STYLDOD, INC.

Information Security Risk Management Policy

Enterprise Policy Document

Document ID	ISRM-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 policy defines how Styldod, Inc. identifies, assesses, treats, monitors, and records information security risks across its systems, customer data, production environments, cloud infrastructure, software development processes, vendors, and personnel.

Styldod does not currently operate a dedicated information security risk management function or a formal enterprise risk platform. Risk management is performed operationally by senior leadership, engineering leadership, and senior engineers as part of product planning, infrastructure decisions, vendor selection, development, deployment, and incident handling.

This policy formalizes the current approach and sets the direction for maturation as Styldod's enterprise programme develops.

Risk Management Objectives

- Identify and understand information security risks that could affect the confidentiality, integrity, or availability of customer data, production systems, or Styldod operations.
- Assess the likelihood and potential impact of identified risks.
- Treat risks through remediation, mitigation, acceptance with rationale, or transfer where appropriate.
- Monitor risks on an ongoing basis and adjust treatment as the environment changes.
- Support enterprise customer commitments and contractual obligations by managing risks that could affect service delivery, data protection, or security.

Risk Management Roles

Role	Responsibility
CXO / Founder-level Leadership	Approve material risk decisions, risk acceptance for customer data or production access, and escalations with legal or regulatory implications.
Engineering Leadership / Head-level Stakeholders	Own technical risk identification, assessment, and treatment for production systems, infrastructure, source code, and customer data handling.
Senior Engineers	Identify and report risks during development, code review, dependency review, infrastructure changes, and operational review.
Legal / Compliance Advisors	Advise on contractual, regulatory, and privacy risk dimensions where required.

Risk Identification

Information security risks are identified through the following sources:

- Engineering and product design reviews for new features, integrations, and infrastructure changes.
- Code review, dependency review, and security testing during development and before releases.
- Cloud-provider alerts, security advisories, and dependency vulnerability notifications.
- Customer questionnaires, security assessments, and enterprise production readiness reviews.
- Security incidents, near-misses, and post-incident reviews.
- Vendor and subprocessor onboarding and monitoring reviews.
- Access control reviews and offboarding processes.
- Internal operational discussions and leadership reviews.

Risk Assessment

Identified risks are assessed based on the following dimensions:

Assessment Dimension	Considerations
Likelihood	How probable is the risk event, given existing controls, exposure, and context?
Impact	What is the potential effect on customer data confidentiality, integrity, or availability; service delivery; contractual obligations; legal compliance; or Styldod's reputation?
Affected assets	Which systems, data categories, customers, or operations are affected?
Existing controls	What controls are already in place (WAF, VPN, MFA, encryption, RBAC, monitoring, code review)?
Residual risk	What risk remains after existing controls are considered?

Risk Severity Levels

Severity	Description	Treatment Expectation
Critical	High likelihood and high impact; could result in customer data exposure, regulatory breach, or significant service disruption.	Immediate treatment required. Escalate to CXO/senior leadership. Apply remediation or strong mitigation within 24 to 72 hours.
High	Significant risk with meaningful likelihood or impact; could compromise customer data, production systems, or contractual obligations.	Prioritize treatment promptly. Define remediation or mitigation plan with owner and target date.
Medium	Moderate risk with limited exposure	Plan and remediate through normal

	or lower likelihood; unlikely to cause material harm if existing controls hold.	engineering workflow. Document rationale and treatment approach.
Low	Minor risk, informational finding, or risk with strong existing compensating controls.	Track, accept with documented rationale, or remediate as part of regular maintenance.

Risk Treatment Options

Treatment Option	Description
Remediate	Implement a control, fix, patch, configuration change, or process improvement that eliminates or substantially reduces the risk.
Mitigate	Apply compensating controls that reduce the likelihood or impact of the risk to an acceptable level (e.g. WAF rules, access restriction, additional monitoring, VPN enforcement).
Accept	Formally accept the residual risk where treatment is not feasible or cost-effective, with documented rationale and owner approval. Material risk acceptance requires senior leadership approval.
Transfer	Transfer risk to a third party through insurance, contractual terms, or vendor agreement where appropriate and permitted.
Avoid	Discontinue the activity, system, or process that creates the risk where feasible.

Risk Treatment Process

1. Identify and document the risk with description, source, and affected assets.
2. Assess severity using the severity levels above.
3. Select and document the treatment option with owner and target date.
4. Implement treatment or compensating controls.
5. Validate effectiveness of treatment through testing, monitoring, or review.
6. Record closure or ongoing monitoring requirement.
7. Escalate to senior leadership where material risk acceptance, customer data impact, or legal/contractual implications exist.

Risk Monitoring and Review

- Risks are monitored on an ongoing basis as part of engineering operations, cloud monitoring, code review, and leadership review.

- Material new risks identified through incidents, vendor notices, customer assessments, or engineering review are assessed and treated promptly.
- Risk treatment records are reviewed after significant security incidents, material infrastructure or product changes, and customer production readiness reviews.
- Styldod does not currently operate a formal periodic risk register review cycle but intends to establish one as the programme matures.

Risk Records

Engineering leadership maintains internal records of identified risks, assessments, treatment decisions, owners, and closure status for material and high-priority items. Records may be maintained in internal project management tools, documentation systems, or engineering records. Formal risk register tooling may be adopted as the programme matures.

Relationship to Other Policies

- Vulnerability Management Policy (VMP-001): covers identification and remediation of specific technical vulnerabilities.
- Security Incident Response Plan (SIRP-001): covers response to active security events.
- Vendor and Subprocessor Management Policy (VSM-001): covers risk assessment for third-party providers.
- Policy Exception Procedure (PEX-001): covers formal exception requests where standard controls cannot be met.

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.