

CYBER SECURITY INCIDENT RESPONSE HANDLING CHECKLIST

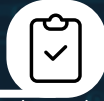
THIS CHECKLIST COVERS THE NECESSARY STEPS FOR THE INCIDENT RESPONSE
PROCEDURES AND HANDLING OF AN INCIDENT.

PREPARATION



- Ensure good behaviour in systems and applications
 - Understand the normal behaviours of networks, systems, and applications
 - Identify precursors and indicators through alerts
 - Create a log retention policy
 - Establish a baseline level for logging and auditing
 - Use and maintain a knowledge database of normal operation and incident handling steps
 - Keep all host clocks synchronised
- Enhance data protection
 - Identify and protect sensitive data
 - Safeguard incident data
 - Obtain file system backups and system snapshots
- Prepare handling and recovery plan
 - Acquire tools and resources
 - Include requirements of incident reporting in incident response policy
 - Follow established evidence gathering and handling procedures
 - Establish incident reporting mechanisms
 - Maintain an updated list of contact information
 - Ensure the ability to capture volatile data from systems as evidence
 - Perform incident response drills for the plan
 - Review and update the plan regularly

POST-INCIDENT ACTIONS



- Create a follow-up report including details of the cause, cost of the incident, and the enhancement measures
- Conduct a lessons learned meeting
 - Collect views from different stakeholders
 - Work out an improvement plan

DETECTION AND ANALYSIS



- Determine whether an incident has occurred
 - Analyse the precursors and indicators
 - Perform event correlation and research
 - Document the investigation and gather the evidence
- Prioritise the handling of the incident
- Report the incident to the appropriate internal personnel and external parties

CONTAINMENT, ERADICATION AND RECOVERY



- Collect evidence
 - Acquire, preserve, secure, and document evidence
- Contain the incident
 - Isolate affected hosts from network
- Eradicate the incident
 - Identify and mitigate exploited vulnerabilities
 - Remove malware, inappropriate materials, and other components
 - Repeat the "Detection and Analysis" steps to identify all other affected systems, then contain and eradicate the incident
- Recover from the incident
 - Resume affected systems to an operationally ready state
 - Confirm that the affected systems are functioning normally
 - Implement additional monitoring measures if necessary

