Data Recovery | Computer Forensics | Cyber Security

DIGITAL INCIDENT INITIAL RESPONSE CHECKLIST

A practical worksheet for recording the facts, protecting potential evidence and organising an expedited response.

0800 328 2522 | www.datalab.co.nz

CONFIDENTIAL

FIRST: A FEW IMPORTANT RULES

- Do not delete, edit, reset, reinstall, factory-reset or run cleanup tools on potentially relevant devices or accounts unless necessary to contain an immediate risk or advised by your incident lead / forensic specialist.
- Do not forward, rename, re-save or repeatedly open potential evidence unnecessarily. Keep original messages, files, devices and records where possible.
- Do not share passwords, recovery codes or MFA codes in this worksheet or by ordinary email. Arrange secure access through an agreed process.
- Record facts separately from assumptions. Use exact dates and times where known; state known facts clearly and flag any assumptions.
- Limit access to this worksheet and incident material to people who need it. Keep a record of who receives copies.
- If there is an immediate safety risk, active financial theft or ongoing compromise, prioritise safety and containment. Evidence preservation should not delay urgent protective action.

This checklist is an initial information-gathering aid, not a substitute for legal advice, an incident response plan or forensic preservation. Complete what you can; leave unknown items blank. Do not delay urgent safety or containment actions to complete it.

1. INCIDENT OVERVIEW

Organisation / individual affected

_____

Incident name / reference

_____

Incident owner (person coordinating the response)

_____

Incident owner Email and Ph;

_____

Date and time first identified

Date: _____ Time: _____

Date and time incident may have started

Date: _____ Time: _____ ☐ Known ☐ Estimated ☐ Unknown

How was it discovered?

☐ Staff report ☐ Customer report ☐ Security alert ☐ Audit/log review

☐ Other: _____

Current status

☐ Ongoing ☐ Contained ☐ Resolved / stopped ☐ Unknown

Brief description (what is known so far?)

_____

_____

2. PEOPLE AND ORGANISATIONS INVOLVED

People who may be involved or affected

Name / role / organisation / contact details:

_____

_____

_____

Key internal contacts

IT / security: _____ PH:

Management: _____PH:

External parties

☐ IT provider ☐ Cloud / platform provider ☐ Insurer ☐ Other: _____

Legal counsel notified?

☐ Yes ☐ No ☐ Not yet decided Name / firm: _____

Date / time notified and advice received

_____

_____

_____

_____

_____

CONFIDENTIAL

3. ACCOUNTS, SYSTEMS AND SERVICES

Record each relevant account or service

Service / provider | Account or user identifier | Owner | Relevant dates / activity

_____

_____

_____

Examples

☐ Microsoft 365 ☐ Google Workspace / Drive ☐ Email ☐ Social media
☐ Messaging apps ☐ Cloud storage / backup ☐ Website / hosting ☐ Other

Access concerns

☐ Unknown login ☐ Password changed ☐ MFA issue / reset ☐ Session still active
☐ Account locked ☐ Access revoked ☐ Data shared externally ☐ Other: _____

Do not record passwords or MFA codes

Record the account identifier and the nature of the access issue only.

4. DEVICES, STORAGE AND PHYSICAL ITEMS

Record each relevant item

Device / asset | Make / model | Serial / asset number | User / custodian | Location

_____

_____

_____

_____

_____

Items potentially involved

☐ Desktop / laptop ☐ Mobile phone / tablet ☐ USB / external drive
☐ Server / NAS ☐ CCTV / recorder ☐ Network equipment ☐ Other: _____

Current condition

☐ In use ☐ Powered on ☐ Powered off ☐ Damaged ☐ Missing ☐ Unknown

Where is each item now, and who has control of it?

_____

_____

CONFIDENTIAL

5. WHAT HAPPENED? — INCIDENT TIMELINE

Record events in time order. Use local time and include the time zone. Mark estimates as estimates.

Date / time	Event / observation (separate what was seen from what is suspected)

Sources for the information

☐ Direct observation ☐ User report ☐ Email / message ☐ System log ☐ Alert
☐ Screenshot / photo ☐ Other: _____

6. DATA AND EVIDENCE TO PRESERVE

Potentially relevant information

☐ Emails ☐ Messages / chats ☐ Files / documents ☐ Shared links / permissions
☐ Audit logs ☐ Login / access logs ☐ Browser history ☐ Photos / video
☐ CCTV ☐ Call / location records ☐ Backups ☐ Other: _____

Where is it held?

Device / account / platform / folder / custodian:
_____
_____

Could it be lost or changed?

☐ Auto-deletion / retention policy ☐ Expiring messages ☐ Account closure
☐ Device being reused / reset ☐ Remote wipe risk ☐ Unknown ☐ Other: _____

Preservation actions already taken

What was done, by whom, and when?
_____
_____

Evidence location / reference

CONFIDENTIAL

File name, export name, ticket number, storage location or other reference:
_____

7. ACTIONS TAKEN AND NOTIFICATIONS

Actions already taken

☐ Password reset ☐ MFA enabled / changed ☐ Sessions revoked
☐ Account disabled ☐ Device disconnected ☐ Device powered off
☐ Files copied / exported ☐ Provider contacted ☐ Other: _____

For each action, record

Action: _____ By: _____
Date / time: _____ Reason: _____

Notifications / reporting

☐ Management ☐ Legal counsel ☐ Insurer ☐ IT provider
☐ Platform / cloud provider ☐ Police ☐ CERT NZ ☐ Privacy Officer
☐ Affected people / customers ☐ Regulator ☐ Other: _____

Notification details / reference numbers

Who was notified, when, how, and any reference number:
_____
_____

8. IMPACT AND PRIORITIES

Potential impact (tick any that may apply)

☐ Personal / sensitive information ☐ Commercially confidential information
☐ Intellectual property ☐ Financial loss / fraud ☐ Service disruption
☐ Safety / welfare ☐ Legal proceedings ☐ Reputational impact ☐ Unknown

What needs attention first?

☐ Stop ongoing unauthorised access ☐ Protect people / safety
☐ Preserve volatile or time-sensitive evidence ☐ Maintain critical services
☐ Identify affected data / people ☐ Meet legal or reporting deadlines

Known deadlines or time limits

_____

9. HANDOVER TO DATA LAB / FORENSIC TEAM

What assistance is requested?

☐ Triage / incident scoping ☐ Device preservation / examination ☐ Mobile forensics
☐ Cloud / account investigation ☐ Data recovery ☐ Timeline reconstruction
☐ Evidence review / independent analysis ☐ Expert report / affidavit ☐ Other

Key questions you need answered

1. _____
2. _____
3. _____

Available material to provide

☐ Incident timeline ☐ Account / device list ☐ Relevant correspondence
☐ Existing exports / logs ☐ Screenshots ☐ Policies / authorisations
☐ Other: _____

CONFIDENTIAL