STYLDOD, INC.

Vulnerability Management Policy

Enterprise Policy Document

Document ID	VMP-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	Enterprise embedded integrations, production systems, source code, cloud services, databases, and third-party libraries

Purpose and Scope

This policy defines how Styldod identifies, reviews, prioritizes, remediates, and records security vulnerabilities affecting applications, infrastructure, dependencies, cloud configuration, vendors, and production systems. Styldod does not currently use a formal enterprise vulnerability management platform; vulnerability review and remediation are handled operationally by engineering leadership and senior engineers.

Sources of Vulnerability Information

- Cloud-provider alerts and security advisories (AWS, MongoDB Atlas).
- Repository and dependency alerts from package manifest and lock file analysis.
- Package manager advisories and third-party vendor notifications.
- Internal engineering review, code review, QA/security testing, and production readiness checks.
- Customer reports, external technology/security updates, and responsible disclosure contacts where applicable.
- Monitoring alerts, WAF/security events, logs, and incident response findings.

Severity Classification and Response Targets

Severity	Description	Target Response
Critical	Actively exploitable issue, exposed customer data, credential exposure, remote code execution, public storage exposure, authentication bypass, or severe production impact.	Prioritize immediately. Target remediation or mitigation within 24 to 72 hours depending on severity, exposure, and production impact.
High	Serious vulnerability that could compromise customer data, production systems, privileged access, or service integrity if exploited.	Prioritize promptly. Target remediation or mitigation within a reasonable short timeframe based on risk.
Medium	Limited exposure, internal-only issue, lower likelihood, or vulnerability requiring specific conditions.	Plan and remediate through normal engineering workflow based on risk and release cycle.
Low	Low-risk finding, informational issue, minor hardening item, or false positive after review.	Track, accept with documented rationale, or remediate as part of regular maintenance.

Evaluation Criteria

- Affected system, service, library, vendor, or cloud resource.
- Whether customer data or personal data may be impacted.
- Internet exposure and authentication requirements to exploit.
- Availability of known exploit or evidence of active exploitation.
- Privilege required to exploit the vulnerability.
- Compensating controls in place (WAF, VPN, RBAC, environment separation, or network restrictions).
- Operational impact and downtime risk of applying a patch.
- Customer contractual obligations and notification requirements.

Remediation Process

1. Identify and log the vulnerability or security issue.
2. Assign owner and classify severity using the table above.
3. Evaluate exposure, customer impact, and compensating controls.
4. Prioritize remediation, mitigation, or acceptance with documented rationale.
5. Test patches or changes in dev/stage environment where applicable.
6. Deploy fix, configuration change, dependency upgrade, access restriction, WAF rule, rollback, or other mitigation.
7. Validate remediation through testing, monitoring, logs, or engineering review.
8. Record closure and any follow-up corrective actions.

Critical Vulnerability Handling

Critical vulnerabilities are prioritized immediately and targeted for remediation within 24 to 72 hours depending on severity, exposure, and production impact. Where a full patch cannot be applied immediately, Styldod applies risk-reduction steps such as access restriction, configuration change, rollback, WAF/security rule, credential rotation, or temporary mitigation until the permanent fix is deployed.

Penetration Testing and External Review

Styldod does not currently conduct formal recurring third-party penetration testing. Internal QA/security testing is performed on an ongoing basis during development and before major releases, covering access control, authentication, input validation, file upload handling, API behaviour, and production-impact scenarios. External penetration testing or third-party security review may be arranged as part of specific enterprise production readiness requirements if agreed with the customer.

Records and Reporting

Engineering leadership maintains internal records of critical and high-priority vulnerabilities including remediation actions, owners, dates, decisions, and residual risk. Customer notification, if required, follows the applicable agreement, DPA, and legal requirements.