**Name of Organization**

**Incident Response Operations Checklist**

December 2021

**Revision History**

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

Instructions

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

**Components of Incident Response Operations**

Every organization should develop an Incident Response Plan (“the Plan”) that defines the scope of preparedness and incident management activities necessary for that organization(s). The Plan should also describe organizational structures, roles and responsibilities, policies, and protocols for providing Incident Response support. The Plan not only facilitates response and short-term recovery activities but drives decisions on long-term prevention and mitigation efforts or risk-based preparedness measures directed as specific events. The Plan should be flexible enough for use in all emergencies.

A complete IR Plan will consist of multiple documents and spreadsheets and should describe the purpose of the Plan, situation and assumptions, concept and context of operations, organization and assignment of responsibilities, administration and logistics, plan development and maintenance, and authorities and references. It should also contain forms, checklists, incident-specific procedures, and escalation/communication plans and up to date contact lists.

IR Plans should pre-designate organizational and/or functional representatives and authorities to the Incident Commander or Unified Command – based on criticality of event or emergency - whenever possible to facilitate responsive and collaborative incident management. IR Plans should also include pre-incident and post-incident public awareness guidance, education, and communications plans and processes.

The checklist below details several components of an Incident Response Plan that are consistent with the National Incident Management System (NIMS) concepts and terminology. Examine your IR Plan and use the checklist to determine which components are included in your plan and those that need to be added. A detailed description that explains what each question means follows the checklist.

| **Incident Response Operations Components Checklist** | | |
| --- | --- | --- |
| **Operations Plan Component** | **Check if Applicable** | **Adoption Date** |
| 1. Does your IR Plan define the scope of preparedness and incident management activities necessary for your organization? |  |  |
| 1. Does your IR Plan describe organizational structures, roles and responsibilities, policies, and protocols for providing Incident Response support? |  |  |
| 1. Does your IR Plan facilitate response and short-term recovery activities? |  |  |
| 1. Is your IR Plan flexible enough to be used in all incident responses? |  |  |
| 1. Does your IR Plan have a description of its purpose? |  |  |
| 1. Does your IR Plan describe the risk situation and assumptions? |  |  |
| 1. Does your IR Plan describe business administration and logistics? |  |  |
| 1. Does your IR Plan contain a section that covers the development and maintenance of your IR Plan? |  |  |
| 1. Does your IR Plan contain authorities and references? |  |  |
| 1. Does your IR Plan include assignment of responsibilities? |  |  |
| 1. Does your IR Plan contain functional annexes, forms, and escalation/communication matrices? |  |  |
| 1. Does your IR Plan include pre-incident and post-incident public awareness, education, and communications plans and protocols? |  |  |
| 1. Does your IR Plan contain IR-specific appendices? |  |  |
| 1. Does your IR Plan pre-designate functional area representatives to the Incident Response Center/Multi-agency Coordination System? |  |  |
| 1. Does your organization have the capability and means to track hours and expenses associated with an Incident? |  |  |
| 1. Have you reached out to the Texas Department of Information Resources (TX DIR) Office of the CISO (mandated for Texas agencies) or your Local Emergency and Incident Response Team for guidance? |  |  |
| 1. Do you have Cybersecurity Insurance? |  |  |

**Question 1: Does your IR Plan define the scope of preparedness and incident management activities necessary for your local or tribal organization?**

The IR Plan should include all cyber security events that your organization may reasonably expect to occur and all the preparedness and incident management activities necessary to ensure an effective response to those cyber security events. Regulatory requirements may also dictate the cyber security events and preparedness activities that must be included in the IR Plan.

**Question 2: Does your IR Plan describe organizational structures, roles and responsibilities, policies, and protocols for providing Incident Response support?**

A description of the organizational structure should clearly identify what organizations will be involved in the Incident Response and/or emergency response. After each organization is identified, they should be assigned a specific set of responsibilities that are normally based on the strengths and capabilities of each. The policies and protocols for providing emergency support should be described in the Plan. This information is typically described in the administration and logistics section as well as the authorities and references section of the basic plan.

**Questions 3: Does your IR Plan facilitate response and short-term recovery activities?**

An IR Plan is usually not a mitigation plan and not a recovery plan. The Plan should however describe and provide the basis for a response and short-term recovery operations. The response activities typically take place initially and are designed to minimization operational downtime and protect data and the IT environment. The short-term recovery activities typically follow the response activities and are designed to stabilize the situation and set the stage for recovery and establish normal business operations.

**Question 4: Is your IR Plan flexible enough to be used in all incident responses?**

The IR Plan should reflect the organization’s approach to all types of Cybersecurity incidents and emergencies. Functional annexes should provide an outline of roles and responsibilities of each responding agency regardless of the type of emergency. In other words, the IR Plan should be flexible and useful in the event of any emergency, not just Cybersecurity Incident Response.

**Question 5: Does your IR Plan have a description of its purpose?**

The purpose should include a general statement of what the IR Plan is meant to do. It should also include a summary of the components of the plan including the functional annexes and emergency/incident-specific appendices and standard operational procedures.

**Questions 6: Does your IR Plan describe the risk situation and assumptions?**

The situation sets the stage for planning. It should be based on the organization’s risk (emergency/incident) identification analysis. The situation section typically includes a Risk Assessment focusing on the probability and impact of the threat, vulnerable facilities or assets, and resource dependencies on other organizations. The assumptions section should describe those things that are assumed to be true that directly impact the execution of the IR Plan. The assumptions may describe the limitations of the IR Plan and provide a basis for improvisation and modification if it becomes necessary. Assumptions may also describe identification of potential Cyber Security events, the nature of those cyber security events and the frequency that are expected to occur.

