STYLDOD, INC.

Responsible Disclosure Policy

Enterprise Policy Document

Document ID	RDP-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	External security researchers, customers, partners, and any party reporting a security vulnerability to Styldod

Purpose and Scope

This policy describes how Styldod, Inc. receives, handles, and responds to reports of security vulnerabilities or concerns submitted by external security researchers, customers, partners, or any other third party. Styldod values responsible disclosure and is committed to working with the security community to identify and address security issues that may affect its products, services, or customer data.

Styldod does not currently operate a formal bug bounty programme with financial rewards. This policy establishes the process for responsible disclosure and the commitments Styldod makes to good-faith reporters.

How to Report a Vulnerability

Security vulnerabilities, concerns, or suspected incidents affecting Styldod products, services, infrastructure, or customer data should be reported to:

- Email: security@styldod.com
- Subject line: include the words 'Security Vulnerability' or 'Responsible Disclosure' to ensure prompt routing.
- Reports may be submitted in English. Styldod will acknowledge receipt and respond in English.

Styldod requests that reporters do not publicly disclose vulnerability details before Styldod has had a reasonable opportunity to investigate and remediate the issue. A coordinated disclosure timeline is described below.

What to Include in a Report

To help Styldod triage and respond effectively, please include as much of the following as possible:

- Description of the vulnerability, including type (e.g. authentication bypass, data exposure, injection, misconfiguration).
- Affected product, service, endpoint, or system.
- Steps to reproduce the vulnerability, including any proof-of-concept code, screenshots, or request/response examples.
- Potential impact: what data, systems, or users could be affected?
- Your name or handle and preferred contact method (optional; anonymous reports are accepted).

Scope

The following are in scope for responsible disclosure:

- Styldod production web applications and API endpoints.
- Styldod embedded iframe and widget services.
- Styldod cloud infrastructure where directly operated by Styldod (AWS-hosted services).

- Authentication, access control, and session management issues in Styldod services.
- Customer data exposure or unauthorized access vulnerabilities.

The following are out of scope:

- Vulnerabilities in third-party services or infrastructure providers (AWS, MongoDB Atlas, Cloudflare) that are not attributable to Styldod configuration or code.
- Denial-of-service (DoS/DDoS) attacks or volumetric testing against Styldod systems.
- Social engineering, phishing, or physical security attacks targeting Styldod personnel.
- Automated scanning or crawling that causes service disruption or generates excessive load.
- Issues in Styldod test, staging, or sandbox environments that do not affect production systems or customer data.

Styldod Commitments to Good-Faith Reporters

- Styldod will acknowledge receipt of a responsible disclosure report within 5 business days.
- Styldod will investigate and assess reported vulnerabilities and provide an update on the status within a reasonable timeframe, targeting 15 business days for an initial assessment.
- Styldod will not pursue legal action against reporters who act in good faith, comply with this policy, and do not exploit the vulnerability beyond what is necessary to demonstrate it.
- Styldod will not share reporter identity with third parties without consent unless required by law.
- Styldod will work toward coordinated disclosure and, where a fix is implemented, notify the reporter of the resolution.
- Styldod does not currently offer monetary rewards for vulnerability reports. Recognition may be offered at Styldod's discretion.

Reporter Expectations

Styldod asks that reporters:

- Act in good faith and avoid actions that could harm Styldod systems, customer data, or service availability.
- Do not access, modify, delete, or exfiltrate data beyond the minimum necessary to demonstrate the vulnerability.
- Do not perform testing that causes or risks service disruption.
- Do not share vulnerability details with third parties or publicly disclose before coordinated disclosure is agreed.
- Allow Styldod a reasonable remediation period before public disclosure, targeting at least 90 days from acknowledgement of the report, extendable by mutual agreement.

Coordinated Disclosure Timeline

Milestone	Target Timeframe
Acknowledgement of report	Within 5 business days of receipt.
Initial triage and severity assessment	Within 15 business days of acknowledgement.
Remediation or mitigation	Depends on severity: Critical within 24 to 72 hours; High within a reasonable short timeframe; Medium/Low through normal engineering cycle.
Notification of resolution to reporter	Upon completion of remediation or mitigation where the reporter has provided contact details.
Coordinated public disclosure	By mutual agreement, generally no sooner than 90 days from initial acknowledgement unless earlier disclosure is required for public safety.

Internal Handling of Reports

Reports received at security@styldod.com are reviewed by engineering leadership and senior leadership. Reports are triaged and handled in accordance with the Vulnerability Management Policy (VMP-001) and the Security Incident Response Plan (SIRP-001). Where a report indicates a personal data breach or risk to customer data, Styldod's incident response process is activated.

No Bug Bounty Programme

Styldod does not currently operate a formal bug bounty programme with financial rewards. Styldod may evaluate establishing a formal programme as its security and compliance programme matures. Researchers who submit high-quality reports that lead to a confirmed and remediated vulnerability may be acknowledged at Styldod's discretion, subject to the reporter's consent.

Review and Updates

This policy is reviewed periodically by senior leadership and engineering leadership and updated as Styldod's responsible disclosure programme matures.