Small-Business MFA Rollout Checklist

A practical implementation guide for protecting email, administrators, financial systems, cloud storage, and client platforms.

For small agencies, consultants, professional-service businesses, and remote teams.

Version 1.0 · Updated: October 2026 · Published by Cintherian

This checklist is general security guidance. It is not a complete security audit, compliance certification, incident-response plan, or substitute for professional advice. Do not record passwords, MFA codes, recovery codes, API keys, access tokens, or other secrets in this document.

How to use this checklist

- ☐ List important accounts and systems.
- ☐ Protect high-risk accounts first.
- ☐ Record recovery arrangements without recording secrets.
- ☐ Document exceptions and assign expiration dates.
- ☐ Assign one accountable owner to each account.
- ☐ Choose the strongest supported MFA method.
- ☐ Test enrollment and recovery.
- ☐ Review the checklist after staffing or system changes.

Suggested completion order

- ☐ Business email and identity provider
- ☐ Password manager
- ☐ Financial and payment systems
- ☐ Administrator and infrastructure accounts
- ☐ Cloud storage and client systems
- ☐ Other business applications
- ☐ Service accounts and integrations

Section 1 · Organization profile

Organization _____ **Primary contact** _____

MFA rollout coordinator _____ **Technical owner** _____

Review owner _____ **Rollout start date** _____

Target completion date _____ **Next scheduled review** _____

Number of employees _____ **Number of contractors** _____

Primary identity provider _____ **Primary email platform** _____

Password manager _____

Scope · check all that apply

- ☐ Business email
- ☐ Banking and finance
- ☐ Cloud storage
- ☐ Domain and DNS
- ☐ Cloud infrastructure
- ☐ Device management
- ☐ Identity provider
- ☐ Accounting and payroll
- ☐ Project management
- ☐ Website and hosting
- ☐ Backup systems
- ☐ Advertising platforms
- ☐ Password manager
- ☐ Payment processing
- ☐ CRM and client portals
- ☐ Code repositories
- ☐ VPN and remote access
- ☐ Social-media accounts

Section 2 · Risk-priority inventory

Use one line per account or service.

PRIORITY	ACCOUNT / SERVICE	OWNER	ADMINISTRATOR	DATA / CAPABILITY

Priority guide

1 · Email, identity provider, password manager. 2 · Finance, payment, payroll, administrators. 3 · Domain, DNS, hosting, cloud, backup, code repositories. 4 · Client data, project management, CRM, file storage. 5 · Other business applications.

Section 3 · Administrator account checklist

Complete for each important administrator account.

Service _____ **Administrator account** _____

Named administrator _____ **Separate daily-use account** _____

Backup administrator _____ **MFA enabled** _____

Preferred MFA method _____ **Recovery process documented** _____

Recovery test date _____ **Last privilege review** _____

Next privilege review _____

Administrator controls · check all

- ☐ Every administrator uses MFA
- ☐ Shared administrator passwords are not used
- ☐ Administrator accounts separate from ordinary accounts
- ☐ At least two approved administrators can recover the service
- ☐ Unnecessary administrator privileges removed
- ☐ Recovery phone numbers current
- ☐ Old devices and keys removed
- ☐ Emergency access documented
- ☐ Recovery email addresses current
- ☐ Registered devices reviewed
- ☐ Recovery tested
- ☐ Administrator access reviewed at least quarterly

Section 4 · MFA method decision

SERVICE	STRONGEST SUPPORTED	SELECTED METHOD	REASON	BACKUP METHOD	OWNER

SERVICE	STRONGEST SUPPORTED	SELECTED METHOD	REASON	BACKUP METHOD	OWNER
(continued)					

Method guidance (strongest first)

1 · Passkey 2 · Hardware security key 3 · Authenticator application 4 · Hardware token 5 · SMS or voice code, only when stronger methods are unavailable. Best choice depends on the provider, recovery process, devices, accessibility needs, and your organization?s ability to manage the method.

