

Recovery from OT-based Security Incidents Checklist

Note: Prior to starting the recovery from OT-based security 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: Checklist for Recovering from OT-based Security Incidents	
Actions	Completed
Whether the perimeter security, including firewall rulesets and boundary gateway access control lists, are tightened	<input type="checkbox"/>
Whether the rebuilt systems are connected to the OT environment using standard procedures	<input type="checkbox"/>
Whether the backup systems are tested thoroughly, including their security controls	<input type="checkbox"/>
Whether the operations of affected devices are continuously monitored after recovery	<input type="checkbox"/>
Whether an independent review of recovery-based activities is performed	<input type="checkbox"/>
Whether the principle of least privilege is enforced to access any resource after restoring them	<input type="checkbox"/>
Whether Open Platform Communications United Architecture (OPC UA) security is correctly configured to improve the security and reliability of ICS systems	<input type="checkbox"/>
Whether the OPC UA certificate's private keys and user passwords are securely stored	<input type="checkbox"/>
Whether all backup systems are patched and maintained to the same level as the primary systems	<input type="checkbox"/>
Whether acceptance tests and procedures are established and executed to ensure that systems have been restored to the pre-incident state	<input type="checkbox"/>
Whether the passwords for the ICS/SCADA devices are frequently changed	<input type="checkbox"/>
Whether only real-time connectivity is allowed to the organizational networks if there is a control function or any requirement	<input type="checkbox"/>
Whether connections to the control systems are terminated from the remote/persistent vendors	<input type="checkbox"/>
Whether the disaster recovery plan (DRP) is updated considering the latest and unplanned incidents	<input type="checkbox"/>
Whether controller configuration, logic code, protection control relays, remote terminal units, and process configurations of the OT infrastructure are implemented for proper recovery of data	<input type="checkbox"/>