Our *Innovation*
Your *Intelligence*

INFORMATION SECURITY POLICY

Version 2 9 September 2025

GEOTERRA IMAGE

www.geoterraimage.com

GEOTERRAIMAGE *(Pty) Ltd*
Agri Hub Business Park, Building C (Ground Floor)
477 Witherite Street | Willows | Pretoria | South Africa | 0184
Tel: +27 (0)12 807 9480 | Fax: +27 (0)12 807 9481
info@geoterraimage.com
www.geoterraimage.com

POLICY NAME	**INFORMATION SECURITY POLICY**		
DOCUMENT ID	**GO-4**		
EFFECTIVE DATE	09 September 2025	**DATE OF LAST REVISION**	03 September 2025
ADMINISTRATOR RESPONSIBLE	Elsa Van Zyl	**CONTACT INFORMATION**	Elsa.vanzyl@geoterraimage.com
Applicable To:	Employees and Management, Third Parties and Contractors, Partners and Affiliates, Systems and Data Assets		

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**
V1	Directors	22 August 2025	New	Alet Henning
V2	Dr. Corné Elof	3 September 2025	Align with ISO9001 Policy Structure & update content	Elsa Van Zyl

APPROVAL AND REVIEW

The **GEOTERRA**IMAGE Information Security Policy is reviewed annually (or sooner if required) by our Information Security Officer and formally approved by Executive Management. This process ensures that the policy remains current, effective, and backed by top-level commitment to security and compliance.

POLICY STATEMENT

GeoTerraImage Group of companies: GeoTerra Image (Pty) Ltd, GeoTerraImage Holdings (Pty)LTD, GeoTerraImage SA (Pty) Ltd (GTI-SA), GeoTerraImage Education NPC, and, in addition, as its European incorporated company GEOTIPT INTERNATIONAL, UNIPESSOAL LDA (GeoTerra360).

Hereafter referred to as "The Group"

"The Group" is a well-regarded organisation, recognised for its strong commitment to regulatory compliance. It has earned a reputable standing among clients and competitors alike by consistently conducting its business in line with high moral, ethical, and legal standards. "The Group" remains firmly committed to ethical and transparent business practices, actively upholding this commitment through the implementation and enforcement of comprehensive corporate governance frameworks, internal controls, and codes of conduct that guide all employees and stakeholders in their professional responsibilities.

GEOTERRAIMAGE *(Pty) Ltd*
Agri Hub Business Park, Building C (Ground Floor)
477 Witherite Street | Willows | Pretoria | South Africa | 0184
Tel: +27 (0)12 807 9480 | Fax: +27 (0)12 807 9481
info@geoterraimage.com
www.geoterraimage.com

SCOPE

This Information Security Policy applies to:

All employees of GEOTERRAIMAGE, including permanent, temporary, and contract staff, regardless of role or seniority.

Third parties such as service providers, consultants, contractors, vendors, and outsourced partners who are granted access to company information, systems, or facilities.

Affiliated entities and business partners where information assets are shared or integrated.

All information assets, including data, systems, networks, applications, and devices owned, leased, managed, or otherwise entrusted to the GeoTerra Image, whether stored digitally or physically.

Compliance with this policy is mandatory for all individuals and entities covered above. Failure to adhere to its provisions may result in corrective measures in line with GeoTerra Image's governance framework.

POLICY SECTIONS

1. SECURITY MODEL

The **GEOTERRA**IMAGE cloud security model has two layers:

- Google Cloud Security – safeguarding the cloud infrastructure, including physical facilities, hardware, and core platform services.
- Our System and Data Security – managing identity and access controls, securing APIs, monitoring applications, and enforcing data protection policies.

This model ensures layered security and transparency between the provider's and customer's responsibilities.

1a. GOOGLE CLOUD SECURITY

Google Cloud is built with security as a foundational principle. Its multi-layered security model spans every aspect of the infrastructure, including:

- Physical security of data centers and facilities
- Hardware and software controls to safeguard systems
- Operational practices that ensure reliability, compliance, and risk management

GEOTERRAIMAGE (Pty) Ltd
Agri Hub Business Park, Building C (Ground Floor)
477 Witherite Street | Willows | Pretoria | South Africa | 0184
Tel: +27 (0)12 807 9480 | Fax: +27 (0)12 807 9481
info@geoterraimage.com
www.geoterraimage.com

1b. GOOGLE COMPLIANCE AND CERTIFICATIONS

Google Cloud maintains compliance with multiple internationally recognised standards, including:

- ISO/IEC 27001 – Information Security Management
- ISO/IEC 27018 – Protection of Personally Identifiable Information (PII) in public clouds
- SOC 2 and SOC 3 – Independent audit reports on security, availability, and confidentiality controls

These certifications demonstrate that Google's controls and security practices align with globally accepted benchmarks for data protection, security, and compliance.

1c. ENCRYPTION AND DATA PROTECTION

All data is encrypted by default:

- A**t rest** – Persistent disks, object storage, and databases are automatically encrypted using AES-128 or stronger algorithms.
- **In transit** – Communication moving between users, services, and APIs is encrypted using HTTPS and TLS protocols.

