

Preparation to Handle Email Security Incidents

Note: Prior to starting the preparation of handle email security 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:			
<i>Additional Details (If any):</i>			

Section 3: Checklist of Preparation Steps for Handling Email Security Incidents	
Actions	Completed
Organizations must install and configure email filtering tools to filter and block all malicious emails transmitted across the network	<input type="checkbox"/>
Deploy email monitoring tools that check for malicious attachments, links, messages as well as sensitive data in incoming and outgoing emails	<input type="checkbox"/>
Establish email independent communication channels, such as telephone, message, VOIP, etc., for reporting the incidents and sending data to the incident response team and other authorities	<input type="checkbox"/>
Create awareness to employees about different email attacks, techniques attackers use to trick users and crimes supported by emails	<input type="checkbox"/>
Train the employees to analyze email information such as sender address, content validation, examining signature, etc.	<input type="checkbox"/>
Develop and implement an acceptable email usage policy to define satisfactory behavior of an employee for using organization email	<input type="checkbox"/>
Configure email client or servers to create regular archives and backups of all emails	<input type="checkbox"/>
Install email log analysis tools	<input type="checkbox"/>

Section 4: Checklist of Preparation Steps for Handling Email Security Incidents	
Actions	Completed
Organizations must install and configure email filtering tools to filter and block all malicious emails transmitted across the network	<input type="checkbox"/>
Deploy email monitoring tools that check for malicious attachments, links, messages as well as sensitive data in incoming and outgoing emails	<input type="checkbox"/>
Establish email independent communication channels, such as telephone, message, VOIP, etc., for reporting the incidents and sending data to the incident response team and other authorities	<input type="checkbox"/>
Create awareness to employees about different email attacks, techniques attackers use to trick users and crimes supported by emails	<input type="checkbox"/>
Train employees to analyze email information such as sender address, content validation, examining signature, etc.	<input type="checkbox"/>
Develop and implement an acceptable email usage policy to define satisfactory behavior of an employee for using organization email	<input type="checkbox"/>
Configure email client or servers to create regular archives and backups of all emails	<input type="checkbox"/>
Install email log analysis tools	<input type="checkbox"/>