

Small-Team Digital Safety Toolkit

Jefferson Otonbara Imgbi | RDE Digital Digest
Version 1.0 • 8 October 2026

Purpose and audience

Create an owned review of important accounts, recovery arrangements and routine digital-safety actions.

Small teams organising their own digital-safety checks with an authorised administrator.

Use the tools in sequence

1. Identify important services and name an owner for each. Record references, never passwords or recovery codes.
2. Review available account protections and recovery contacts with the service owner.
3. Plan a recovery exercise using a harmless practice file and an approved backup location.
4. Record actions and review dates. Escalate a suspected incident through the organisation's established route.

Files and working method

Save a personal copy of the Word file to type into the forms. Use the PDF as a printable version. The PDF has no interactive form fields. Duplicate a tool page when you need more records. Retain the same record IDs across the three tools and record the date and version when you make a change.

These organising forms do not replace incident response, specialist advice or a security assessment. Follow your organisation's approved procedures.

Tool 1: Service and account review

Use A01, A02 and similar IDs. Check available protections with official service guidance and the authorised administrator.

Record date: _____ Version: _____

Service ID, purpose and accountable owner

Authorised users and access review date

Passkey or multi-factor option reviewed

Recovery contact checked and secure reference location

Departed user access and update arrangements

Action, owner and due date

Tool 2: Practice recovery record

Use non-sensitive practice data. Do not delete production files or disconnect systems to perform this exercise.

Record date: _____ Version: _____

Exercise ID and linked service ID

Practice file and approved backup location

Person authorised to perform the exercise

Recovery steps followed and date

Recovered file opened and contents compared

Failure, corrective action and next test

Tool 3: Safety action and contact sheet

Keep this record in an approved shared location. Store secrets elsewhere using the approved secure method.

Record date: _____ Version: _____

Action ID and linked service or exercise

Issue, priority and reason

Action owner, due date and completion evidence

Known official support or internal reporting route

Reviewer and next review date

Completed action and residual issue

Worked example

Fictional example for practice. Adapt the structure, not the facts.

A01 is a fictional team's shared document service. The owner checks the supported sign-in protections and confirms who can recover access. R01 restores a non-sensitive practice file from the approved backup and compares its contents. The file opens but one paragraph is missing, so action T01 asks the owner to review the backup timing and repeat the exercise. The contact sheet stores an internal support route, not credentials.

Review your completed pack

Are important services owned, recovery exercises evidenced and outstanding actions assigned without exposing secrets?

- All three tools use matching record IDs.
- Facts and assumptions are distinguishable.
- Outstanding actions have an owner and a date.
- Confidential information and credentials are excluded.
- The next reviewer can find the supporting evidence.

Your next action

Action: _____

Owner: _____ Due date: _____

Completion evidence: _____

Use and attribution

Original RDE educational forms. Personal and internal organisational adaptation permitted with Jefferson Otonbara Imgbi author credit retained. Review the adapted forms for your context before use.

Further guidance

NCSC: Small organisations guide to cyber security: <https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security>