COMPLIANCE & SECURITY STATEMENT

Our approach to security, data protection, and governance

TRUST FRAMEWORK PUBLICATION TC-SEC-002

Last updated: August 2026

---

1. DOCUMENT CONTROL

Document Title	Compliance & Security Statement
Document Number	TC-SEC-002
Document Owner	Craig Cloete, Information Officer
Responsible Entities	Terracloud Technologies CC (South Africa) Terracloud Technology GmbH (Germany) Terracloud Technology Ltd (United Kingdom)
Document Classification	Public
Version	1.0
Effective Date	August 2026
Next Review Date	August 2027
Approved By	Craig Cloete, Information Officer

2. REVISION HISTORY

Version	Date	Summary of Changes	Author
1.0	Aug 2026	First issue as TC-SEC-002 within the Terracloud Trust Framework. Original document; no prior version exists.	Craig Cloete

1. Purpose

This statement explains how Terracloud Technology approaches information security, data protection, governance, and compliance. It is intended to give clients and other stakeholders a clear, honest picture of the controls and practices we have in place, appropriate to the size and nature of our organisation.

2. Scope

This statement applies to Terracloud Technology's own systems, services, and operations across South Africa, Germany, and the United Kingdom. It does not constitute a certification, warranty, or guarantee of security, and should be read together with the other publications in the Terracloud Trust Framework.

3. Our Security Approach

Terracloud Technology takes a layered approach to security, combining technical controls, documented policies, and ongoing monitoring. Our approach is designed to help reduce risk across our systems and the services we deliver, and is reviewed periodically as our organisation and the threat landscape evolve.

4. Governance and Accountability

Security and compliance at Terracloud Technology are overseen by our Information Officer, who is accountable for data protection compliance and for coordinating our security practices. Our approach is supported by documented policies covering privacy, access to information, and responsible disclosure, which are reviewed periodically.

5. Data Protection and Privacy

Terracloud Technology's approach to personal information is set out in our Privacy Policy and PAIA Manual, which describe what information we collect, how it is used, and the rights available to data subjects. Our data protection practices are informed by POPIA, GDPR, and UK GDPR, applied appropriate to the jurisdiction in which personal information is processed.

6. Access Control

Access to our systems and client data is restricted on the basis of role and business need. Access controls are supported by authentication measures and are reviewed periodically to help ensure they remain appropriate as roles and responsibilities change.

7. Endpoint and Device Security

Devices used to access Terracloud Technology systems are protected by endpoint protection and endpoint detection and response (EDR) tooling, designed to help identify and respond to suspicious activity on managed endpoints.

8. Cloud and Microsoft 365 Security

Terracloud Technology operates on Microsoft 365, and our configuration of this environment is aligned with recognised cybersecurity good practice for cloud collaboration platforms. Configuration and access settings are reviewed periodically as part of our ongoing security practices.

9. Backup and Recovery

We maintain backup and recovery arrangements designed to help support the continuity of our services and the recoverability of data in the event of loss or disruption. These arrangements are reviewed periodically to help ensure they remain fit for purpose.

10. Monitoring and Threat Detection

Terracloud Technology uses monitoring tools to help identify potential security events across the systems we manage. Monitoring is supported by our endpoint detection and response tooling and forms part of our broader approach to threat detection.

11. Supplier and Third-Party Controls

Where Terracloud Technology relies on third-party suppliers to deliver services, we apply a level of due diligence appropriate to the nature of the service and the data involved. This may include reviewing supplier security practices and putting appropriate contractual protections in place, including data processing agreements where relevant.

12. Incident Response and Breach Notification

Terracloud Technology maintains an approach to incident escalation designed to help ensure that security events are identified, investigated, and addressed. Where a data breach affecting personal information occurs, we will notify the Information Regulator and affected data subjects in accordance with our Privacy Policy and applicable law.

13. Responsible Disclosure

Terracloud Technology welcomes reports of security vulnerabilities from researchers acting in good faith. Our approach to receiving and handling such reports is set out in our Responsible Disclosure Policy.

14. Compliance Alignment

Terracloud Technology's policies and practices are aligned with the requirements of POPIA and PAIA in South Africa, and are informed by GDPR and UK GDPR where relevant to our operations in Germany and the United Kingdom. Our practices are also aligned with recognised cybersecurity good practice and a risk-based approach to governance, appropriate to the size and nature of our organisation.

Terracloud Technology does not hold ISO 27001, SOC 2, or Cyber Essentials certification. Where certifications are obtained in future, this statement will be updated accordingly.

15. Continuous Improvement

Our security and compliance practices are reviewed periodically and updated as our organisation, our services, and the risks we face continue to evolve. We view security and compliance as an ongoing process rather than a fixed state.

16. Contact Details

For any questions about this statement, or about our approach to security and compliance, please contact:

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

17. Related Documents

This statement 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-004 — Cookie Policy
- TC-LEG-005 — Applicant Privacy Notice
- TC-LEG-006 — Data Subject Request Form
- TC-SEC-001 — Responsible Disclosure Policy