Incident Response Quick-Action Plan

Phase 1: Preparation

- ❑ Maintain updated contact list for IR team members
- ❑ Ensure logging and monitoring are functional
- ❑ Define communication channels (secure & out-of-band)
- ❑ Ensure backups are tested and recoverable
- ❑ Pre-build forensic collection tools & playbooks

Phase 2: Identification

- ❑ Detect and validate suspicious activity (EDR/SIEM/alerts)
- ❑ Determine incident type (malware, ransomware, insider threat, data breach)
- ❑ Identify affected hosts, accounts, applications, or cloud resources
- ❑ Classify severity and potential impact
- ❑ Document all initial findings immediately

Phase 3: Containment

Short-term containment:

- ❑ Isolate infected devices from the network
- ❑ Disable compromised accounts
- ❑ Block malicious IPs/domains
- ❑ Stop lateral movement

Long-term containment:

- ❑ Apply temporary firewall rules
- ❑ Patch vulnerabilities related to current incident
- ❑ Change privileged credentials
- ❑ Deploy additional monitoring

Phase 4: Eradication

- ❑ Remove malware or malicious artifacts

- ❑ Terminate malicious processes
- ❑ Delete unauthorized users or applications
- ❑ Patch exploited vulnerabilities
- ❑ Harden misconfigurations exploited by attackers

Phase 5: Recovery

- ❑ Restore clean systems from backups
- ❑ Rebuild servers or systems as needed
- ❑ Gradually reintroduce production systems
- ❑ Monitor systems for reinfection
- ❑ Validate business operations return to normal

Phase 6: Lessons Learned

- ❑ Conduct a post-incident review within 7 days
- ❑ Identify control gaps that allowed the attack
- ❑ Update policies, monitoring, and configurations
- ❑ Strengthen detection/prevention based on findings

Signature: _____
Name: _____
Date: _____