TERRACLOUD TECHNOLOGY

RESPONSIBLE DISCLOSURE POLICY

Reporting security vulnerabilities to Terracloud Technology

TRUST FRAMEWORK PUBLICATION TC-SEC-001

Document Number	TC-SEC-001
Version	1.0
Status	Approved for Publication
Document Classification	Public
Effective Date	July 2026
Next Review Date	July 2027

Responsible Entities

Terracloud Technologies CC (South Africa) — Registration No. 2011/083806/23 — trading as Terracloud Technology — primary operating entity.

Terracloud Technology GmbH (Germany) — Registration No. HRB 5105 02124665 3 — active operating entity.

Terracloud Technology Ltd (United Kingdom) — Company No. 13652901 — registered but currently dormant.

Document Control

Document Title	Responsible Disclosure Policy
Document Number	TC-SEC-001
Document Owner	Craig Cloete Information Officer
Responsible Entities	Terracloud Technologies CC (South Africa); Terracloud Technology GmbH (Germany); Terracloud Technology Ltd (United Kingdom, dormant)
Document Classification	Public
Version	1.0
Effective Date	July 2026
Next Review Date	July 2027
Approved By	Craig Cloete, Information Officer

Revision History

Version	Date	Summary of Changes	Author
1.0	Jul 2026	First issue as TC-SEC-001 within the Terracloud Trust Framework. Original document; no prior version exists.	C. Cloete

Table of Contents

1. Purpose

Terracloud Technology values the work of security researchers who help us identify and address vulnerabilities. This policy explains how to report a security vulnerability to us responsibly, what we ask of researchers, and what you can expect from us in return.

2. Scope

This policy applies to the websites, systems, and services owned and operated by Terracloud Technology. It does not extend to the systems or services of third parties, including cloud, hosting, or software providers we use, unless we have express authority to accept reports on their behalf.

3. Responsible Disclosure Principles

We welcome reports submitted in good faith by researchers acting within the terms of this policy. We are committed to working with researchers in a professional, respectful, and cooperative manner, and to treating reports as an opportunity to improve the security of our systems.

4. What We Ask Researchers To Do

- Act in good faith and avoid disrupting or degrading our services
- Limit testing to what is necessary to demonstrate a vulnerability
- Stop testing immediately and notify us if you encounter customer information
- Give us a reasonable opportunity to investigate and remediate before disclosing a vulnerability publicly
- Comply with all applicable laws while conducting your research

5. Authorised Security Research

Security research conducted in accordance with this policy, and limited to what is necessary to identify and demonstrate a vulnerability, is authorised. Researchers should avoid any action that goes beyond what is needed to confirm a vulnerability exists, and should not access, download, modify, or delete data beyond what is strictly necessary for this purpose.

6. Prohibited Activities

- Denial-of-service testing or any activity that disrupts or degrades our systems or services
- Social engineering of our staff, contractors, or customers
- Phishing or any attempt to obtain credentials through deception
- Physical attacks against our premises, staff, or infrastructure
- Destruction or alteration of data
- Accessing, copying, or retaining data beyond what is necessary to demonstrate a vulnerability

Activities of this kind fall outside the scope of this policy and may be treated as unauthorised access.

7. How To Report A Vulnerability

If you believe you have found a security vulnerability affecting Terracloud Technology, please report it to us at security@terracloud.technology.

8. What Information To Include

To help us investigate efficiently, please include where possible:

- A description of the vulnerability and its potential impact
- The steps required to reproduce it
- The system, URL, or component affected
- Any supporting evidence (e.g. screenshots or logs), avoiding access to customer information
- Your contact details, if you would like us to follow up with you (reports may also be submitted anonymously)

9. Our Commitment

Where a report is submitted in good faith and in accordance with this policy, we will:

- Acknowledge receipt of your report
- Investigate your report in good faith
- Keep you informed of our progress where practical
- Treat you and your report with respect
- Not pursue legal action against you for research conducted in good faith and within the limits of this policy

10. Coordinated Disclosure

We ask that you do not publicly disclose a vulnerability until we have had a reasonable opportunity to investigate and remediate it. Where you wish to publish details of a vulnerability you have reported, we are willing to discuss a disclosure timeline with you in good faith.

11. Legal Position

This policy does not authorise any activity that is unlawful, or any testing that falls outside the scope and limits described above. Researchers remain responsible for ensuring that their activities comply with applicable law. Nothing in this policy creates a contractual right to any reward, payment, or specific response time.

12. Contact Details

To report a vulnerability, or for any questions about this policy, please contact:

Security Contact	security@terracloud.technology
Information Officer	Craig Cloete
Privacy Contact	privacy@terracloud.technology
Website	https://www.terracloud.technology
Trust Centre	https://www.terracloud.technology/trust-centre

13. Related Documents

This policy forms part of the Terracloud Trust Framework and should be read together with the following controlled publications:

- TC-LEG-001 — Privacy Policy
- TC-LEG-002 — Terms of Use
- TC-LEG-003 — PAIA Manual
- TC-LEG-006 — Data Subject Request Form
- TC-SEC-002 — Compliance & Security Statement