This provides end-to-end protection of sensitive data, ensuring confidentiality and integrity throughout its lifecycle.

2. GEOTERRA IMAGE SYSTEM AND DATA SECURITY

2a. Authentication and Access Management

Our systems and user data are safeguarded through industry-standard authentication and authorisation methods provided by Google Cloud, including:

- **Username and password protection**
- **Access and ID tokens, such as OAuth 2.0, OpenID Connect, and JWTs**
- **Industry-standard token mechanisms** for secure inter-service communication

These measures are widely recognised and trusted across the industry, ensuring strong identity assurance and controlled access.

GEOTERRAIMAGE (Pty) Ltd
Agri Hub Business Park, Building C (Ground Floor)
477 Witherite Street | Willows | Pretoria | South Africa | 0184
Tel: +27 (0)12 807 9480 | Fax: +27 (0)12 807 9481
info@geoterraimage.com
www.geoterraimage.com

2b. Industry Standards and Frameworks

Google Cloud security practices align with globally recognised frameworks, ensuring that our use of GCP meets industry expectations for:

- Identity and Access Management best practices
- The Shared Responsibility Model, where Google secures the infrastructure, while we secure application-level configurations and IAM policies
- Security blueprints and guidance, including reference architectures, monitoring tools, and compliance frameworks for building secure systems

By leveraging Google Cloud Infrastructure, we benefit from a secure foundation that:

- Implements robust authentication and token-based access mechanisms
- Provides encryption at rest and in transit by default
- Complies with ISO and SOC industry standards
- Aligns with best practices and industry frameworks through the shared responsibility model

Google's compliance and certifications extend to the services we use. This assures that our systems, APIs, and data are protected under globally recognised security frameworks and standards.

2c. Email Security — Sendmarc Compliance

GEOTERRAIMAGE maintains a current Sendmarc compliance certificate together with an accompanying security report for our email domain(s).

The Sendmarc report confirms that our domain authentication is correctly configured and actively enforced through industry-standard controls (SPF, DKIM, DMARC).

These controls are supported by continuous monitoring and quarterly reviews of alignment and delivery outcomes.

In practice, this means that messages failing authentication are detected and handled according to policy, significantly reducing the risk of spoofing, phishing, and impersonation attacks targeting our staff, clients, and supply-chain partners.

The Sendmarc report also provides aggregate and forensic visibility into sending sources, enabling us to identify and remove unauthorised senders, tighten DNS records, and document improvements over time.

Together, these measures complement the encryption-in-transit protections already described in our cloud stack and reinforce the shared responsibility model outlined in this document.

GEOTERRAIMAGE (Pty) Ltd
Agri Hub Business Park, Building C (Ground Floor)
477 Witherite Street | Willows | Pretoria | South Africa | 0184
Tel: +27 (0)12 807 9480 | Fax: +27 (0)12 807 9481
info@geoterraimage.com
www.geoterraimage.com

2d. Backup & Recovery — Redstor Certificates (Nightly Server Backups)

GEOTERRAIMAGE backup and recovery controls are underpinned by Redstor, supported by current Redstor certificates confirming our service status and configuration.

Backup process: Server data is backed up nightly, capturing daily changes on a schedule and replicating them to secure storage with encrypted transfer and encrypted data at rest.

- GTI-LINUX-01 – Dormant backup (files retained, not actively backing up).
- GTI-LINUX-03 – Active nightly backup.

Integrity checks: Redstor's integrity checks and job analytics verify that each backup completes successfully; exceptions are alerted to administrators for remedial action.

Retention and recovery: Recovery points are maintained in line with our data-retention policy, supporting both point-in-time restores and rapid recovery of critical systems to meet our RPO/RTO targets.

These controls sit on top of the secure-by-default platform capabilities already detailed (including default encryption at rest and in transit), providing layered protection from accidental deletion, corruption, or ransomware events and aligning with our broader cloud security and shared responsibility approach.

2e. Email Evidence & Availability

Copies of the current Sendmarc compliance certificate and security report, along with the Redstor service certificates and recent backup job summaries, are available on request to auditors, clients, or stakeholders who require assurance.

This documentation aligns with the encryption, compliance, and access-control sections of our cloud security model, providing traceable evidence that our email security posture and nightly backup regime are consistently effective.

ROLES AND RESPONSIBILITIES	
ROLE	**RESPONSIBILITY**
INFORMATION SECURITY OFFICER	Monitor compliance and risk exposure at the governance level.
OPERATIONS MANAGER	Maintain, update and circulate policy
IT DEPARTMENT	Configure, monitor, and maintain technical security controls
DIRECTORS	Provide strategic direction and oversight for information security

.

APPROVAL SIGNATURE		
TITLE	**NAME**	**EMAIL**
INFORMATION SECURITY OFFICER	Corne Eloff	corne.eloff@geoterraimage.com
SIGNATURE & DATE	Corne Eloff Digitally signed by Corne Eloff Date: 2025.09.09 15:30:23 +02'00'	09 September 2025