MFA Account Tracking Sheet

Record MFA status, recovery ownership, device reviews, exceptions, and next review dates.

Version 1.0 · Updated: October 2026 · Published by Cintherian

Safety note

Record account-management information only. Do not write passwords, authentication codes, recovery codes, API keys, private keys, access tokens, or other secrets in this document.

Organization details

Organization _____ **MFA tracking owner** _____

Technical contact _____ **Review period** _____

Tracking start date _____ **Next full review** _____

MFA status legend · use one status consistently

Complete · MFA enabled and verified. In progress · enrollment started, not complete. Exception · MFA unavailable or deferred with approval. Review · MFA exists but recovery, devices, or ownership need review. Not applicable · the account does not support human MFA or uses another approved control. Unknown · information not yet confirmed.

Account tracking table

One row per account or service. Repeat the table over several pages rather than crowding one page.

#	SERVICE	OWNER	ADMIN	DATA HELD	METHOD	STATUS	VERIFIED	REVIEW

Detailed account record

Use this page for high-risk accounts: email, identity providers, password managers, financial systems, domain accounts, and

infrastructure accounts.

Identification

Service _____ **Account / workspace** _____

Account URL _____ **Business purpose** _____

Account owner _____ **Administrator** _____

Backup administrator _____ **Current plan / type** _____

Risk priority _____ **Sensitive data / capability** _____

MFA configuration

MFA enabled _____ **MFA method** _____

Backup method _____ **Enrollment date** _____

Last verified _____ **Next review** _____

Registered devices reviewed _____ **Active sessions reviewed** _____

Connected applications reviewed _____

Recovery information

Do not write recovery codes, passwords, keys, or tokens here.

Recovery owner _____ **Backup recovery owner** _____

Recovery process location _____ **Recovery test date** _____

Recovery test result _____

Access and ownership review

- ☐ Owner confirmed
- ☐ Administrator confirmed
- ☐ Backup administrator confirmed
- ☐ MFA enabled
- ☐ Backup method confirmed
- ☐ Recovery process documented
- ☐ Recovery tested
- ☐ Registered devices reviewed
- ☐ Active sessions reviewed
- ☐ Connected applications reviewed
- ☐ Old devices removed
- ☐ Former users removed
- ☐ Next review scheduled

Notes and follow-up

_____

_____

_____

_____

User enrollment tracking

Use C = Complete, I = In progress, E = Exception, R = Review, N/A = Not applicable, ? = Unknown.

PERSON	ROLE	EMAIL	PWD MGR	FINANCE	CLOUD	CLIENT SYS	STATUS

Device and key register

Do not record passwords or secret codes.

PERSON	DEVICE / KEY	ACCOUNT / SERVICE	REGISTERED	LAST REVIEWED	LOST / REPLACED?	REMOVED?	NOTES

Device-review checklist

- ☐ Device belongs to the named person
- ☐ Device current and supported
- ☐ Old devices removed
- ☐ Replaced keys removed
- ☐ Device protected by a screen lock
- ☐ Device still required
- ☐ Lost devices revoked
- ☐ Ownership documented

Recovery review log

Do not record the actual recovery code or secret.

DATE	SERVICE	TESTED BY	METHOD USED	RESULT	FOLLOW-UP	NEXT TEST

MFA exception register

An exception without an owner or expiration date is treated as incomplete.

SERVICE	REASON	RISK	COMPENSATING CONTROL	OWNER	APPROVED BY	TARGET DATE	EXPIRES

Service-account and integration register

Use a reference such as "password manager / Operations / Integrations", not the actual credential.

SERVICE / ACCOUNT	OWNER	PURPOSE	PERMISSION LEVEL	CREDENTIAL REFERENCE	ROTATION DATE	LAST REVIEWED	STATUS

Monthly or quarterly review page

Review period _____ **Reviewer** _____

Date _____ **Accounts reviewed** _____

Accounts complete _____ **Accounts requiring action** _____

Exceptions reviewed _____ **Devices reviewed** _____

Recovery methods reviewed _____ **Service accounts reviewed** _____

Former users removed _____ **Next review date** _____

Review checklist

- ☐ MFA coverage checked
- ☐ Recovery methods checked
- ☐ Old phone numbers removed
- ☐ Unexpected prompts reviewed
- ☐ Service accounts reviewed
- ☐ New applications added
- ☐ Follow-up owners assigned
- ☐ Administrator access checked
- ☐ Registered devices checked
- ☐ Former users removed
- ☐ Connected applications reviewed
- ☐ Exceptions reviewed
- ☐ Departed users removed
- ☐ Next review scheduled

Follow-up actions

ACTION	OWNER	DUE DATE	COMPLETION DATE	VERIFIED BY

Start here

Start with business email, the identity provider, password manager, financial systems, and administrator accounts. Then review cloud storage, client platforms, backups, and the remaining business applications.

Companion resources: MFA Rollout Checklist · Employee Offboarding Checklist · Small-Business Software Audit · SaaS Renewal Audit · cintherian.com/how-we-test