STYLDOD, INC.

Acceptable Use Policy

Enterprise Policy Document

Document ID	AUP-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 acceptable and prohibited use of Styldod systems, customer data, production environments, devices, credentials, and company tools by employees, contractors, affiliated entity personnel, and other authorized users. The policy supports confidentiality, data protection, access control, secure operations, and responsible handling of customer and company information.

General Use Requirements

- Use company systems only for authorized business purposes consistent with the assigned role.
- Follow confidentiality obligations, employment agreements, NDAs, and internal policies at all times.
- Access only the systems, repositories, data, and environments required for the assigned role.
- Handle customer data and personal data only for approved service delivery, support, monitoring, security, or operational purposes.
- Report suspected security, privacy, access, or data handling concerns promptly to leadership or engineering/security owners.

Credential and Authentication Rules

- Use strong, unique passwords for all company systems in accordance with the Password Policy (PWD-001).
- Do not share passwords, API keys, tokens, SSH keys, MFA codes, or any other credentials.
- Do not store passwords or secrets in plain text, source code, public channels, tickets, documents, or chat messages.
- Use MFA for key production, cloud, source code, database, and sensitive operational systems where supported.
- Immediately report suspected credential compromise, phishing, or unauthorized account access.

Customer Data Handling

- Access customer data only when required for assigned work and an approved business need.
- Do not download, copy, export, share, or retain customer data locally unless explicitly authorized and required for the task.
- Do not use customer data for personal purposes, direct marketing, unrelated product testing, or unrelated AI training unless expressly agreed in writing with the customer.
- Do not share customer data through unauthorized channels, personal email, public tools, personal storage, or unapproved AI or chat tools.
- Delete temporary working copies when no longer required and follow applicable retention and deletion requirements.

Device and Endpoint Expectations

- Use company-approved devices where provided or required for the role.
- Maintain login passwords, operating system updates, firewall where supported, auto-lock/screen lock, and anti-malware protection where supported.
- Do not bypass security controls, disable required protections, or allow unauthorized people to use company devices or accounts.
- Report lost, stolen, compromised, or suspicious devices promptly to engineering or senior leadership.
- Do not store customer production data locally unless explicitly authorized.

Production and Infrastructure Use

- Production access is limited to authorized personnel based on role, business need, and least privilege.
- Use approved VPN or office-network paths where required for production access.
- Do not access production systems from untrusted networks or unmanaged devices where prohibited.
- Do not make unreviewed or unauthorized production changes; all production-bound changes must go through code review.
- Follow release, code review, testing, logging, and change-management expectations.

Prohibited Activities

- Unauthorized access, scanning, testing, copying, deletion, or modification of systems or data.
- Sharing credentials or allowing another person to use an assigned account.
- Uploading customer data to unauthorized third-party services or public AI tools.
- Using company systems to harass, discriminate, infringe, defraud, or violate applicable law.
- Installing unauthorized software or tools that create a security risk.
- Attempting to bypass logging, monitoring, access controls, MFA, VPN, or security restrictions.
- Using customer data for direct marketing, unrelated analytics, or unrelated model training unless expressly agreed in writing.

Monitoring and Enforcement

Styldod may monitor use of company systems, production environments, logs, cloud accounts, repositories, and collaboration tools for security, operational, compliance, and investigation purposes. Violations may result in access removal, disciplinary action, contractual action, or legal action where appropriate.