Section 5 · User enrollment checklist

Before enrollment

- ☐ Account owner confirmed
- ☐ Instructions sent through an approved channel
- ☐ User knows not to share authentication codes
- ☐ Backup method approved
- ☐ Correct account and workspace identified
- ☐ User can report unexpected prompts
- ☐ Recovery process available
- ☐ Personal-device requirements reviewed

During enrollment

- ☐ MFA method registered
- ☐ Backup method registered
- ☐ User completes a fresh-login test
- ☐ Device or key name recorded
- ☐ Recovery information confirmed
- ☐ User knows how to report a lost device

After enrollment

- ☐ Enrollment visible in the administrator dashboard
- ☐ User listed as complete in the tracking sheet
- ☐ Next review date assigned
- ☐ Old devices removed
- ☐ Exception recorded if incomplete

Section 6 · Recovery setup

Do not write actual recovery codes or secrets in this PDF.

Service _____ **Recovery owner** _____

Backup recovery owner _____ **Recovery method location** _____

Recovery process link _____ **Last recovery test** _____

Next recovery test _____ **Result** _____

Follow-up action _____

Recovery checklist

- ☐ Recovery codes stored in an approved secure location
- ☐ Recovery codes not in an open spreadsheet
- ☐ Recovery contact details current
- ☐ Recovery codes not in ordinary email
- ☐ At least two approved people can recover the service
- ☐ Lost-device steps documented

☐ Recovery actions logged

☐ Recovery reviewed after staff changes

Section 7 · Employee and contractor enrollment

PERSON	ROLE	ACCOUNTS IN SCOPE	MFA ENROLLED	BACKUP METHOD	EXCEPTION	REVIEW DATE

Section 8 · Service accounts and integrations

MFA for human users does not automatically protect service accounts, API tokens, or integrations. Never enter the actual credential here.

SERVICE / INTEGRATION	OWNER	PURPOSE	PERMISSION LEVEL	CREDENTIAL LOCATION	ROTATION DATE	STATUS

Section 9 · MFA exception register

ACCOUNT / SERVICE	WHY UNAVAILABLE	RISK	COMPENSATING CONTROL	OWNER	APPROVAL	EXPIRES

Section 10 · MFA-fatigue training

☐ Users deny unexpected prompts

☐ Users report repeated prompts

☐ Approved help channel known

☐ Number matching enabled where supported

☐ Suspicious sessions can be revoked

☐ Users never share one-time codes

☐ Users verify unusual support requests

☐ Admins can review recent sign-ins

☐ Sign-in context shown where supported

☐ Password-reset and incident steps documented

Section 11 · Offboarding controls

- ☐ Identity account disabled
- ☐ Registered devices removed
- ☐ Hardware keys revoked
- ☐ Recovery email addresses removed
- ☐ Connected applications reviewed
- ☐ Ownership transferred
- ☐ Active sessions revoked
- ☐ Authenticator methods removed
- ☐ Recovery phone numbers removed
- ☐ Application access removed
- ☐ Shared credentials rotated
- ☐ Completion recorded

Companion resource: the Cintherian Employee Offboarding Checklist.

Section 12 · Review schedule

REVIEW ACTIVITY	FREQUENCY	OWNER	LAST COMPLETED	NEXT DUE

Suggested frequencies: MFA coverage · monthly during rollout. Administrator access · quarterly. Registered devices · quarterly. Exceptions · monthly or quarterly. Service accounts · quarterly. Offboarding controls · after every departure. Vendor authentication changes · as announced.

Section 13 · Completion sign-off

MFA rollout coordinator _____ **Organization** _____

Rollout start date _____ **Completion date** _____

Accounts reviewed _____ **Accounts protected** _____

Exceptions _____ **Unresolved items** _____

Reviewed by _____ **Role** _____

Signature or approval _____ **Date** _____

Next review date _____

Final review · check all

- ☐ High-risk accounts protected
- ☐ Recovery arrangements documented
- ☐ Exceptions have owners and expiration dates
- ☐ Offboarding includes MFA removal
- ☐ Administrators protected
- ☐ Recovery tested
- ☐ Service accounts reviewed
- ☐ Next review scheduled