STYLDOD, INC.

Security and Privacy Awareness Training Policy

Enterprise Policy Document

Document ID	SPAT-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 Styldod's internal privacy, confidentiality, security, and data handling guidance for employees, contractors, affiliated entity personnel, and other authorized users. It supports enterprise customer commitments and production readiness.

Training Approach

Styldod currently provides internal privacy, confidentiality, data handling, and security guidance as part of onboarding and ongoing operational processes. This is reinforced through team guidance, policy communication, engineering reviews, operational discussions, and leadership communication as needed.

Styldod does not currently operate a formal externally-certified or separately-tracked security awareness training programme. Formal training records and a periodic structured programme will be developed as enterprise customer requirements mature.

Training and Guidance Topics

- Confidentiality obligations and NDA requirements.
- Customer and personal data handling, access restrictions, and retention/deletion rules.
- Access control and least-privilege access practices.
- Secure use of company systems and approved tools.
- Password, credential, MFA, and secret protection.
- Restrictions on unauthorized sharing, downloading, or local storage of customer data.
- Use of approved channels and restrictions on unapproved AI/chat tools for customer data.
- Phishing, suspicious activity, credential compromise, and incident escalation procedures.
- Secure development expectations for engineering teams including code review, dependency review, secrets exposure, input validation, and production impact.
- Offboarding access removal and return or deletion of company or customer data.

Frequency and Delivery

Training / Guidance Type	Frequency / Trigger	Content
Onboarding guidance	At onboarding or initial access provisioning.	Confidentiality, acceptable use, access control, customer data handling, passwords, and reporting channels.
Operational reinforcement	As needed during team meetings, policy communication, engineering review, or process updates.	Customer data restrictions, secure development, access restrictions, incident escalation, and customer-

		specific requirements.
Production readiness guidance	Before or during customer-specific production readiness.	Customer-specific data flow, access limitations, retention, support process, incident response, and DPA obligations.
Formal periodic refresh	To be formalized. Periodic privacy/security awareness and evidence records as the programme matures.	All key policy areas including updates to customer requirements and regulatory developments.

Records and Evidence

Where training or formal guidance is provided, Styldod may keep internal records such as attendance, acknowledgement, policy distribution, onboarding checklist completion, or training notes. Formal completion tracking will be added where required by customer commitments or internal process.

Responsibilities

- Senior leadership owns policy communication and organizational expectations.
- Engineering leadership reinforces secure development, access control, and production data handling.
- HR or people operations supports onboarding and offboarding policy awareness where applicable.
- All personnel are responsible for following confidentiality, data handling, access, and reporting obligations.