Process Step	Description	Responsible Role	Key Activities/Checks
1. Incident Identification	Identify and classify incidents.	All Employees	- Use Intrusion Detection Systems (IDS), antivirus, and SIEM tools to monitor for unusual activities. - Establish criteria for incident alerts.
2. Incident Reporting	Report and record incidents.	All Employees	- Report incidents to the Incident Response Team (IRT) via designated channels, such as email or a dedicated hotline. - Include details like date, time, location, affected systems, and the nature of the incident in reports.
3. Incident Triage	Assess incident impact and validity.	Incident Responder(s)	- Evaluate the severity and potential impact of the incident based on predefined criteria. - Verify the authenticity of reported incidents using validation procedures.

4. Incident Categorization	Categorize incidents by type.	Incident Responder(s)	- Classify incidents into predefined categories like malware, data breaches, denial of service, or other incident types. - Determine the appropriate response strategies based on the incident category.
5. Incident Containment	Prevent the incident from spreading.	Incident Responder(s)	- Isolate affected systems or networks to prevent the incident from spreading. - Implement access controls and network filtering to stop unauthorized access.
6. Incident Recovery	Restore affected systems.	Incident Responder(s)	- Use the latest available backups for system and data recovery. - Continuously monitor system health and performance to ensure proper operation.
7. Notification and Communication	Inform relevant stakeholders.	Incident Responder(s)	- Notify senior management, legal, and communication teams about the incident. - If required by law, inform external entities such as regulatory authorities or law enforcement.

8. Forensic Investigation	Collect evidence and conduct analysis.	Forensic Analyst(s)	- Collect logs, artifacts, and data for analysis. This includes memory captures, disk images, and network packet captures. - Analyze evidence to determine the extent and source of the incident, including intrusion vectors and malware analysis.
9. Root Cause Analysis	Identify underlying causes.	Incident Responder(s)	- Conduct a root cause analysis to understand the origins of the incident. - Identify any lapses in security controls, misconfigurations, or vulnerabilities that contributed to the incident. Recommend preventive measures.
10. Documentation and Reporting	Maintain records and create reports.	Incident Responder(s)	- Maintain a detailed incident log containing all actions taken, findings, and timelines. - Create a comprehensive incident report summarizing the incident, response actions, and findings, and share it with senior management and stakeholders.

11. Incident Review	Evaluate the effectiveness of the response.	Incident Responder(s)	- Review the incident response process to assess its effectiveness. - Assess the performance of individuals involved and identify areas for improvement.
12. Lessons Learned	Document and apply lessons learned.	Incident Responder(s)	- Document lessons learned from the incident, including what worked well and what needs improvement. - Incorporate these lessons into future processes, training, and awareness programs.
13. Remediation	Address vulnerabilities and weaknesses.	Incident Responder(s)	- Ensure all identified vulnerabilities, weaknesses, or misconfigurations that contributed to the incident are addressed. - Apply patches, updates, and provide training or awareness campaigns as needed.
14. Incident Closure	Officially close the incident.	Incident Responder(s)	- Confirm that the incident has been fully resolved and that all affected systems and data are back to normal operation.

15. Post-Incident Review	Evaluate the overall incident response.	Incident Responder(s)	- Review the entire incident response process, from detection to resolution. - Assess the effectiveness of remediation efforts, including any changes made to prevent future incidents.
16. Reporting to Management	Provide management with incident summary.	Incident Responder(s)	- Share a final incident report with senior management and stakeholders, summarizing the incident, response actions, and lessons learned.