STYLDOD, INC.

Vendor and Subprocessor Management Policy

Enterprise Policy Document

Document ID	VSM-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 describes how Styldod reviews, approves, and monitors vendors, infrastructure providers, and subprocessors that may process customer data or support enterprise embedded integrations. Styldod does not outsource core enterprise service delivery or development work to external third-party development subcontractors unless specifically disclosed and agreed. Core development and operations are handled internally by Styldod and authorized personnel within Stylstage India Private Limited, Styldod's wholly owned subsidiary.

Vendor Classification

Vendor Type	Description	Review Level
Critical infrastructure provider	Hosts, stores, transmits, or secures customer data or production systems.	Security/privacy review required before use.
Operational support provider	Supports monitoring, logging, alerts, customer support, or engineering operations.	Review based on data access and business criticality.
Development tool provider	Source code, CI/CD, dependency management, issue tracking, or collaboration tools.	Review based on access to code, secrets, or customer data.
Administrative vendor	Finance, HR, legal, or corporate service provider with no customer production data access.	Review based on sensitivity of data processed.
No-data vendor	Provider that does not process customer or personal data.	Basic business approval may be sufficient.

Due Diligence Criteria

- Business need and necessity of the vendor.
- Types and categories of customer data or personal data processed.
- Data hosting location, access location, and international transfer implications.
- Security controls, encryption, access controls, logging, monitoring, and incident response commitments.
- Privacy documentation, data processing terms, DPA availability, and SCCs or equivalent transfer safeguards where required.
- Subprocessor disclosures and material subcontracting practices.
- Retention, deletion, and return-of-data capabilities.
- Availability, resilience, backup, and recovery practices where relevant.
- Relevant certifications, attestations, whitepapers, audits, or security documentation where available.

- Breach notification obligations and support commitments.

Approval Process

1. Business owner identifies the vendor need and expected data access.
2. Engineering or security owner reviews technical and security implications where customer data or production systems are involved.
3. Senior leadership approves vendors that may process customer data or access production systems.
4. Legal or compliance review is obtained where data processing terms, SCCs, customer commitments, or regulated data may be involved.
5. Vendor details are recorded in a vendor/subprocessor inventory where required for customer or compliance purposes.

Subprocessor Inventory

For enterprise customers, Styldod may maintain a list of relevant subprocessors or infrastructure providers in the applicable agreement, DPA, security questionnaire, or technical documentation. The list includes provider name, service description, nature of processing, location/hosting information where known, and duration of processing.

Ongoing Monitoring

- Review material vendor notices, security updates, privacy updates, and breach notifications.
- Review vendor security documentation when material changes occur or when required by customers.
- Reassess vendors when scope changes, data categories change, hosting locations change, or new customer obligations apply.
- Remove or replace vendors that no longer meet business, security, privacy, or contractual requirements.

Contractual Safeguards

- Confidentiality obligations covering customer and personal data.
- Data processing obligations where personal data is involved.
- Security controls and breach notification commitments.
- Standard Contractual Clauses (SCCs) or equivalent safeguards where required for international transfers.
- Deletion/return obligations and subprocessor notification where applicable.