

Preparation for Handling OT-based Incidents Checklist

Note: Prior to starting the preparation for handling OT-based incidents 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 OT-based Incidents	
Actions	Completed
Whether the OT and ICS-specific incident response plans are established	<input type="checkbox"/>
Whether the roles and responsibilities of IH&R team members are properly defined for OT-based security incident response	<input type="checkbox"/>
Whether the IH&R team is trained on ICS or OT-specific security incidents	<input type="checkbox"/>
Whether the employees are trained on the best practices and reporting mechanisms of OT-based security incidents	<input type="checkbox"/>
Whether the business continuity plan and architectural design of the OT environment is properly created	<input type="checkbox"/>
Whether the network maps are maintained and updated in a central location	<input type="checkbox"/>
Whether the passive or active network discovery tools are maintained to identify anomalous or malicious traffic or devices in the network	<input type="checkbox"/>
Whether the multi-team architectural discussions are conducted before or while beginning incident response	<input type="checkbox"/>
Whether crown jewel analysis is performed for the detection and analysis of security incidents	<input type="checkbox"/>
Whether the isolation and communication plans are created for OT-based incident response	<input type="checkbox"/>
Whether supporting forms and documentation for OT-based incidents are prepared by the engineers	<input type="checkbox"/>
Whether the necessary tools and resources are included to manage the OT-based security incidents	<input type="checkbox"/>
Whether contact information of both the internal and external resources is maintained	<input type="checkbox"/>
Whether routine drills for the IH&R team are conducted by involving real evidence to effectively respond during actual crisis time	<input type="checkbox"/>