STYLDOD, INC.

Security Incident Response Plan

Enterprise Policy Document

Document ID	SIRP-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 plan defines Styldod's operational process for identifying, triaging, containing, investigating, remediating, recording, and communicating security incidents, including incidents that may involve customer data or personal data processed through enterprise embedded integrations.

The plan is designed for Styldod's current operating model as a small company where security responsibilities are handled by senior leadership, engineering leadership, and authorized senior engineers. Styldod does not currently maintain a dedicated security operations centre or external security monitoring service.

Incident Categories

- Confirmed or suspected unauthorized access to customer data, systems, databases, storage, or production infrastructure.
- Loss, alteration, corruption, or unauthorized deletion of customer data.
- Exposure of secrets, API keys, credentials, or access tokens.
- Malware, ransomware, account compromise, phishing, or suspicious authentication activity.
- Abnormal traffic, abuse, scraping, denial of service, or application misuse.
- Cloud configuration error, storage exposure, logging misconfiguration, or access-control failure.
- Availability incident or service degradation with potential customer impact.
- Personal data breach or suspected personal data breach affecting customer data.

Roles and Responsibilities

Role	Responsibilities
Incident Lead	Coordinates response, assigns owners, tracks timeline, manages severity, and ensures records are maintained.
Engineering Lead	Investigates technical root cause, coordinates containment and remediation, validates recovery, and reviews logs.
CXO / Senior Leadership	Approves customer escalation, legal escalation, material business decisions, and external communications.
Legal / Compliance Advisor	Provides guidance on contractual, privacy, regulatory, and notification obligations where required.
Customer Contact Owner	Coordinates communications with impacted enterprise customers through agreed channels.
Authorized Engineers	Perform investigation, containment, code/configuration changes, access review, and recovery steps.

Detection and Reporting Channels

- Backend application monitoring and operational alerts via AWS CloudWatch.
- Cloud-provider alerts, infrastructure alerts, WAF/security alerts, and database/service notifications.
- Application logs, server logs, error logs, and job/session metadata.
- Email and Slack notifications to engineering and operational teams.
- Customer-reported issues, support requests, or third-party notifications.
- Internal engineering review, QA/security testing, code review, and production readiness checks.

Severity Classification

Severity	Description	Examples
Critical / P0	Confirmed or highly likely compromise, data exposure, significant service impact, or regulated personal data breach.	Unauthorized access to customer data; exposed database or storage; production credential compromise.
High / P1	Serious security issue with customer or production impact, or vulnerability that could lead to exposure if not contained.	Privileged account compromise; severe access-control weakness; active abuse.
Medium / P2	Security issue with limited exposure, contained impact, or no confirmed customer data compromise.	Misconfiguration without confirmed exposure; suspicious traffic; isolated system issue.
Low / P3	Minor issue, policy exception, low-risk vulnerability, or informational event.	Low-risk dependency alert; non-sensitive configuration gap; false positive after review.

Response Process

1. Identify and triage: collect initial facts, affected systems, detection source, time, customer impact, and possible data categories.
2. Contain: restrict access, disable affected credentials, rotate secrets, block traffic, isolate systems, roll back releases, or apply temporary mitigations.
3. Investigate: review logs, application behaviour, infrastructure configuration, code changes, accounts, network events, customer reports, and timeline.
4. Assess impact: determine affected customers, data categories, volume where known, regions, duration, root cause, and whether personal data may be involved.
5. Remediate: patch, reconfigure, restore, validate access controls, update code, remove exposed data, apply WAF/security rules, or implement compensating controls.

6. Recover: validate service stability, confirm containment, monitor for recurrence, and document recovery evidence.
7. Communicate: notify internal leadership and, where required, customers, legal advisors, or regulators per the applicable agreement and law.
8. Post-incident review: document lessons learned, corrective actions, owners, target dates, and follow-up verification.

Customer and Legal Notification

Styldod notifies affected enterprise customers when a confirmed or suspected incident may materially impact the security, confidentiality, integrity, or availability of their data or systems. Initial notification is provided without undue delay after validation of the incident and initial impact assessment. Follow-up updates are provided as additional facts become available. Notification timing and process are governed by the applicable commercial agreement, DPA, and legal requirements.

Incident Records

Styldod maintains internal records of security incidents including:

- Detection time and reporting source.
- Affected systems, services, customers, and data categories.
- Severity and impact assessment.
- Containment, investigation, remediation, and recovery actions.
- Owners, dates, evidence, customer/legal notifications, and post-incident follow-up items.