

Eradication of Malware Incidents Checklist

Note: Prior to starting the eradication of malware 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 Received:	Report		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: Eradication of Malware Incidents Checklist	
Actions	Completed
Whether antivirus software, intrusion prevention systems (IPSs), content filtering tools, and firewalls are used to mitigate malware threats	<input type="checkbox"/>
Whether the services, programs, applications, and executables that install malware onto the system are blacklisted	<input type="checkbox"/>
Whether the organizational malware databases are regularly updated	<input type="checkbox"/>
Whether the browsers, applications, and operating systems are updated, and the vulnerabilities that the malware had exploited as entry points are patched	<input type="checkbox"/>
Whether application whitelisting is implemented to only allow network access to crucial applications	<input type="checkbox"/>
Whether user-account privileges are implemented for all users	<input type="checkbox"/>
Whether the websites containing malicious content and auto-downloads are blocked to prevent automatic malware downloads	<input type="checkbox"/>
Whether all access to system and server basic input/output systems BIOSs are blocked by segregating functional systems using virtualization technologies	<input type="checkbox"/>
Whether the drives are reformatted, the systems are reimaged, and critical files from the backup are restored	<input type="checkbox"/>
Whether a well-defined business continuity and disaster recovery (BCDR) plan is implemented to respond quickly and effectively to a malware incident	<input type="checkbox"/>
Whether automatic update settings for all patched operating systems are turned on	<input type="checkbox"/>
Whether the physical hard drives or forensically sound snapshots of those storage drives are preserved before rebuilding or replacing physical systems	<input type="checkbox"/>
Whether it is ensured that obsolete platforms are properly segregated from the rest of the network	<input type="checkbox"/>
Whether autorun is disabled for removable media such as USB drives	<input type="checkbox"/>
Whether the passwords for all compromised accounts are reset or replacement accounts are created and the compromised accounts are permanently disabled	<input type="checkbox"/>
Whether open-source projects, such as code repositories, that enter the enterprise from untrusted external sources are tracked properly	<input type="checkbox"/>
Whether network packets are inspected using protocol monitoring tools	<input type="checkbox"/>