First-week cybersecurity checklist

Assign a person to each task. Check it off when the verification passes.

Business or team _____ **Week of** _____ **Accountable lead** _____

Task | **Owner role and name**

☐ **Assign leads and list critical workflows** — **Business owner** _____

Do. Name leads for IT, finance and incident response. List the workflows the business must keep running.

Verify. Check that each workflow has a named owner, a support contact and a list of its key systems.

☐ **Keep emergency contacts available offline** — **Incident lead** _____

Do. Save trusted numbers for the incident lead, backup, IT provider and bank fraud line. Agree on a backup channel.

Verify. In a drill, ask a staff member to find the list and reach the incident lead without company email.

☐ **Secure priority accounts** — **IT lead or provider** _____

Do. Require phishing-resistant sign-in, such as passkeys or security keys, for priority accounts where supported.

Verify. Check enforcement for admin, email, remote access, backup and finance. Test sign-in and recovery with a pilot account.

☐ **Triage urgent internet-facing risks** — **IT lead or provider** _____

Do. List public websites, VPNs and gateways. Check vendor advisories and apply urgent fixes or approved mitigations.

Verify. Check versions or controls after changes. Record each remaining high-risk item with an owner and due date.

☐ **Verify supplier payment changes** — **Finance lead** _____

Do. Hold payments with changed bank details until you call a supplier number already on file and a second person approves.

Verify. Rehearse a mock supplier change. Confirm both checks were recorded before any payment would be released.

☐ **Restore one critical record** — **Recovery owner** _____

Do. Restore a recent critical file or record into an approved test environment.

Verify. A business user opens it and checks its contents and date against a known record. Save the result and any gaps.

Gaps to close

Action, owner and due date

_____

_____