

Preparing your organisation for a security incident

Reviewed: 2026-10-07

Use this guide before an incident to agree who does what. The plan should fit your systems, responsibilities and business priorities.

Prepare the plan

1. Name an incident coordinator and a deputy.
2. Keep an accessible contact list for technical support, management and relevant suppliers.
3. Agree a way to communicate if normal email or systems are unavailable.
4. Identify the services that need to recover first and the dependencies they require.
5. Decide how incident records and evidence will be collected, protected and accessed.
6. Identify who will assess contractual, privacy and reporting obligations.
7. Run a discussion exercise and record unclear responsibilities or missing information.
8. Update the plan after exercises, significant system changes and incidents.

If an incident is already under way

Contact your responsible technical team or response provider directly. Coordinate containment and recovery with qualified responders. Record what was observed and actions taken. Avoid deleting or altering potential evidence without appropriate guidance. Keep passwords and confidential records out of public forms.

Explore Incident Response (<https://www.cyberxperts.co.za/services/incident-response>) or contact our team (<https://www.cyberxperts.co.za/contact>). For a general review of preparedness, use the complimentary Pre-Assessment (<https://www.cyberxperts.co.za/security-pre-assessment>).

The fictional business mailbox scenario (<https://www.cyberxperts.co.za/resources/account-misuse-scenario>) shows why account misuse needs a coordinated response.

Further reading

NIST incident response guidance (<https://csrc.nist.gov/pubs/sp/800/61/r3/final>) explains preparation, response and recovery. It is technical guidance, not a statement of South African legal requirements.