STYLDOD, INC.

Policy Exception Procedure

Enterprise Policy Document

Document ID	PEX-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 procedure defines how Styldod requests, reviews, approves, tracks, and closes exceptions to approved security, privacy, access, operational, or customer-data handling policies. The procedure applies to exceptions affecting customer data, personal data, production systems, infrastructure, credentials, vendors, endpoints, retention, logging, and enterprise customer commitments.

Exception Principles

- Exceptions must be rare, time-bound, risk-reviewed, and approved by appropriate owners.
- Exceptions must include a business reason, affected systems/data, risk assessment, compensating controls, owner, and expiry date.
- Exceptions affecting customer data, production access, vendor risk, or material security decisions must be escalated to senior leadership and, where needed, legal/compliance.
- Permanent exceptions are not permitted. If a control cannot be implemented, a compensating control or policy update must be considered.

Exception Request Content

Field	Required Information
Requester / owner	Name, team, role, and accountable owner.
Policy/control impacted	Specific policy, control, system, or customer commitment affected.
Business justification	Why the exception is needed and why the standard control cannot be followed.
Data/system impact	Customer data, personal data, production systems, vendors, credentials, or endpoints involved.
Risk assessment	Security, privacy, legal, customer, operational, and reputational risk.
Compensating controls	Alternative controls, restrictions, monitoring, or manual checks.
Duration / expiry	Start date, end date, review date, and closure plan.
Approvals	System owner, engineering leadership, senior leadership, and legal/compliance where required.

Review and Approval Process

1. Requester submits exception request to the relevant owner or leadership channel.
2. System owner or engineering owner reviews technical feasibility and risk.

3. Security/privacy impact is assessed based on data categories, access level, exposure, customer commitments, and duration.
4. Compensating controls are defined and documented.
5. Appropriate approver grants or denies the exception.
6. Approved exception is recorded with owner, expiry date, and review requirement.
7. Exception is reviewed before expiry and either closed, extended with approval, or converted into a tracked remediation item.

Approval Levels

Exception Type	Approval Required
Low-risk operational exception with no customer data or production impact	Functional owner / engineering owner.
Customer data, personal data, production access, privileged access, or vendor-risk exception	Engineering leadership and senior leadership.
Material contractual, legal, privacy, or customer-facing exception	Senior leadership and legal/compliance review where required.
Emergency exception during incident response	Engineering leadership or senior leadership as soon as practical; post-event review required.

Records and Review

Styldod maintains an internal record of approved exceptions, owners, expiry dates, compensating controls, and closure status. Exceptions are reviewed periodically and after material security, privacy, or customer-impacting events.