

Incident Handler Checklist

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the Incident Handler

Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 3: Identify the Incident Scope and Impact

Observation that led to consulting incident handling and response team	<input type="checkbox"/> Missing IT Resources <input type="checkbox"/> Internal Data Breach <input type="checkbox"/> External Data Breach <input type="checkbox"/> Internal/External Rumor <input type="checkbox"/> Others, Specify <hr/>	
Method used to detect the problem	<input type="checkbox"/> Security Controls Audit (IDS/Firewall/SIEM) <input type="checkbox"/> External Audit <input type="checkbox"/> Third Party <input type="checkbox"/> Others, Specify <hr/>	
Date and time of incident detection	Date:	
	Time:	
Details of person who detected the incident	Name:	
	Job Title:	
	Email Address:	
	Contact Number:	
	Contact Address:	
Departments aware of this incident	<input type="checkbox"/> Higher-Level Management <input type="checkbox"/> Administration <input type="checkbox"/> IT <input type="checkbox"/> SoC <input type="checkbox"/> Legal <input type="checkbox"/> Others, Specify <hr/>	

Other organizations that are aware of the incident (e.g., law enforcement, third-party vendor, regulators, etc.)		
Assets target/affected by the incident	<input type="checkbox"/> Customer Data <input type="checkbox"/> Employee Data <input type="checkbox"/> Business Plans <input type="checkbox"/> Financial Information <input type="checkbox"/> Others, Specify <hr/>	
List out the recent incidents occurred in this organization, if any (e.g., identity theft, employee misbehavior, log issues, malware detection, etc.)		
Describe the history and impact of similar incidents in the past		
Name of the primary/backup Incident response coordinators	Name:	
	Job Title:	
	Name:	
	Job Title:	
Name of the authorized person responsible for taking business decisions on the affected operations and IT infrastructure	Name:	
	Job Title:	
Specify legal/compliance obligations, if any (e.g., HIPAA, PCI, Laws, etc.)		

Stakeholders responsible for internal compliance/privacy/legal issues	Name:	
	Job Title:	
	Name:	
	Job Title:	
Location of evidence preservation		
Current incident handling and response stage (check all that apply)	<input type="checkbox"/> Detection and Analysis <input type="checkbox"/> Containment <input type="checkbox"/> Eradication <input type="checkbox"/> Recovery	
Whether the incident involves external parties (e.g., external services, business partners, alliances, etc.)		

Section 4: Incident Review by the Organization

(To be Filled with the help of IT/HR/Legal Departments)

Persons responsible for preserving the evidence	Name:	
	Job Title:	
	Name:	
	Job Title:	
Evaluations performed to define the scope and impact of the incident	<input type="checkbox"/> IT <input type="checkbox"/> HR <input type="checkbox"/> Legal <input type="checkbox"/> Security <input type="checkbox"/> Others, Specify _____	
Steps taken for the containment and eradication of the incident (submit separate reports)	<input type="checkbox"/> Containment Report <input type="checkbox"/> Eradication Report	
Specify tools/commands used for investigating the incident (submit separate detection and analysis reports)	Report Name:	
	Report Name:	
Log analysis reports, if any	Report Name:	
	Report Name:	
Alerts generated by infrastructure systems and security controls (submit notification report)	Report Name:	
	Report Name:	
Specify, if any unresolved issues related to the incidents		
Specify, if any further analysis required		
Involvement of law enforcement	<input type="checkbox"/> Yes <input type="checkbox"/> No If Yes, Specify Details _____	

Section 5: Technical Assessment to Determine Scope and Impact of Incident

(To be Filled with the help of IT/IS Professionals)

