DARKRISK / SECURITY

Vulnerability Disclosure Policy

OWNER	VERSION	EFFECTIVE
DARKRISK (PTY) LTD	1.0	1 AUGUST 2026

1. Purpose

DarkRisk (Pty) Ltd ("DarkRisk") is committed to safeguarding our systems and the information entrusted to us by customers, partners, personnel, and users. This policy provides a clear process for reporting suspected security vulnerabilities and establishes the conditions for good-faith security research involving DarkRisk assets.

We value researchers who report issues responsibly. When appropriately notified of a legitimate issue, we will investigate, assign suitable resources, and work to remediate or mitigate confirmed vulnerabilities as quickly as reasonably possible.

2. Reporting a security issue

If you believe you have discovered a vulnerability in a DarkRisk-owned asset or need to report a security incident, email:

> **security@darkrisk.io**

A useful report should include, where available:

- the affected domain, endpoint, product, or asset;
- a clear description of the issue and its potential impact;
- reproducible steps or a minimal proof of concept;
- relevant timestamps, request details, screenshots, or logs; and
- a safe way for us to contact you with follow-up questions.

Do not include live credentials, unnecessary personal information, or copies of data belonging to another customer or user.

3. Research guidelines

To remain within this policy, you must:

- act in good faith and test only accounts and systems you own or are expressly authorised to use;
- use the minimum interaction necessary to demonstrate the vulnerability;
- stop testing and notify us immediately if you encounter personal information, credentials, confidential information, or Customer Data;
- avoid retaining, copying, transmitting, changing, or destroying data;
- stop after confirming the first vulnerability and request permission before continuing any testing that could expand its scope;
- report the issue promptly and without attaching conditions to disclosure; and
- allow DarkRisk reasonable time to investigate and address the issue before any public disclosure.

4. Prohibited activity

You must not:

- exfiltrate data or access more information than required to verify the issue;
- exploit a vulnerability to compromise additional accounts or systems;
- disable security controls or establish persistence;
- perform social engineering, phishing, or physical security testing;

- conduct denial-of-service, resource-exhaustion, spam, or traffic-flooding tests;
- use automated scanners in a way that degrades service or generates excessive traffic;
- test third-party services, infrastructure, or applications not owned by DarkRisk; or
- violate any applicable law or the rights of another person.

5. Scope

This policy applies to internet-accessible systems and applications owned and operated by DarkRisk, including DarkRisk-controlled domains and subdomains. Third-party services are out of scope unless DarkRisk confirms otherwise in writing. If ownership is unclear, contact us before testing.

This is a vulnerability disclosure programme and not a paid bug bounty. DarkRisk does not promise payment or other reward unless separately agreed in writing before the report is submitted.

6. Safe harbour

If you conduct research in good faith and comply with this policy, DarkRisk will consider that activity authorised and will not pursue legal action against you solely for that research. If a third party initiates legal action relating to your compliant research, we may clarify that your activity was conducted in accordance with this policy.

Safe harbour does not apply to activity that is unlawful, harmful, deceptive, outside the scope of this policy, or continued after we ask you to stop. This policy does not authorise activity against systems owned by a third party.

7. Our response process

1. **Receipt and confidentiality.** We receive the report through our security channel and ask that related communications remain confidential.
2. **Investigation and verification.** We review the evidence, reproduce the issue where possible, and assess its scope and severity.
3. **Remediation or mitigation.** We work to correct the issue or deploy appropriate mitigations. Where an immediate fix is not practical, we assess interim controls.
4. **Ongoing communication.** We aim to keep the reporter informed as the investigation progresses and confirm when the matter has been addressed.

8. Disclosure and recognition

Coordinate any proposed public disclosure with DarkRisk. We may recognise a researcher's contribution if the researcher requests recognition and we agree that doing so is appropriate. We will not disclose your identity without permission unless required by law.

We appreciate the security community's efforts to improve our products and protect our customers. Thank you for reporting issues constructively.

---

9. Contact

Security reports: **security@darkrisk.io**
Policy or compliance enquiries: **compliance@darkrisk.io**