

# Incident Handling and Response Plan

## <Organization Name and Details>

Source: <https://www.cisa.gov>

Date: \_\_\_\_\_ Name of person completing this form: \_\_\_\_\_

### Executive Support

List the executives who had input to this document and endorse its development and applicability.

Name of Executive	Date	Signature
<i>Sponsor</i>		
<i>Incident Manager</i>		

### Process Description

Explain the incident management process in a manner that provides a high-level understanding to personnel who must implement this plan.

### Critical Services

*Indicate the priority of critical services.*

Priority Level	Service Restoration Time Objective	Status

### Plan Activation Criteria

*Describe conditions that must be met before the incident management plan can be executed.*

### Assignment of Responsibility

*List employees at your organization who are responsible for developing and maintaining this plan.*

Name of the Employee	Date	Signature	Responsibility

### Communication Channels

*Identify communication channels used to notify stakeholders if this plan is to be executed.*

Stakeholders	Channel Types

### Key Contacts

*List the key contact information essential to the service and this plan. Include the service owner as well as internal and external technical support (examples embedded).*

Name	Role	Company Name	Phone	Email
	Service owner			
	Internal technical support for information assets			
	Internal technical support for technology assets			
	External support for information assets			
	External technical support for technology assets			
	Hardware vendor			
	Primary software vendor			
	ISP			
	MSP			
	Testing partner			

	Identity and access team lead			
	Audit and compliance body			
	Human resources			
	Regulatory body			
	Fire company			
	Police			
	Alternate processing site contact			
	Electric utility POC			
	Telecommunications POC			
	Water utility POC			
	Executive management			
	Legal counsel			
	Public relations lead			
	Social media lead			
	Internal resource for continuity plan execution			
	Stakeholder who requires notification of plan activation			
	Stakeholder who requires notification of plan activation			
	Regulatory organizations that require notification if this plan is activated			

	Health-care providers who should be notified if this plan is activated			
	Other organizations that should be notified if this plan is activated			

### Service Owner(s)

*List the business owner(s) responsible for critical services.*

Name of Employee	Date	Signature	Role

### Essential Roles and Alternates

*Identify roles essential for incident management, as well as primary and backup/alternate personnel to perform those roles.*

Role	Primary Personnel	Alternate Personnel

### **Essential Information Assets**

*List the information assets essential to incident management.*

Information Asset Name	Description	Logical Location	Physical Location	Backup Strategy and Schedule

### **Special Considerations for Information Assets**

*Identify any special considerations for handling information assets in the event of plan activation.*

--

### **Essential Technology Assets**

*List the technology assets essential to incident management.*

Asset Name	Description	Physical Location	Backup Strategy/Location

### **Primary and Alternate Site(s)**

*Identify the location(s) for command, control, and communication.*

Site Name	Physical Location

### **Incident Management Checklist**

*List the steps to follow when obtaining an incident status (examples embedded).*

Issue	Responsible Party	Guidance	Status
Safety	Security, HR, Facilities		
Physical damage			
Business impact			
Immediate actions			
Media attention			

### Plans of Action

*List the predetermined plans and procedures to be relied on during an incident (examples embedded).*

<b>Fire and evacuation</b>	Instruct personnel to evacuate the immediate area. Locate available fire extinguishers, if possible, and contact fire department.
<b>Communications/Media</b>	
<b>Health and Safety</b>	
<b>Disaster Recovery</b>	
<b>Service Continuity</b>	
<b>Cybersecurity</b>	
<b>Physical Security</b>	
<b>Pandemic</b>	
<b>Emergency Procurement and Transportation</b>	

### **Document Management**

*List out the details of documents related to this IH&R plan.*

Name of the Document	
Old Version	
New Version	
Document Owner	
Approver	
Last Review Date	



**Schedule for testing this plan**  
**This plan will be tested <at a defined frequency>**  
**Date of last test <YYYY/MM/DD>**

*Identify any support plans that are related to this plan.*

Plan Name	Relationship	Observations