

Preparation for Handling Insider Threats Checklist

Note: Prior to starting the preparation to handle insider threats checklist, 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: Preparation Steps to Handle Insider Threats	
Actions	Completed
Whether the policies are documented, framed, and implemented to mitigate insider threats like data theft, modification, and IT sabotage	<input type="checkbox"/>
Whether the details of previous insider incidents are preserved and investigated carefully while preparing an incident response plan	<input type="checkbox"/>
Whether the employees are provided with training and awareness on how to safeguard organizational data	<input type="checkbox"/>
Whether employees are trained to detect and avert social engineering attempts	<input type="checkbox"/>
Whether regular security awareness training is provided to sensitize employees about threats and the organization's security controls	<input type="checkbox"/>
Whether policies that prohibit employees from disclosing or forwarding any confidential information are implemented	<input type="checkbox"/>
Whether employees are aware of the need for security policies and access controls, their responsibilities and constraints of employment, and the consequences of violations	<input type="checkbox"/>
Whether employees are trained on how to identify and report any policy violation or suspicious espionage events	<input type="checkbox"/>
Whether employees are trained to understand the security risks involved in exchanging information over the phone, voice mails, messages, or unencrypted email	<input type="checkbox"/>
Whether the critical assets of an organization are identified and prioritized, and a risk management strategy is defined to protect these assets	<input type="checkbox"/>
Whether audits and maintenance of records are done for all critical assets, such as servers, computer systems, and accessories	<input type="checkbox"/>
Whether logging for all access attempts is enabled and regularly audited them to identify violations or attempts made to violate a security policy	<input type="checkbox"/>

Whether it is ensured that all employees are following strict password and account management policies and a reporting mechanism is implemented for unauthorized account access and potential attempts at social engineering	<input type="checkbox"/>
Whether the principle of least privileges is implemented when granting access to organizational resources	<input type="checkbox"/>
Whether policies are enforced for the separation of duties and are provided with minimum privileges required by employees to perform their duties	<input type="checkbox"/>
Whether employee activities such as phone calls and email are monitored	<input type="checkbox"/>
Whether employee monitoring software are used to track computer activities using screen capturing, data, keystroke, idle time, printer, removable drives, and audio/video monitoring	<input type="checkbox"/>
Whether employees' Internet activities such as browsing history, uploads, downloads, web access, data traffic are monitored along with other activities, such as accessed files and privilege misuse	<input type="checkbox"/>
Whether physical entry and exit, system logins, network activities, accessed files, uploads and downloads, privilege misuse, and so on are recoded properly for all employees	<input type="checkbox"/>
Whether access violations and attempts to violate physical space and other equipment are logged and audited properly	<input type="checkbox"/>
Whether physical monitoring devices such as CCTV cameras and alarms are used across the organization to record suspicious activities	<input type="checkbox"/>
Whether it is ensured that terminated employees do not have any access to the physical space or non-public areas of the organization	<input type="checkbox"/>
Whether data loss prevention, log management, IDS, SIEM, and behavior analysis tools are deployed	<input type="checkbox"/>
Whether honeypots are installed to lure attackers to a seemingly soft target and identify potential attackers	<input type="checkbox"/>
Whether honeytokens are used, which work the same way as honeypots, but at the directory or file level	<input type="checkbox"/>

Whether a thorough background check of new employees before hiring is performed	<input type="checkbox"/>
Whether the organization's security policy is framed to include that access cards or ID cards must be worn or displayed for all employees and visitors at all times	<input type="checkbox"/>
Whether an acceptable level of loss and plan security policies are defined accordingly	<input type="checkbox"/>
Whether application whitelisting and blacklisting is implemented to prevent employees from downloading and executing malicious software	<input type="checkbox"/>
Whether selected trustworthy employees are trained and employed for insider watch and protocols are implemented to report any suspicious co-worker	<input type="checkbox"/>
Whether a proactive and evolving insider threat detection governance program is established	<input type="checkbox"/>