** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Elevation of Privilege** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Data Theft** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **Malware/Ransomware Outbreak** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |
| **DDoS (distributed Denial of Service) Attack** | Standard Operating Procedures (SOPs) and step-by-step actions for Incident Life Cycle for this type of incident. |