

Preparation to Handle Web Application Security Incident

Note: Prior to starting the preparation to handle web application 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: Preparation to Web Application Security Incident Checklist	
Actions	Completed
Whether the IH&R team prepared IH&R plans for the most common web incidents, such as SQL injection, cross-site scripting (XSS), and CSRF	<input type="checkbox"/>
Whether a backup website is developed and maintained to publish its content	<input type="checkbox"/>
Whether an alternate Internet connection from another provider is subscribed or selected any anti-DDoS service provider	<input type="checkbox"/>
Whether the contact lists of the ISPs (the current ISP and alternate ISP), all the clients, critical customers, key stakeholders, third-party advertising agencies, and law enforcement authorities are maintained	<input type="checkbox"/>
Whether all critical IP addresses and protocols are whitelisted	<input type="checkbox"/>
Whether an inventory of organizational IT Infrastructure is maintained, which may include IP addresses, routing tables, autonomous system settings, a circuit ID, a network topology of the organizational network, etc.	<input type="checkbox"/>
Whether a disaster recovery plan and business continuity plan are developed and maintained	<input type="checkbox"/>
Whether the latest web application and network monitoring tools are deployed that can alert the IH&R team in the case of suspicious events and other activities	<input type="checkbox"/>
Whether the organization have maintained a good network infrastructure such that there are no bottlenecks in the network	<input type="checkbox"/>
Whether the time-to-live (TTL) settings are customized for the critical systems	<input type="checkbox"/>
Whether the web server logs and settings are reviewed and audited	<input type="checkbox"/>
Whether details about active assets and their business impacts are gathered for further proceeding with the IH&R processes	<input type="checkbox"/>
Whether access controls for the website login page are designed properly	<input type="checkbox"/>