Infrastructure Assessment		
Person(s) responsible for IT network functions and operations	Name:	
	Job Title:	
	Name:	
	Job Title:	
Topology or architecture of the affected network/system (submit in a separate report)	Report Name:	
	Report Name:	
Physical locations of the affected IT infrastructure (specify both individual names and locations)		
Organization's IT infrastructure is hosted by third party (specify, if any)		
Network restrictions implemented for employees/stakeholders/third-parties/others		
List out the asset management and discovery tools used		
IT asset inventory report for all the infrastructure components related to the incident (report must include hardware and software information)	Report Name:	
	Report Name:	

Log Analysis		
Current existing logs for the IT infrastructure (specify all the logs currently active and running)	<div><input type="checkbox"/> Network Logs<ul style="list-style-type: none"><input type="checkbox"/> Firewalls<input type="checkbox"/> Routers<input type="checkbox"/> IDS/IPS<input type="checkbox"/> SIEM<input type="checkbox"/> Web Proxies<input type="checkbox"/> Firewalls<input type="checkbox"/> File/Network Servers<input type="checkbox"/> Printers<input type="checkbox"/> Others, Specify _____</div> <div><input type="checkbox"/> Physical Logs<ul style="list-style-type: none"><input type="checkbox"/> Campus Entry/Exit Logs<input type="checkbox"/> Sign-in Sheets<input type="checkbox"/> CCTV Video Surveillance<input type="checkbox"/> Room/Equipment Access Registers<input type="checkbox"/> Others, Specify _____</div>	
Specify the retention policy for security logs		
Is there any log backup strategy (if yes specify frequency of backup)	<div><input type="checkbox"/> Yes <input type="checkbox"/> No</div> <div>If Yes, Specify Frequency _____</div>	
Security Analysis		
Last security/vulnerability assessment conducted (if yes, submit report)	Date of Assessment:	
	Assessment Report Name:	

List out the hardware and software components in the affected IT infrastructure (e.g., IDS/IPS, firewall, authentication systems, etc.)	Hardware Components:	
	Software Components:	
Network diagram or document that defines security components topology and architecture	Report Name:	
	Report Name:	
IT department need to establish inventory of IT assets if not available	<input type="checkbox"/> Operating system versions <input type="checkbox"/> Service patches for networked and servers and computers <input type="checkbox"/> Access privileges for groups/individuals <input type="checkbox"/> Network and Security policies (need to submit proof for distribution of policies within the organization) <input type="checkbox"/> Others, Specify <hr/>	
IDS/IPS system in the organization	Network/Host-Based:	
	Type/Version:	
	Passive/Reactive:	
	Updates:	<input type="checkbox"/> Auto <input type="checkbox"/> Manual
Anti-virus system in the organization	Network/Host-Based:	
	Type/Version:	
	Updates:	<input type="checkbox"/> Auto <input type="checkbox"/> Manual
Available password policies/employee account audits		

Configuration of wireless access point security		
Details of email systems used (e.g., applications, configurations, email security policy, remote access policy, etc.)		
File servers in the organization	Type:	
	Share Permissions:	
	File System:	
	Archived/Backed Up:	
IT professionals responsible for backup policies, business continuity and disaster recovery (specify name, job title, and department)		
	Whether these IT professionals are informed of incident <input type="checkbox"/> Yes <input type="checkbox"/> No	

Section 6: Further Steps for Incident Response and Remediation

(To be Filled with the help of IT/HR/Legal Departments)

Are there any incident response plans/guides/instructions available for the affected departments/groups	<input type="checkbox"/> Yes <input type="checkbox"/> No
List out the IT professionals who have been trained in incident response/computer forensics (specify type of training provided)	
List out the network/system components that cannot be kept offline without critical impact on business continuity	
Tools available for to assess network/host-based activities	
List out the data that can be moved/deleted from the organization for further review/analysis	
Security measures needed to protect such data	
Backup/restore capabilities available to recover from incident	
Final incident handling report to be submitted to:	<input type="checkbox"/> Higher-Level Management <input type="checkbox"/> IT <input type="checkbox"/> HR <input type="checkbox"/> Legal <input type="checkbox"/> Security <input type="checkbox"/> Others, Specify _____