Incident response checklist

Keep this beside your response plan. Agree owners and contact details before you need them.

Adapt these steps to the incident and your environment. Your incident lead should coordinate containment and evidence handling.

Prepare

- ☐ Name an incident lead, a deputy, and an approved way to reach them outside your usual systems.
- ☐ Record your IT provider, insurer, and key system contacts. Keep an offline copy.
- ☐ Agree who can isolate systems, approve recovery, and communicate with customers.

Assess and contain

- ☐ Record what happened, when it was noticed, and the systems or people affected.
- ☐ Notify your incident lead using a trusted channel. Avoid sending sensitive details through a potentially compromised account.
- ☐ With your technical lead, isolate affected devices from the network where appropriate. Avoid wiping or rebooting before evidence is considered.
- ☐ Preserve relevant alerts, logs, and a timeline of decisions in a restricted location.

Recover and learn

- ☐ Address the cause and verify that systems are ready before restoring trusted backups or reconnecting.
- ☐ Review whether affected credentials, sessions, or tokens need to be revoked or replaced.
- ☐ Assign an owner to assess contractual and applicable reporting duties, and coordinate communications.
- ☐ Monitor for recurrence. Record lessons, owners, and improvements to your response plan.

Owner: _____ Reviewed: _____

Further reading

CISA: #StopRansomware Guide