



System

Administrator

NIST SP 800-61

Support Specialist

Responder

Information Systems Security Manager

Information Systems

Security Officer

Page 3/4

Verify data, accounts, ISs, and/or networks support mission requirements.	Rebuild affected ISs by reinstalling its OS/apps from trusted media. Reload user data using trusted backups. Change all passwords on the IS as well as any IS within its trust domain.	Update IDS signatures. Retune the logging policy. Retune or deploy file integrity checkers, URL checkers, email filters, etc. Monitor for warnings/indicators suggesting the incident is reoccuring.	Coordinate recovery strategies.		Start Recovery phase. Notify stakeholders.
			Submit an updated report to ISSO.	Notify ISSM.	

User	System Administrator	Network Administrator	Infrastructure Support Specialist	Incident Responder	Information Systems Security Officer	Information Systems Security Manager
	Discuss detection and response timeframes. Discuss user, technician, and leader actions executed correctly/incorrectly. Discuss the availability, applicability, and adherence to procedures. Discuss which security controls would prevent similar incidents in the future. Identify which tools/resources are needed to detect, analyze, and mitigate similar incidents in the future.	Discuss detection and response timeframes. Discuss user, technician, and leader actions executed correctly/incorrectly. Discuss the availability, applicability, and adherence to procedures. Discuss which security controls would prevent similar incidents in the future. Identify which tools/resources are needed to detect, analyze, and mitigate similar incidents in the future.	Discuss detection and response timeframes. Discuss user, technician, and leader actions executed correctly/incorrectly. Discuss the availability, applicability, and adherence to procedures. Discuss which security controls would prevent similar incidents in the future. Identify which tools/resources are needed to detect, analyze, and mitigate similar incidents in the future.	Add AAR comments to the final report. Submit the final report to ISSO. Archive the final report in support of trend analysis. Coordinate the implementation of Lessons Learned. Use the final report to build future training scenarios.	Notify ISSM.	Start Post-Incident Activity phase. Notify stakeholders. Start Preparation
						phase.