Simple Incident Response Plan Template

This quick-start plan is designed to be actionable, not overwhelming.

# How to Use This Template

* Dotted lines are for you to fill in ahead of time; like key contacts, roles, and pre-assigned responsibilities. These fields help your team respond faster and with less confusion during a real incident.
* Checkboxes are there to guide your actions during a live incident. They give you a simple, clear path to follow when time is tight and stress is high.

*Keep this document saved in a shared folder and print a copy for your office or team hub. Make sure everyone knows where to find it and what to do.*

We recommend reviewing and updating it at least once a year or when your team, systems, or tools change.

# 1. Who Takes Charge

Incident Response Lead:

…………………………………………………………………………………………………………………………

Backup Contact (if unavailable):

…………………………………………………………………………………………………………………………

# 2. What to Isolate Immediately

☐ Disconnect affected device(s) from the network
☐ Disable compromised user account(s)
☐ Take screenshots or save evidence (logs, error messages)
☐ Notify IT support or technical contact (if applicable)

# 3. Who to Inform Internally

☐ Senior manager / owner

…………………………………………………………………………………………………………………………
☐ All affected employees
☐ Relevant departments (e.g., finance, HR)

…………………………………………………………………………………………………………………………

# 4. What to Record

Date & time incident was discovered

…………………………………………………………………………………………………………………………

How it was detected (email, alert, user report)

…………………………………………………………………………………………………………………………

 What systems/data may be affected

…………………………………………………………………………………………………………………………

What actions were taken immediately

…………………………………………………………………………………………………………………………

# 5. Who to Inform Externally (if needed)

☐ Customers or clients

…………………………………………………………………………………………………………………………
☐ External IT providers

…………………………………………………………………………………………………………………………
☐ Legal or data protection contact

…………………………………………………………………………………………………………………………

☐ Cyber insurance provider (if applicable)

…………………………………………………………………………………………………………………………
☐ Information Commissioner’s Office (UK GDPR/reportable breaches only)

…………………………………………………………………………………………………………………………

# 6. What Happens Next

Investigate root cause (e.g., phishing, software vulnerability)

…………………………………………………………………………………………………………………………
☐ Reset passwords if necessary
☐ Apply updates or patches
☐ Consider staff awareness refresher

Review what went well and what can improve

…………………………………………………………………………………………………………………………

…………………………………………………………………………………………………………………………