VIDA ICT SOLUTIONS

Security Baseline Checklist

Twenty-two controls that stop most incidents, in priority order

How to read this

Work top to bottom. Each control is ordered by how much risk it removes per unit of effort. If you do nothing else this quarter, do the first six. They address the failure modes behind the large majority of incidents we are called to clean up.

Tier 1 • Do this month

- Enable two-factor authentication on email, banking, domain registrar and any admin panel. Use an authenticator app, not SMS, where offered.
- Back up critical data automatically to a destination the everyday machines cannot write to, and run one documented restore test.
- Inventory every account with access to business systems; disable anything belonging to people who have left.
- Replace shared passwords with a password manager and unique passwords per system. Revoke the old shared ones.
- Turn on full-disk encryption on every laptop that leaves the building.
- Patch operating systems and browsers automatically; reboot on the schedule the vendor sets.

Tier 2 • Do this quarter

- Separate admin accounts from daily-use accounts on servers and workstations.
- Put a verified second-person check on every emailed payment or bank-detail change request.
- Enable audit logging on your core systems and confirm someone reviews it monthly.
- Restrict remote access to named devices or a VPN; close anything reachable from the whole internet that does not need to be.
- Document an incident plan: who decides, who communicates, where the backups and credentials live, which lawyer and insurer to call.
- Run one phishing simulation and one short awareness session; measure the click rate before and after.

Tier 3 • Do this half-year

- Classify your data into public, internal and confidential; apply access rules per class.
- Review third-party processors: what data leaves your organisation, to whom, under what agreement.
- Test restore of your most critical system end to end, timed, and record the result against a recovery-time target.
- Establish change control for production systems: no unreviewed change, however small.