DOC-IT-0003 - MFA Standard

Document ID: DOC-IT-0003
Owner: IT Director
Approver: CIO
Version: 2.0
Status: Published
Effective date: 2025-09-01
Review date: 2026-09
Applicability: All employees, contractors, and temporary workers with a Compass One account
Source system: Policy repository; enforcement in the identity provider

Fictional document created for the GS Reference Enterprise. Not real policy.

PURPOSE

This standard defines how Compass One proves that a person presenting a credential is the person the credential belongs to. It supports the parent identity policy in DOC-IT-0002 and applies wherever a Compass One identity is used to reach a system, a dataset, or a customer environment.

SCOPE

The standard covers interactive human authentication to Compass One systems.
Machine-to-machine authentication is governed separately by the platform credential standard.

- Every Compass One account must enroll multi-factor authentication before first system use.
- Contractors must complete factor enrollment within one business day of engagement start.
- Service accounts are exempt from interactive factor enrollment under a documented exception.

APPROVED FACTORS

Factor strength is matched to the sensitivity of the access being protected. The identity provider enforces the factor tier automatically at sign-in.

- Compass One requires a phishing-resistant factor for all administrative consoles.
- Hardware security keys are the preferred factor for privileged roles.
- Authenticator application push approval is permitted for standard workforce access.
- SMS delivery is prohibited as a primary authentication factor.
- Voice call delivery is prohibited for any account with customer data access.
- Employees must register a second backup factor within seven days of enrollment.

RESET AND RECOVERY

Factor resets are the most commonly attempted social-engineering path into a workforce identity. Verification effort therefore scales with the access the factor protects.

- A factor reset requires identity verification proportional to the access at risk.
- The service desk must verify a government photo identifier before resetting a privileged factor.
- Manager confirmation is required for any factor reset requested outside business hours.
- Recovery codes are issued once at enrollment.

- Employees must store recovery codes in the approved password manager.

EXCEPTIONS

- An MFA exception requires CISO approval with a documented compensating control.
- Every exception expires ninety days after approval.
- IT must review all active exceptions each month.

ENFORCEMENT AND REPORTING

- Repeated authentication denial reports must be escalated to Security within one hour.
- An account with three failed factor challenges is locked pending service desk review.
- IT publishes factor enrollment coverage to the CIO each month.

OWNERSHIP AND REVIEW

- The IT Director owns this standard.
- Compass One reviews this standard each September.