Understand two-factor expectations

Know which accounts must enrol, how test identities differ and why administrators cannot bypass personal factor setup.

Task: Use the understand two-factor expectations process consistently and retain the right evidence.

Audience: Users, administrators and security reviewers

Owner: Obedience Governance

Version 2026.08 | Reviewed 2026-08-22 | Next review 2027-02-22

Purpose and scope

Know which accounts must enrol, how test identities differ and why administrators cannot bypass personal factor setup.

Use this guide as orientation, then rely on the signed agreement, current policy or named support response where those sources set a more specific obligation.

Prepare the right information

- The account class and role.
- Current factor enrolment state.
- Access to the trusted account security page.

Follow the controlled process

1. Frame the need

State the desired outcome, affected product and accountable contact. For understand two-factor expectations, avoid assumptions that have not been confirmed in writing.

2. Review and decide

Use the current governed source, record material questions and obtain approval from the person who owns the decision.

3. Retain evidence

Keep the final reference, date, decision and any follow-up action together so a later reviewer can reconstruct what happened.

Expected record

- An enrolled personal second factor.
- Stored recovery codes held by the user.
- A refreshed session using the factor.

Keep in mind

Test-account exemptions never grant staff or owner privilege, and staff cannot view factor secrets.

Security and disclosure boundary

- Never send passwords, authentication codes, private keys or recovery codes to Obedience staff.
- Share the minimum customer, project and commercial information needed for the stated purpose.

- Public documentation explains controls and responsibilities without publishing exploitable topology, credentials or confidential implementation detail.