

MFA and Account Recovery Checklist

Mark a check after reviewing the evidence. Assign open items an owner and date. This is a planning aid, not a certification.

☐ 01 List the accounts with the biggest impact

Identify email, administrator, finance and other business-critical accounts. Include the owner and the service used for account recovery.

Evidence: A prioritized account list without passwords or recovery codes.

Owner

Target date

☐ 02 Choose the strongest supported method

Evaluate phishing-resistant passkeys or FIDO-based security keys where supported. Check device compatibility, user verification and your organization's access policies.

Evidence: A documented method selected for each service.

Owner

Target date

☐ 03 Plan enrolment before enforcement

Confirm who assists users, how approved devices are registered and how access is recovered if enrolment goes wrong.

Evidence: An enrolment and support plan.

Owner

Target date

☐ 04 Check coverage account by account

Confirm that MFA is actually enabled for the intended users and administrators. Assign an owner to services that cannot support it.

Evidence: A service-side coverage report and an exception list.

Owner

Target date

☐ 05 Keep passwords unique where required

Use a different strong password for each service that still needs one. Use an approved password manager and protect access to it.

Evidence: An agreed password-management process.

Owner

Target date

☐ 06 Review sign-in prompt behaviour

Teach people to reject unexpected prompts and report them using a trusted contact method. Never share one-time sign-in codes with someone requesting them.

Evidence: A short instruction included in team guidance.

Owner

Target date

MFA and Account Recovery Checklist

Continue the review. Record the result, including gaps and decisions that need follow-up.

☐ 07 Register an approved backup method

Where the service supports it, arrange a second authorized method or spare security key. Confirm who may use it and under what conditions.

Evidence: A recovery-method inventory that excludes secret values.

Owner

Target date

☐ 08 Secure recovery information

Protect recovery codes and administrator recovery details in approved storage. Make sure recovery does not depend entirely on the account or device being recovered.

Evidence: A documented storage and access process.

Owner

Target date

☐ 09 Rehearse a lost-device scenario

Use the provider's supported process to review how a lost authenticator is reported, access restored and the old method removed. Coordinate any live test with IT.

Evidence: A recorded walkthrough and owner for unresolved gaps.

Owner

Target date

☐ 10 Protect the devices holding credentials

Keep authenticator devices and passkey stores updated and secured with an appropriate screen lock. Review the account that synchronizes credentials.

Evidence: Device and credential-store protection settings reviewed.

Owner

Target date

☐ 11 Remove access when roles change

Review old accounts, registered authenticators and supplier access through your offboarding process. Follow current vendor instructions when compromise is suspected.

Evidence: An offboarding and account-change record.

Owner

Target date

☐ 12 Set a recurring review date

Revisit service compatibility, recovery ownership and exceptions when staff, devices or important applications change.

Evidence: A review owner and next review date.

Owner

Target date

Turn checks into next steps.

For routine account-security planning. Follow the service provider's current setup and recovery instructions; avoid changes that could lock out the team.

YOUR BUSINESS REVIEW

Review led by Date

Next review

NEXT THREE ACTIONS / OWNER / TARGET DATE

Sources and scope

Cyber Centre: Multi-factor authentication (ITSAP.30.030)

<https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030>

Cyber Centre: Passkey considerations (ITSAP.30.033)

<https://www.cyber.gc.ca/en/guidance/cyber-security-considerations-passkeys-itsap30033>

Cyber Centre: Foundational security actions (ITSAP.10.300)

<https://www.cyber.gc.ca/en/guidance/foundational-cyber-security-actions-small-organizations-itsap10300>

Prepared by Canada NexTech. Source guidance checked October 28, 2026. This independent educational resource is not endorsed by the source organizations. Adapt it with the person responsible for your systems.