Cybersecurity Incident Response Checklist

Safety & Compliance

INCIDENT DATE/TIME	INCIDENT ID	REPORTED BY	INCIDENT LEAD	SEVERITY

DETECTION & INITIAL ASSESSMENT

How was the incident detected _____

Type of incident _____

- [ ] Systems/data affected identified
- [ ] Scope of impact assessed (users, systems, data)

Severity level assigned [ ] Critical [ ] High [ ] Medium [ ] Low

- [ ] Incident response team activated

CONTAINMENT

- [ ] Affected systems isolated from network
- [ ] Compromised accounts disabled

Firewall rules updated to block threat [ ] Done [ ] N/A

- [ ] Evidence preserved (logs, disk images, memory dumps)
  Do NOT shut down — image live systems first if possible
- [ ] Backup integrity verified (not compromised)

Threat still active? [ ] No — contained [ ] Yes — escalate

ERADICATION

Root cause identified _____

	DONE	IN PROGRESS	N/A
Malware removed from all affected systems	○	○	○
Vulnerability patched / closed	○	○	○

- [ ] Compromised credentials reset
- [ ] All indicators of compromise (IOC) checked across environment

No additional compromise found [ ] Confirmed [ ] Still Investigating

RECOVERY

Systems restored from clean backups [ ] Done [ ] In Progress [ ] N/A

- [ ] Systems patched and hardened before reconnecting
- [ ] Monitoring increased on restored systems
- [ ] Users re-enabled with new credentials

Normal operations resumed [ ] Yes [ ] Partial [ ] Not Yet

Go digital with Miratag

Skip the paper — fill checklists faster on the Miratag mobile app. Add photos, videos, notes and signatures. Track compliance in real time. Start free at miratag.com

This template is a general-purpose resource, not tailored to any specific jurisdiction. Each organisation must validate compliance with local regulations.

Scan to view

Time to recovery _____

COMMUNICATION

- [ ] Management / executives notified

Legal counsel consulted ☐ Yes ☐ Not Required

Affected users / customers notified ☐ Yes ☐ Pending ☐ Not Required

Regulatory notification required ☐ Yes — filed ☐ Yes — pending ☐ No

	YES	NOT REQUIRED
Insurance company notified	○	○
Law enforcement notified	○	○

POST-INCIDENT REVIEW

- [ ] Timeline of events documented
- [ ] Root cause analysis completed
- [ ] Lessons learned documented

Preventive measures identified

Incident response plan updated ☐ Yes ☐ No Changes Needed

Incident lead signature _____

Notes

Go digital with Miratag

Skip the paper — fill checklists faster on the Miratag mobile app. Add photos, videos, notes and signatures. Track compliance in real time. Start free at miratag.com

This template is a general-purpose resource, not tailored to any specific jurisdiction. Each organisation must validate compliance with local regulations.

Scan to view