

Security checks for your organisation

Reviewed: 2026-10-07

Use this checklist with the people who manage your systems. Record what is in place, what evidence is available and who will follow up. It is a discussion aid, not an audit or proof of compliance.

Checks to work through

1. Identify the systems and records your organisation relies on.
2. Check who has access, including administrators, former staff and suppliers.
3. Confirm where multifactor authentication is enabled and how accounts are recovered.
4. Check that devices receive supported security updates and have appropriate protection.
5. Establish what is backed up, who can access the backups and when restoration was last tested.
6. Confirm how staff report suspicious messages or unexpected activity.
7. Identify who coordinates a security incident and how they can be reached if email is unavailable.
8. Review how changes to supplier payment details are independently verified.

Record the follow up

For each uncertainty, note the question, the person responsible and the next action. Keep internal records in an approved location. Do not put passwords, account recovery codes or confidential documents into a general enquiry form.

Start the complimentary Pre-Assessment (<https://www.cyberxperts.co.za/security-pre-assessment>) for an indicative view of your current practices. For a scoped review, explore Risk Assessments (<https://www.cyberxperts.co.za/services/risk-assessments>).

The fictional backup recovery scenario (<https://www.cyberxperts.co.za/resources/backup-recovery-scenario>) explains what a restoration exercise should establish.

Further reading

NCSC guidance for small organisations (<https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security>) covers account, device and backup protection.