

Recover of Malware Incidents Checklist

Note: Prior to starting the recovery from malware incidents, 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 malware incidents	
Actions	Completed
Whether the infected systems are recovered by reimaging and rebuilding them from scratch.	<input type="checkbox"/>
Whether any data lost owing to infection is recovered using data recovery tools, trusted clean backup sources, or backup data through cloud synchronization.	<input type="checkbox"/>
Whether the hosts and file shares scanned with updated antivirus software signatures/definitions.	<input type="checkbox"/>
Whether a full scan on system and device backups is run to ensure that all malware traces have been removed before using backups to restore servers, systems, and databases.	<input type="checkbox"/>
Whether email services are restored after blocking malicious email senders at the server level.	<input type="checkbox"/>
Whether two-factor authentication is enabled for organizational email, login, and user accounts.	<input type="checkbox"/>
Whether scanning of links and attachments is enabled for all emails passing through the server.	<input type="checkbox"/>
Whether automatic file sharing is disabled between systems.	<input type="checkbox"/>
Whether the systems are connected to a clean network to download, install, and update the OS and all other software.	<input type="checkbox"/>
Whether Internet security gateways are implemented to analyze content for known malware in specific protocols (including encrypted protocols).	<input type="checkbox"/>
Whether containment measures are kept in effect until the estimated number of unpatched or infected systems is sufficiently low.	<input type="checkbox"/>
Whether the 3-2-1 backup strategy is implemented for better recovery from backup storage.	<input type="checkbox"/>
Whether a robust data protection strategy is implemented.	<input type="checkbox"/>
Whether the affected systems are completely wiped, including the master boot record (MBR).	<input type="checkbox"/>

Whether the Windows System Restore utility tool is utilized to recover data in the Windows system using point-in-time backups.	<input type="checkbox"/>
Whether previous file versions are restored from the restore point in Windows.	<input type="checkbox"/>
Whether the critical software and components such as BIOS, drivers, etc. are rebuilt and cleaned from a trusted software library and verified software hashes.	<input type="checkbox"/>
Whether automatic alerts triggering API-driven workflows are used for post-malware recovery.	<input type="checkbox"/>