

Eradication of Insider Threats Checklist

Note: Prior to starting the eradication of 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 Eradicating Insider Threat	
Actions	Completed
Human Resources	
Check whether policies are created and implemented pertaining to employee behavior and ethical use of information.	<input type="checkbox"/>
Check whether employees signed a confidentiality and nondisclosure agreement that describes their agreement with the company's confidentiality policies.	<input type="checkbox"/>
Ensure to use interviews, feedback forms, or surveys, to allow employees to raise their concerns regarding the workplace and organization.	<input type="checkbox"/>
Ensure that employees can express their feelings and problems at the workplace and provide suggestions to improve them.	<input type="checkbox"/>
Keep track of employee expenditures and income generation activities as unexpected and unexplained changes in the financial status of an employee signify an income generated from external sources.	<input type="checkbox"/>
Audit financial reports to identify if an employee was involved in any fraud.	<input type="checkbox"/>
Check whether proper training and awareness is provided for all employees regarding insider activities.	<input type="checkbox"/>
Check whether a thorough background check is conducted on new employees and employees who hold sensitive positions.	<input type="checkbox"/>
Check the employee history in previous organizations, such as arrest history, history of policy violations, and evidence of financial problems.	<input type="checkbox"/>
Ensure to monitor all the activities carried out by the staff using surveillance cameras in all important areas.	<input type="checkbox"/>
Examine and respond to suspicious behavior of employees, beginning with the hiring process.	<input type="checkbox"/>
Interact with employees so that they can brief any employee to keep an eye on and notify them about the individuals who have been disciplined or promoted.	<input type="checkbox"/>

Check whether co-workers, vendors, and clients are notified about the departure of an employee.	<input type="checkbox"/>
Review and audit network activity prior to the employee's departure.	<input type="checkbox"/>
Network Security	
Check whether the computer networks are secured by configuring firewalls and monitoring outbound traffic to HTTP and HTTPS services.	<input type="checkbox"/>
Check whether rules have been created to reduce the outbound transfer of files to an authorized set of users and systems.	<input type="checkbox"/>
Check whether file sharing, instant messaging, and other features among employees are prevented.	<input type="checkbox"/>
Scan all outgoing and incoming emails for sensitive information and malicious codes.	<input type="checkbox"/>
Check whether a strict password policy is implemented with multi-factor authentication.	<input type="checkbox"/>
Check whether account management policies and procedures are implemented.	<input type="checkbox"/>
Check whether proper system administration safeguards are implemented for critical servers.	<input type="checkbox"/>
Check whether zero-trust network access (ZTNA) solutions are implemented to provide access only after satisfying certain characteristics.	<input type="checkbox"/>
Access Controls	
Check whether the access privileges to employees or users are enabled based on the routine performance of their job roles.	<input type="checkbox"/>
Disable employees' ability to download content, install applications, enable remote access, modify system logs, or access the boot menu of their systems.	<input type="checkbox"/>

Check whether modification alert tools are installed on user systems to flag any attempts to change system settings.	<input type="checkbox"/>
Regularly audit the access rights of the employees and revoke unnecessary access.	<input type="checkbox"/>
Check whether strict policies are implemented for accessing sensitive information.	<input type="checkbox"/>
Ensure to document all access requests that are granted to users along with justification after being vetted by a supervisor.	<input type="checkbox"/>
Ensure that employees get permission prior to accessing sensitive systems.	<input type="checkbox"/>
Disable employee's access after termination, including access to premises, applications, accounts, and network devices.	<input type="checkbox"/>
Change passwords for wireless networks regularly.	<input type="checkbox"/>
Restrict concurrent logins to prevent repudiation issues.	<input type="checkbox"/>
Check whether data loss prevention (DLP) tools are implemented to restrict an employee from exfiltrating data.	<input type="checkbox"/>
Check whether identity security solutions are deployed to track accounts and access across the organization.	<input type="checkbox"/>
Privileged Users	
Check whether a non-repudiation technique is implemented to view all the actions performed by administrators and privileged users.	<input type="checkbox"/>
Check whether the default administrative accounts are disabled to ensure accountability.	<input type="checkbox"/>
Ensure that administrators use unique accounts during the installation process.	<input type="checkbox"/>

Check whether encryption methods are used to prevent administrators and privileged users from accessing backup tapes and sensitive information.	<input type="checkbox"/>
Monitor the activities of system administrators and privileged users who have permission to access sensitive information.	<input type="checkbox"/>
Ensure to have control over access to administrators and privileged users.	<input type="checkbox"/>
Implement just-in-time privileged access management (JIT PAM) solutions to provide necessary privileges for the required period to avoid persistent privilege access.	<input type="checkbox"/>
Use privileged password managers to avoid administrators viewing the password in plain text.	<input type="checkbox"/>
Audit Trails and Log Monitoring	
Enforce account and password policies and procedures to ensure that employees regularly change their passwords using password management tools and active directory configurations.	<input type="checkbox"/>
Check whether the measures are implemented to monitor the online activities of insiders.	<input type="checkbox"/>
Ensure to notify employees that the organization will log all their activities related to the organizational systems and data.	<input type="checkbox"/>
Ensure to perform regular assessments of logging, monitoring, and auditing processes to identify and investigate suspicious insider actions.	<input type="checkbox"/>
Configure audit trails for network devices, operating systems, commercial software, and custom applications.	<input type="checkbox"/>
Auditing should review and examine the changes performed on the critical assets of any organization.	<input type="checkbox"/>
Ensure to protect audit files through file permissions and store them in a central host server to avoid alterations.	<input type="checkbox"/>
Ensure to maintain a chain of custody document for accessing and handling log files.	<input type="checkbox"/>

Check whether intrusion detection and file integrity software are deployed to detect and monitor suspicious activities on sensitive data.	<input type="checkbox"/>
Physical Security	
Ensure proper logging devices with ID and biometric scanning abilities at all the entry and exit points.	<input type="checkbox"/>
Deploy security guards to investigate unauthorized entry or to stop employees from taking unauthorized personnel into the organization's premises.	<input type="checkbox"/>
Check whether a system security policy is implemented wherein the systems automatically lock after a certain amount of inactivity.	<input type="checkbox"/>
Make it mandatory for employees to lock their data centers or computers when leaving their desks.	<input type="checkbox"/>
Strictly prohibit entry of portable media by placing metal detectors at all entry points.	<input type="checkbox"/>
Ensure physical security of the server rooms, databases, and other critical data resources by placing dual authentication, such as a combination of a password and biometric lock.	<input type="checkbox"/>
Use cable locks for portable devices such as laptops and smartphones.	<input type="checkbox"/>
Secure the hard drives in the systems by placing physical locks on them.	<input type="checkbox"/>
Place surveillance cameras at all important areas, such as the entrance, near meeting rooms, and server rooms.	<input type="checkbox"/>
Ensure all meeting rooms are soundproof to avoid eavesdropping and espionage attempts.	<input type="checkbox"/>
Ensure that all documents that contain crucial information are shredded before discarding.	<input type="checkbox"/>
Wipe all the hard disks and other media before discarding old computers and laptops.	<input type="checkbox"/>

Have strict access policies for third-party staff and vendors.	<input type="checkbox"/>
Implement a clean desk policy both digitally and physically.	<input type="checkbox"/>
Prohibit the use of cell phone cameras.	<input type="checkbox"/>