STYLDOD, INC.

Access Control and Offboarding Policy

Enterprise Policy Document

Document ID	ACO-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	Enterprise embedded integrations, customer data, production systems, and all authorized personnel

Purpose and Scope

This policy defines how Styldod grants, reviews, manages, and removes access to company systems, customer data, production environments, cloud infrastructure, source code, databases, and operational tools. Access is managed based on role, business need, least privilege, and production impact.

Access Principles

- Least privilege: access is limited to what is required for the role and no more.
- Need to know: customer data and sensitive systems are accessed only for legitimate business purposes.
- Individual accountability: shared accounts are avoided where individual accounts are available.
- MFA where supported: key production, cloud, database, source code, and sensitive systems use MFA where technically supported.
- Environment separation: development, staging, and production access are separated where applicable.
- Prompt removal: access is removed when no longer required, including during offboarding and role changes.

Access Provisioning Process

1. Manager or functional owner identifies the access required for the role.
2. Access request is reviewed based on business need, role, customer impact, and least-privilege principles.
3. Senior leadership, engineering leadership, or system owner approves access to production, infrastructure, database, source code, or customer-data systems.
4. Access is provisioned using individual accounts where supported.
5. MFA, VPN/office-network restrictions, and other security controls are applied where supported and required.
6. Access is documented or traceable through system records, access logs, tickets, or internal records.

Production and Privileged Access

- Production access is restricted to authorized personnel with a clear business need.
- Production infrastructure, database, and customer-data access is limited to approved senior or designated personnel required for deployment, monitoring, support, security, or incident response.
- Privileged access includes administrator, owner, root, production database, cloud administrator, billing administrator, security administrator, or deployment rights.

- Privileged access must be granted only to authorized personnel, reviewed for business need, protected by MFA where supported, and removed promptly when no longer required.

Access Reviews

Access is periodically reviewed by senior leadership, engineering leadership, or system owners. Reviews consider role changes, inactive users, privileged users, production access, database access, cloud access, source code access, customer support access, and terminated personnel.

Role Change Process

7. Manager or HR informs relevant system owners of the role change.
8. Access is reviewed against the new role and business need.
9. Unnecessary access is removed or reduced promptly.
10. New access is approved and provisioned only where required by the new role.
11. Privileged or production access is separately reviewed and approved.

Offboarding Process

Offboarding Step	Owner / Notes
Confirm last working date and offboarding trigger	HR / Manager / Senior leadership
Remove or suspend email and collaboration access	System owner / IT or operations
Remove source code repository access	Engineering owner
Remove cloud infrastructure and production access	Engineering / infrastructure owner
Remove database, storage, logs, and monitoring access	Engineering / data owner
Remove customer support and business application access	System owner
Rotate shared secrets or credentials if exposure risk exists	Engineering / security owner
Collect company assets where applicable	HR / operations

Confirm return or deletion of customer or company data	Manager / HR / system owner
Record completion of key access removal actions	Manager / HR / system owner

Emergency Access

Emergency access may be granted for urgent production incidents, security incidents, or customer-impacting issues. Emergency access must be limited in scope and duration, approved by senior leadership or engineering leadership where practical, and reviewed after the emergency ends.