

Security Baseline Standard

Owner	Andrew Smith, Security Owner
Version	1.1, effective October 19, 2026
Part of	Swapt Information Security Policy

1. Screen lock and workstation security

- Screens lock automatically after no more than 5 minutes of inactivity, and a password or Touch ID is required to unlock.
- People lock their screen whenever they step away from their device.
- FileVault full-disk encryption is enabled on every device (see the Endpoint Protection Standard).
- Clear desk: customer data, credentials and printed confidential material are not left unattended or visible, and screens are not shared in public places while confidential data is on them.

2. Password requirements

- Company accounts use unique passwords of at least 12 characters, generated and stored in an approved password manager.
- Passwords are never reused between accounts, shared by email or chat, or written down.
- Shared service credentials are stored only in the password manager or the production platform's secret configuration, and are rotated when someone with access leaves.
- In the Swapt application, every new password must be at least 8 characters. Passwords are hashed with scrypt, a slow, salted algorithm, and are never stored or logged in plain text.

3. Multi-factor authentication

MFA is required and enforced on every company account that can reach systems or data:

System	MFA
Google Workspace (email and documents)	Required
GitHub (source code)	Required
Google Cloud (application and database)	Required
Amazon Web Services	Required
Cloudflare	Required

System	MFA
Temporal and other administrative consoles	Required

Approved methods are authenticator apps, security keys and passkeys. SMS is used only where nothing else is available.

4. Swapt application accounts

- The application rate-limits login, password reset and magic-link requests to block brute-force and credential-stuffing attacks. It answers sign-in requests the same way for unknown emails, so attackers cannot discover which accounts exist.
- Session cookies are HTTP-only, Secure and SameSite=Lax.
- Internal administrative ("super admin") access requires signing in with an allowlisted company Google account. Google Workspace 2-Step Verification provides the second factor, and the shared password form is disabled.
- When a staff member signs in as a seller to give support, the session is flagged as impersonation.
- Multi-factor authentication for seller logins to the Swapt application is on our product roadmap.

5. Account lifecycle

- Accounts are created only with the Security Owner's approval and are tied to a named person. Shared personal logins are not allowed.
- Access is removed on the day a person leaves (see the Access Control Policy).