Vulnerability Disclosure Policy

Date	Name	Role	Change	Version
Tue Jan 27 2026	Wikus Du Plessis	Security Architect	Approved	V1.0

Vulnerability Disclosure Policy

Stratech (Pty) Ltd
This Vulnerability Disclosure Policy (VDP) provides a **clear, safe, and responsible mechanism** for security researchers to report potential vulnerabilities in StraTech-operated systems.

This program supports:

- Ongoing improvement of StraTech's security posture
- Compliance with **PCI DSS v4.0**
- Responsible, coordinated vulnerability handling

This is not a bug bounty program. **No monetary rewards are offered** at this time.

Goals of the Program

- **Clarity;** Clearly define what can and cannot be tested
- **Safety;** Protect customer data, availability, and business operations
- **Trust;** Encourage responsible disclosure without legal uncertainty
- **Low operational overhead;** Scaled for a maturing security function

Vulnerability Disclosure Program

StraTech is committed to protecting the security and availability of our systems and the data entrusted to us.

We welcome responsible disclosure of security vulnerabilities and value the efforts of the security community in helping us improve our security posture.

This Vulnerability Disclosure Policy (“Policy”) outlines how security researchers can safely and responsibly report vulnerabilities in systems operated by StraTech.

This program is not a bug bounty program and does not offer monetary rewards.

Purpose

The purpose of this Policy is to provide a clear and coordinated mechanism for reporting security vulnerabilities, while ensuring the safety of our customers, systems, and operations.

This Policy supports StraTech’s broader information security program and ongoing compliance with PCI DSS v4.0.

Scope

In Scope

The following public-facing, production systems owned and operated by StraTech are eligible for testing and reporting:

- Public websites and web applications
- Public APIs
- Authentication, authorization, and session management mechanisms
- Security controls protecting public-facing services

Testing must be **non-disruptive** and limited to what is necessary to demonstrate the vulnerability.

Out of Scope

The following activities and systems are **strictly prohibited**:

- Denial of Service (DoS / DDoS) attacks, stress testing, or traffic flooding
- Automated vulnerability scanning that impacts system availability
- Social engineering or phishing.
- Physical security testing
- Testing of third-party systems, vendors, or service providers.
- Attempts to access, modify, or exfiltrate data belonging to users.

PCI Restriction:
Active testing of **Cardholder Data Environments (CDE)** or payment processing systems is **not permitted**.

If a potential vulnerability related to payment data is identified, testing must stop immediately, and the issue should be reported.

Safe Harbor

StraTech considers security research conducted in g**ood faith** and in accordance with this Policy to be **authorized**.

Provided that researchers:

- Act responsibly and in good faith
- Avoid privacy violations, data destruction, and service disruption
- Do not exploit vulnerabilities beyond proof-of-concept

- Follow coordinated disclosure requirements

StraTech will not pursue legal action for such research.

This **safe harbor does not apply** to activities that are malicious, disruptive, or explicitly listed as out of scope.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability, please report it as soon as possible.

Email:
📧 security@stratech.co.za

When submitting a report, please include where possible:

- A description of the vulnerability
- The affected system or endpoint
- Steps to reproduce (proof-of-concept)
- The potential impact
- Supporting material such as screenshots or request samples

Please avoid including sensitive personal or customer data unless strictly necessary.

Disclosure and Confidentiality

- All vulnerability reports are treated as **confidential**
- Public disclosure must be coordinated with **StraTech**
- **Researchers may not disclose vulnerabilities publicly** without explicit written consent

- Stratech will manage disclosure timelines based on risk and operational impact

Response and Remediation

- Reports are acknowledged on a **best-effort basis**
- Vulnerabilities are assessed using a **risk-based approach**
- Prioritization considers severity, likelihood, and business impact
- Remediation timelines are determined internally

No guaranteed response or remediation service-level agreements (SLAs) are provided.

Program Limitations

- This program does not provide financial rewards
- Duplicate, low-impact, or out-of-scope reports may not receive individual responses
- Abuse of this Policy may result in loss of safe harbor protections

Contact

For security-related matters, please contact:
📧 security@stratech.co.za
or
https://stratech.co.za/.well-known/security.txt

pgp signed security.txt

Contact: mailto:security@stratech.co.za

Policy: https://stratech.co.za/security/vulnerability-disclosure

Preferred-Languages: en

Disclosure: Coordinated

Expires: 01/01/2030

Security email:
Email: security@stratech.co.za

Used as main intake for security related risks. Shared between Security Architect and other relevant parties.