**Question 7: Does your IR Plan describe administration and logistics?**

This section covers general support requirements and availability of support services from other agencies or organizations. This section of the IR Plan should also reference mutual aid agreements; liability provisions; policies to manage communication to the public; and vendor management to include backup solution, spare parts, and hardware replacement.

**Question 8: Does your IR Plan contain a section that covers the development and maintenance of your IR Plan?**

The IR Plan should include a section describing the overall approach to planning, participants included in the planning process, and how the plan will be maintained and updated. One individual should be assigned to coordinate these processes and provisions should be made to regularly review, test, and revise them. This information is typically found in the organization’s Incident Response Policy.

**Question 9: Does your IR Plan contain authorities and references?**

The IR Plan should list out references to any laws, statutes, ordinances, executive orders, regulations, and formal agreements relevant to the emergencies. These will indicate the legal basis for incident response/emergency operations and should specify the extent and limits of authorities.

**Question 10: Does your IR Plan describe the organization and assignment of responsibilities?**

The organization and assignment of responsibilities should establish which organizations will be relied upon to respond to the emergency. The IR Plan should describe the tasks each element of the organization is responsible for and expected to perform. The IR Plan can contain a list that plots response functions provided by third parties (e.g., vendors and suppliers) and allow for a quick clarification of the assignment of primary and support responsibilities.

**Question 11: Does your IR Plan contain functional annexes?**

Functional annexes are the part of the IR Plan that begin to provide specific information and direction. Functional annexes should contain activities to be performed by anyone with a responsibility under that function. Functional annexes also clearly define actions before, during, and after an incident. Some examples of functional annexes are Communications Matrix, list of vendors and suppliers, various check lists, Standard Operating Procedures, etc.

**Question 12: Does your IR Plan include pre-incident and post-incident public awareness, education, and communications plans and protocols?**

The IR Plan should describe how the organization will deal with communication to the public and clients to provide valuable information about the cyber security events, protective action options for those events, and next steps. How this information will be communicated to the public before and after incidents occur should be described in the IR Plan.

**Question 13: Does your IR Plan contain IR-specific appendices?**

Incident-specific appendices (e.g., Standard Operating Procedures for ransomware, phishing, DDoS, etc.) are part of an IR Plan. Whereas planning consideration, common to all key incidents, are addressed in functional annexes, incident-specific information is included in the appendices. An IR Plan is considered compliant when it contains incident-specific appendices or annexes.

**Question 14: Does your IR Plan pre-designate functional area representatives to the Emergency Operations Center / Multi-Agency Coordination System?**

This information is typically described in functional or hazard-specific annexes and is more detailed than the information in the Cyber Security IR Plan. NIMS doctrine states that all incidents use the Incident Command System (ICS) to establish command and control for the response at the scene of an incident. Most incidents are managed locally, and the local—or organizational—IR Plan is the guide to how the local response to an incident will be handled. Therefore, it is appropriate that the organization set up and utilize an Emergency Operations Center (EOC) or a Multi- agency Coordination System depending on the size and complexity of the incident. The IR Plan should pre-designate which organization is assigned which responsibilities and that organization should provide representatives to the EOC or the Multi-agency Coordination System that is being utilized. In some cases, a local or state agency has the lead for a particular incident/hazard that requires that an agency to take control of an incident scene. These designations are normally established by laws, regulations, executive orders, or policies. The designated agency should have trained personnel in place to set up an ICS structure at the scene and provide the Incident Commander for that incident. If an agency is requested to send a representative to the scene, that representative should be folded into the Unified Command of the incident. As an organization you need to have the in your communication/escalation matrix the contacts to the local or Texas state emergency teams

**Question 15: Does your organization have the capability and means to track hours and expenses associated with an Incident?**

During each Incident – not just Cybersecurity – each organization needs to be able to track resources, time and costs associated with the incident. This includes internal and external costs. Tools, third parties that need to be engaged, additional resources - throughout the entire IR lifecycle until Restore and Lessons learned. Tracking these expenses – especially if the incident is of critical and large/regional/national nature is key to obtain state or national funds and/or obtain reimbursement and be able to collaborate and align with NIMS.

**Question 16: Have you reached out to the Texas Department of Information Resources (TX DIR) Office of the CISO (mandated for Texas agencies) or your Local Emergency and Incident Response Team for guidance?**

Depending on the size of the incident, various organizations and groups are available to you for support with Incident Management. Texas Department of Information Resources (TX DIR) can provide your organization with incident response support, guidance, and resources, before, during, and after a cybersecurity incident. Having established contact with TX DIR or your local Emergency Response Team prior to an Incident, knowing who to reach out to and how they can assist will be very beneficial and facilitate a resolution.

**Question 17: Do you have Cybersecurity Insurance?**

Having Cybersecurity Insurance as part of your Incident Response Toolkit can not only cover many of the expenses associated with Incident Management (such as resources, tools, recovery, and remediation costs) but Cyber Insurance companies often have additional resources available that can be of assistance to investigate and collaborate on remediation efforts. As an organization it is key to understand what incidents your Cyber Insurance will cover, what information you will need to provide them when contacting them, who to reach out to when you have an incident to be able to receive support quickly.