# Incident response card

Fill this in before you need it. In an incident, the person reading it will be stressed, keep it short, specific and current.

Business

Plan owner / decision-maker

Deputy decision-maker

Last reviewed

## FIRST 60 MINUTES

1. Stop the spread: disconnect affected devices from the network, but do not power them off.
2. Call the incident lead. If unavailable, call the deputy. Record the time.
3. If money has moved, call the bank's fraud line immediately and quote the transaction.
4. Call the insurer's incident line before engaging your own IT forensics.
5. Preserve evidence: do not delete emails, rebuild machines or wipe accounts yet.
6. Agree who talks to staff, customers and suppliers, and what they say.
7. Report to the relevant authority and log the crime / incident reference.

## CONTACTS

| ROLE | NAME | NUMBER | NOTES |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## DO NOT

- ☐ Do not pay a ransom without advice from your insurer and a specialist.
- ☐ Do not email the suspected attacker from the affected mailbox.
- ☐ Do not restore backups until you know how the intruder got in.
- ☐ Do not post details on social media or speculate publicly.

## INCIDENT LOG

Time detected

Detected by

What we know

Actions taken

## DECISIONS AND TIMELINE



Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

### Printing tips

Use A4 portrait, 100% scale, and turn off headers and footers for the cleanest result. Keep a printed copy somewhere you can reach without email or the shared drive.