CYBER INCIDENT: FIRST 60 MINUTES

Discover or suspect a cyber incident?

- The first hour is about limiting further harm, protecting evidence, alerting the right people and maintaining essential services.
- Use this checklist immediately and activate your organisation's full Cyber Incident Response Plan.
- Do not wait until you have confirmed an attack.

CONTAIN THE INCIDENT

- Stop using any device or account suspected of being compromised.
- Isolate affected devices from the network where safe to do so.
- Do not wipe, rebuild, restart or switch off affected systems unless directed by IT or the incident response lead.
- Do not reuse potentially compromised accounts or credentials until assessed by IT.

ALERT THE RIGHT PEOPLE

- Contact IT support, your managed service provider (MSP) or incident response provider.
- Inform the business owner, senior manager or designated Incident Lead.
- Involve your data protection, communications and business continuity leads as appropriate.
- Check your emergency contacts directory.

ESTABLISH SAFE COMMUNICATIONS

- Use a trusted phone, separate conference call or approved alternative communication channel.
- Do not rely on potentially compromised email, messaging systems or devices.
- Agree who will coordinate the response and provide updates.

PRESERVE EVIDENCE AND RECORD ACTIONS

- Record when the incident was discovered, what was observed and which systems or accounts may be affected.
- Photograph suspicious messages or screens where safe.
- Preserve relevant logs and information where possible.
- Start an incident log, recording actions, decisions, times and who authorised them.

ASSESS THE IMMEDIATE IMPACT

- Which systems, accounts and essential services are affected?
- Could customers, staff, suppliers or partners be affected?
- Is personal or confidential information at risk?
- Is there a risk of financial loss, fraud or further disruption?
- Consider whether business continuity arrangements are needed.

AGREE PRIORITIES AND NEXT STEPS

- Protect people and essential services.
- Assign responsibility for containment, investigation, communications and recovery.
- Contact your cyber insurer promptly where applicable, following policy requirements.
- Assess whether police, ICO or sector-specific reporting is required.
- Agree when the response team will next review the situation.

EMERGENCY CONTACTS — COMPLETE BEFORE AN INCIDENT

- Incident Lead: _____
- IT / MSP emergency number: _____
- Cyber insurer / response provider: _____
- Senior decision-maker: _____
- Alternative communication method: _____

IMPORTANT: This checklist supports immediate action. It does not replace your organisation's Cyber Incident Response Plan, business continuity arrangements or specialist incident response advice. Technical containment and recovery decisions should be coordinated with appropriately qualified personnel.