Last reviewed: _____

Backups & Continuity

- Follow **3-2-1**: primary + **2 backups** (one **offline/offsite**); **encrypt** backups.
- Run and verify this month's **backup jobs**; perform a **small test restore**.
- Keep printed copies of the **incident response plan** and **key contacts** in a safe place.

Access, Patching & Protection

- Enforce **MFA** on email, payroll/banking, VPN, and all admin portals; **disable old accounts**.
- Patch **OS/apps** on endpoints/servers; update **router/NAS/Wi-Fi** firmware.
- Verify **EDR/antivirus** is running and updating on every device; review today's detections.
- Disable **exposed RDP/SSH**; require **VPN + MFA**; disable **UPnP**; separate **guest Wi-Fi**.

Email, SaaS & Web

- Tighten email: block **executables**, limit **macros**; verify **SPF/DKIM/DMARC**.
- Export/backup critical **SaaS data** (accounting/CRM); confirm **admin roles/SSO**.
- Back up **website** and **DNS registrar** settings; store recovery codes safely.

Awareness & Vendors

- Send a **10-minute security tip** to staff and run a **quick phishing simulation**; log completions.
- Check **status pages/advisories** for key vendors/MSP; record actions needed.

Monthly Notes / Follow-ups