POL-VM-001 — Penetration Testing & Responsible Disclosure Policy

Field	Value
Document ID	POL-VM-001
Version	1.0
Status	Accepted
Classification	Internal
Owner	Chief Technology Officer (Jay Johnson)
Approver	Chief Executive Officer (Tom Tansy)
Effective date	2026-04-18
Last reviewed	2026-04-19
Next review	*annually from effective date*

1. Purpose

This Policy defines DERSec's approach to penetration testing and to receiving and handling externally reported vulnerabilities, complementing the Vulnerability & Patch Management Standard (STD-VM-001).

2. Scope

This Policy covers penetration testing of DERSec's products and production environment, and the handling of vulnerability reports from external researchers and customers.

3. Penetration testing

- DERSec engages a qualified, independent third party to penetration-test DERSec's products and production environment on a periodic basis — at least annually — and after significant architectural change.
- Test scope, rules of engagement, and authorization are agreed in writing before testing.
- Findings are risk-rated and tracked to closure in the Vulnerability Scan & Pen-Test Tracker (REG-VM-001) against the remediation SLAs in STD-VM-001.
- The most recent test summary and remediation status are available to customers under NDA on request.

4. Responsible disclosure

- DERSec publishes a security contact — **security@dersec.io** — and a `security.txt` file so that researchers can report suspected vulnerabilities.

- DERSec commits to acknowledge a report promptly, investigate in good faith, keep the reporter informed, and not pursue legal action against researchers who act in good faith, avoid privacy violations and service disruption, and do not access or modify data beyond what is needed to demonstrate the issue.
- Reported vulnerabilities are triaged and remediated under STD-VM-001.

5. Customer-reported vulnerabilities

Vulnerabilities reported by customers are handled with the same triage and SLA process and, where the issue affects the product, the customer-notification provisions of STD-VM-001 apply.

6. Coordinated disclosure

Where a vulnerability affects the product, DERSec coordinates disclosure timing with the reporter and affected customers, balancing prompt customer protection with responsible release of detail.

7. Roles & responsibilities

Role	Responsibility
CTO	Owns this Policy; commissions penetration tests; triages disclosure reports.
Engineers	Remediate findings within SLA.

8. References

STD-VM-001 · POL-SD-001 · PLN-IR-001 · REG-VM-001.

Revision History

Version		Author	Summary of change
1.0	2026-05-22	J. Johnson, CTO	Initial release; content finalized and issued for signature.

Document Control & Adoption

This document is a controlled DER Security Corp policy. It is maintained under DER Security Corp document control by its Owner, the Chief Technology Officer (Jay Johnson), and is adopted for use under the authority of POL-IS-001 (Information Security Policy), which is signed by the Approver, the Chief Executive Officer (Tom Tansy). Approval of this document is recorded in the DER Security Corp policy register; no separate executive signature block is applied here.

Its currency is governed by the Document Control table at the top of this document and by the corporate policy register. The Effective date and Last reviewed date are recorded there.