STYLDOD, INC.

Password Policy

Enterprise Policy Document

Document ID	PWD-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	Personnel accounts, privileged accounts, service accounts, API keys, machine credentials, and in-scope systems

Purpose and Scope

This policy establishes requirements for the creation, protection, use, and management of passwords and related authentication credentials used to access information systems operated by Styldod. The scope covers employees, contractors, freelancers, and authorized users, including standard user accounts, privileged and admin accounts, service accounts, API keys, OAuth secrets, SSH keys, tokens, and machine credentials.

Password Requirements

Account Type	Requirement
Standard workforce accounts	Strong, unique passwords; minimum 12 characters where supported; no reuse between personal and company systems; no plain-text storage; MFA where supported.
Privileged / admin accounts	Stronger passwords; minimum 16 characters where supported; separated from standard accounts where supported; MFA required where supported; protected through VPN/office-network path where applicable.
Service accounts / API keys	Random high-entropy secrets; minimum necessary permissions; stored in managed secret/configuration systems; no hardcoding in source code; rotation on suspected compromise or personnel departure where exposure risk exists.
Shared accounts	Strongly discouraged. Where technically unavoidable, require explicit approval, documented membership, secure storage, and rotation when users leave or no longer require access.

Multi-Factor Authentication (MFA)

- MFA must be enabled for key production, cloud, source code, database, monitoring, financial, and collaboration systems where technically supported.
- Acceptable MFA factors include hardware security keys, TOTP authenticator apps, and push-based authenticators with number matching where available.
- SMS-based MFA is not preferred for privileged access and should be treated as an interim measure where no stronger factor is available.
- Where MFA is not technically supported, compensating controls may include VPN-mediated production access, restricted infrastructure and database access, WAF, environment separation, code review, RBAC, least privilege, and encryption.

Credential Handling Rules

- Do not share passwords, API keys, tokens, MFA codes, SSH keys, or any other credentials.

- Do not send credentials in clear text over email, chat, tickets, SMS, screenshots, documents, or code comments.
- Do not store secrets in plain-text files, source code, configuration files, or unapproved tools.
- Lock or sign out of workstations when unattended.
- Immediately report suspected credential compromise; affected credentials must be changed or revoked.

Lifecycle and Review

- Initial passwords and temporary credentials must be changed promptly after first use where supported.
- Password changes are required on suspected compromise, credential sharing, vendor incident, personnel departure, or other security concern.
- Access and credentials are removed during offboarding or role changes where no longer required, in accordance with the Access Control and Offboarding Policy (ACO-001).
- Policy exceptions must follow the Policy Exception Procedure (PEX-001).