Incident Response Quick-Action Plan

Rapid Internal Guide

Contents

1, Introduction

When something goes wrong, speed and clarity are everything. This quick-action plan gives your team the essential steps to follow in the first moments of a potential security incident. Clear actions that help contain the threat, protect evidence, and keep the organisation safe while the incident response process is activated.

Use this guide the moment you suspect unusual activity. When in doubt, treat it as an incident and escalate immediately. Quick action reduces impact, prevents spread, and ensures a clean, effective recovery.

1. Identify the Incident

Act fast and confirm whether what you're seeing is genuinely suspicious:

- Unexpected system shutdowns, freezes, or reboots
- Unknown or unauthorised software running
- Login attempts from unusual locations
- Files encrypted, missing, or modified
- Alerts from security tooling (AV, EDR, SIEM, firewall)
- Reports of phishing, vishing, or social engineering

If there's **any doubt**, treat it as an incident.

2. Contain Immediately

Your first objective is to stop the spread.

- Disconnect affected machines from the network (unplug ethernet / disable Wi-Fi)
- Block suspicious accounts or reset passwords
- Remove access tokens or session keys
- Halt malicious processes if safe to do so
- Disable compromised services or endpoints

Do **not** power off devices unless instructed, evidence may be lost.

3. Preserve Evidence

Good evidence means a faster, cleaner investigation.

- Do not wipe or reinstall anything
- Do not delete suspicious emails or files
- Document every action you take
- Take screenshots of alerts or system behaviour
- Record dates, times, user actions, and system names

This protects the integrity of your investigation.

4. Escalate Immediately

Notify the correct people with *clear, concise information*:

- What happened
- When it was first noticed
- Who reported it
- What systems/users are affected
- What you've done so far

Escalate to:

- Internal IT/security lead
- Line management
- Incident Response team (if applicable)

- External provider (BlackBox Pentesters IR support, if engaged)

Faster escalation = faster containment.

5. Assess the Impact

Determine:

- What systems are affected
- Whether data has been accessed, modified, or exfiltrated
- Whether business operations are impacted
- Whether customer-facing services are affected

This helps prioritise the response effort.

6. Eradicate the Threat

Once evidence is captured and assessment complete:

- Remove malicious files or malware
- Patch vulnerabilities
- Reset/rotate credentials
- Harden affected systems
- Review and tighten access controls
- Implement compensating controls as needed

7. Recover Safely

Bring systems back online in a controlled way:

- Restore from known-good backups
- Monitor systems closely for recurrence
- Validate user access and service availability
- Confirm all patches and mitigations applied

Do not rush recovery, stability matters more than speed.

8. Communicate

Provide updates to:

- Internal teams
- Leadership
- External stakeholders (if required by policy or regulation)

Use approved channels only.

9. Post-Incident Review

Within 24–72 hours:

- Analyse root cause
- Review what worked and what didn't
- Update policies and procedures
- Improve monitoring and alerting
- Conduct team awareness briefings
- Implement long-term security enhancements

Every incident is a chance to strengthen your environment.

Emergency Contacts (Add Internally)

- IT/Security Lead: _____
- IR Team: _____
- Out-of-Hours Contact: _____
- External Support / BlackBox Pentesters: _____