INCIDENT RESPONSE CHECKLIST

A Step-by-Step Guide for Responding to Security Incidents

Created by Jamola Cybersec Services Limited

INTRODUCTION

A security incident can happen at any time. This checklist provides a structured approach to responding to incidents, minimising damage, and restoring normal operations quickly.

INCIDENT SEVERITY CLASSIFICATION

CRITICAL: Active data breach, ransomware, or system compromise

- HIGH: Suspected breach, malware outbreak, or significant data exposure

- MEDIUM: Policy violation, unsuccessful attack attempt

- LOW: Unusual activity, false positive, or minor issue

IMMEDIATE RESPONSE (FIRST 15 MINUTES)

□ 1. DETECTION & REPORTING

- Confirm the incident has occurred

- Document initial observations

Note date/time of detection

- Keep a log of all actions taken

□ 2. RESPONSE TEAM ACTIVATION

- Alert the designated incident response team

- Assign roles (lead, technical, communications)

- Establish communication channels

- Activate external support if needed

□ 3. INITIAL TRIAGE

- Determine severity level

- Assess potential impact

-

- Identify affected systems

- Determine if active attack is ongoing

CONTAINMENT (FIRST 30-60 MINUTES)

□ 4. IMMEDIATE CONTAINMENT

- Disconnect affected systems from network

- Block malicious IP addresses/domains

- Disable compromised user accounts

- Preserve evidence (logs, disk images)

□ 5. SYSTEM ISOLATION

- Quarantine infected systems

- Block network access from affected devices Implement firewall rules if needed

- Disable external access if compromised

□ 6. COMMUNICATION

- Notify executive leadership

- Inform legal and HR if needed

- Prepare initial stakeholder communication

- Do NOT discuss publicly yet

INVESTIGATION (FIRST 2-4 HOURS)

□ 7. EVIDENCE COLLECTION

- Collect system logs

- Capture network traffic

- Take forensic images of affected systems

- Document all findings

□ 8. ANALYSIS

- Identify attack vector/entry point

- Determine scope of compromise

- Identify data or systems affected

-

- Trace attacker activity

□ 9. ROOT CAUSE ANALYSIS

- Identify how the incident occurred

- Determine what vulnerabilities were exploited Identify any failed controls

ERADICATION (WITHIN 4-8 HOURS)

□ 10. REMOVAL OF THREAT

- Remove malware/viruses

- Delete malicious files

- Close exploited vulnerabilities

- Reset all compromised credentials

□ 11. SYSTEM RESTORATION

- Rebuild affected systems

- Restore from clean backups

- Apply security patches

- Verify system integrity

RECOVERY (WITHIN 8-24 HOURS)

□ 12. SYSTEM RECONNECTION

- Reconnect systems gradually

- Monitor for suspicious activity

- Verify normal operation

- Test critical functions

□ 13. POST-RECOVERY ACTIONS

- Change all passwords and keys
- Review and update security controls
- Document lessons learned
- Update incident response plan

POST-INCIDENT

□ 14. INCIDENT REPORTING

- Prepare detailed incident report
- Document timeline of events
- List all actions taken
- Include recommendations

□ 15. COMMUNICATION & NOTIFICATION

- Notify affected parties
- Comply with regulatory requirements
- Notify law enforcement if applicable
- Update stakeholders

□ 16. LESSONS LEARNED

- Conduct post-mortem review
- Identify what went well
- Identify areas for improvement
- Update policies and procedures

□ 17. IMPROVEMENTS

- Implement security improvements
- Provide additional training
- Review and update DR/BCP plans
- Test updated response plan

INCIDENT RESPONSE TEAM CONTACTS

Security Lead: _____

Phone: _____

Technical Lead: _____

Phone: _____

Communications Lead: _____

Phone: _____

Legal Contact: _____

Phone: _____

External Support: _____

Phone: _____

CRITICAL RESOURCES

- Backup Location: _____

- Emergency Documentation: _____

- Alternative Communication: _____

REMEMBER THE 4 KEY PHASES

1. DETECT & RESPOND - Activate your response team immediately

2. CONTAIN & CONTROL - Stop the spread of the incident

3. INVESTIGATE & ANALYSE - Understand what happened

4. RECOVER & LEARN - Restore operations and improve

ABOUT JAMOLA CYBERSEC SERVICES LIMITED

Jamola Cybersec Services Limited provides remote cybersecurity services to SMEs worldwide. We help businesses secure their systems, protect their data, and build resilient security programmes.

Contact: info@jamolacybersec.uk

Website: https://jamolacybersec.uk