

Recovery from Insider Threats Checklist

Note: Prior to starting recovery from insider threats, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

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

Section 2: Details of the Incident Responder

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

Section 3: Checklist for Recovering from Insider Threats

Actions	Completed
Ensure to gather the evidence required for legal proceedings through forensic processes.	<input type="checkbox"/>
If the stolen data impacts user accounts, change the passwords of all the accounts and make two-factor authentication mandatory. If application data is stolen, use copyright to prevent other companies from using it.	<input type="checkbox"/>
If the attacker has damaged any data or placed malware, remove the malicious artifacts and recover the data from clean and trusted backups.	<input type="checkbox"/>
Check whether the recovery processes and backups are implemented to continue business operations after the incident.	<input type="checkbox"/>
Check whether the data backup plan is developed and implemented to recover any data affected by the attack.	<input type="checkbox"/>
Ensure to secure backup media and its content from alteration, theft, or destruction. Administrators should ensure that regular backups are performed and tested for integrity and availability.	<input type="checkbox"/>
Check whether the separation of duties and configuration management procedures are implemented to perform backups on computer systems, networks, and databases.	<input type="checkbox"/>
Check whether a person-to-person rule is implemented to secure the backup process and physical media.	<input type="checkbox"/>
Check whether a chain-of-custody document is maintained for accessing and handling backup media.	<input type="checkbox"/>
Check whether the cloud-to-cloud backup solutions are implemented.	<input type="checkbox"/>
Secure the backup media from unauthorized access and ensure that it is accessed only by limited individuals.	<input type="checkbox"/>
Check whether “immutable” and “unbreakable” backups are implemented.	<input type="checkbox"/>
Check whether the administrator keys are stored in a separate location.	<input type="checkbox"/>
Check whether patches for the identified vulnerabilities have been applied to prevent similar incidents.	<input type="checkbox"/>