STYLDOD, INC.

Information Security Policy

Enterprise Policy Document

Document ID	ISP-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	All Styldod systems, services, customer data, production systems, personnel, and affiliated operations

Purpose and Scope

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets entrusted to Styldod by customers, employees, contractors, and other stakeholders.

Scope covers Styldod, Inc. and its wholly owned subsidiary Stylstage India Private Limited, all products and services including enterprise embedded integrations, all workforce members including contractors and freelancers, all information assets, and all infrastructure including production, staging, and development systems.

Roles and Responsibilities

Role	Responsibilities
All Personnel	Follow this policy, protect information assets and credentials, report security events promptly.
Senior Engineers / Engineering Leadership	Operate technical controls, configure systems, review access, investigate and remediate findings.
Engineering Leadership / Head-level Stakeholders	Own policy implementation, maintain subordinate policies, approve exceptions, review security risks.
CXO / Founder-level Leadership	Approve material decisions, customer escalations, and exceptions involving customer data or production access.
Legal / Compliance	Advise on regulatory, contractual, privacy, and disclosure obligations as needed.
Internal QA / Testing	Perform testing as part of development and release readiness including access-control, file handling, API behaviour, input validation, and production-impact scenarios.

Information Security Principles

- Confidentiality, integrity, and availability of customer and company data.
- Least privilege and need-to-know access for all systems and data.
- Defense in depth across access controls, VPN, WAF, RBAC, environment separation, code review, encryption, and monitoring.
- Secure by design and secure by default.
- Individual accountability and logging where supported by the system.
- Customer trust as the first priority.

Access Control and Authentication

- Access is granted on a role-based, least-privilege basis and reviewed periodically.
- Shared accounts are not standard practice and require explicit approval where technically unavoidable.
- Multi-factor authentication (MFA) is enabled on in-scope systems where technically supported.
- Remote production access is restricted through approved VPN or office-network paths where applicable.
- Direct infrastructure and production database access is limited to authorized senior or designated personnel.
- Access is removed during offboarding and when no longer required for the role.

Cryptography and Data Protection

- Customer data and personal data are encrypted in transit using HTTPS/TLS.
- Customer data is encrypted at rest where supported by cloud-provider managed encryption (AWS S3, MongoDB Atlas).
- Deprecated algorithms (MD5, SHA-1 for security-sensitive purposes, DES, 3DES, RC4) are not used.
- Secrets and credentials must not be hardcoded in source code or plaintext configuration files.
- API keys and secrets are stored in managed secret/configuration systems with restricted access.

Operations Security

- Production environments operate primarily on AWS infrastructure (AWS Lambda, S3, SQS, CloudFront, API Gateway, WAF).
- AWS WAF or equivalent controls are used in front of public-facing application surfaces.
- Development, staging, and production environments are separated where applicable.
- Vulnerabilities are managed through cloud-provider controls, engineering review, internal testing, and dependency monitoring.
- Styldod does not currently use a formal enterprise vulnerability-management platform; vulnerability review and remediation are handled operationally by engineering leadership and senior engineers.

Logging and Monitoring

- Audit trails and logs are maintained through AWS CloudWatch and server/application logging for systems processing customer data.
- Logs include service events, API/application activity, request or job identifiers, timestamps, errors, and operational or security-relevant events.
- Access to logs is restricted to authorized engineering personnel based on role and business need.

- Current AWS CloudWatch/server log retention is generally 5 days, after which logs are automatically deleted.
- Alerts are communicated to engineering owners through email and Slack and escalated based on severity.

Secure Software Development

- Production-bound code changes are reviewed by senior engineers or engineering leads before merge and deployment.
- Reviews cover access control, authentication, secrets exposure, input validation, dependency changes, API behaviour, and production impact.
- Customer data is not used in development or staging environments without approval, de-identification, or customer consent.
- Internal QA/security testing is performed during development and before major releases.
- Styldod does not currently run a formal automated static analysis (SAST) tool as a mandatory pipeline step; manual code review by senior engineers serves as the primary control.

AI and Machine Learning Security

- Customer data and generated outputs are not used to train unrelated public AI models unless expressly agreed in writing.
- Access to model infrastructure, model configuration, and production inference systems is restricted to authorized personnel.
- AI-generated or AI-assisted outputs may be accompanied by user-facing notices where required by platform rules, customer requirements, or applicable law.

Incident Management

Security incidents are handled through the Security Incident Response Plan (SIRP-001). All personnel must report suspected security events without delay to engineering leadership or senior leadership.

Vendor and Third-Party Management

Vendors and infrastructure providers that may process customer data are reviewed through the Vendor and Subprocessor Management Policy (VSM-001) before use.

Policy Exceptions

Policy exceptions are reviewed through the Policy Exception Procedure (PEX-001) and must include a business justification, risk assessment, compensating controls, owner, expiry date, and appropriate approvals.

Review and Maintenance

This policy is reviewed periodically and updated as Styldod's security and compliance programme matures. Material changes require approval from senior leadership and engineering leadership.