

# Containment of Insider Threats Checklist

**Note:** Prior to starting the containment of 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:			
<i>Additional Details (If Any):</i>			

Section 3: Checklist for Containing Insider Threats	
Actions	Completed
Whether incident responders have isolated the affected systems after detecting the incident	<input type="checkbox"/>
Whether the IT and computer security teams have blocked the suspect's organizational email account and network credentials and seized company-issued desktops, laptops, mobile, or other devices	<input type="checkbox"/>
Whether the appropriate permissions are obtained to seize any personal devices that might have been used in the attack	<input type="checkbox"/>
Whether the individual's ability to access organization premises are removed	<input type="checkbox"/>
Whether attack vectors such as malware, portable storage devices, secret cameras, and recording devices are examined and contained	<input type="checkbox"/>
Whether the affected departments are informed and requested to check for any potential losses	<input type="checkbox"/>
Whether strict guidelines have been issued to other employees to discourage tailgating, using unauthorized drives, transferring data using unencrypted means, and discussing confidential matters in common areas	<input type="checkbox"/>
Whether system and account passwords have been changed for all users	<input type="checkbox"/>
Whether employees, contractors, third-party vendors, or outsiders identified as spies are continuously monitored until the organization terminates them from the office	<input type="checkbox"/>
Whether the suspect for portable devices carrying the stolen data is checked and all account data used during the incident has been gathered	<input type="checkbox"/>
Whether a complaint is registered in the appropriate jurisdiction to take the appropriate legal action, up to and including prosecuting the responsible individual	<input type="checkbox"/>
Whether the HR team has blocked all access to suspicious employees and put them under continuous monitoring until further decision from the management	<input type="checkbox"/>
Whether the security personnel have blocked any unauthorized communication channels used by insiders	<input type="checkbox"/>