Incident Response Checklist

Summary
This checklist is designed for enterprise IT teams.

Preparation
* Validate incident severity and scope
* Notify on-call and incident commander
* Create incident channel and timeline

Identification
* Confirm indicators of compromise
* Identify affected systems and users
* Preserve evidence (logs, images)

Containment
* Isolate impacted systems
* Disable compromised accounts
* Apply temporary blocks / firewall rules

Eradication
* Remove malicious artifacts
* Patch vulnerabilities and rotate secrets
* Validate clean system state

Recovery
* Restore services and monitor health
* Validate business workflows
* Communicate status to stakeholders

Post-Incident
* Hold post-mortem and document learnings
* Update detection and response playbooks