Our *Innovation*
Your *Intelligence*

# INFORMATION SECURITY INCIDENT RESPONSE PLAN

Version 1 5 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 INCIDENT RESPONSE PLAN** | | |
| **DOCUMENT ID** | **GO-5** | | |
| **EFFECTIVE DATE** | 05 September 2025 | **DATE OF LAST REVISION** | 04 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 | | |

**VERSION HISTORY**

| VERSION | APPROVED BY | REVISION DATE | DESCRIPTION OF CHANGE | AUTHOR |
|---|---|---|---|---|
| V1 | Dr. Corné Elof | 4 September 2025 | Align with ISO9001 Policy Structure | Elsa Van Zyl |

## APPROVAL AND REVIEW

The **GEOTERRA**IMAGE **Information Security Incident Response Plan** is designed to uphold and align with the Information Security Policy

## COMPANY OVERVIEW

**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.*

## PURPOSE

The purpose of this Information Security Incident Response Plan (ISIRP) is to confirm **GEOTERRA**IMAGE's commitment to define a structured approach for identifying, detecting, reporting, responding to, and recovering from information security incidents. This Plan aligns with the **GEOTERRA**IMAGE **Information Security Policy** and ensures accountability, timely response, and continuous improvement

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 Plan applies to all employees, directors, managers, contractors, suppliers, service providers, and third parties engaged with **GEOTERRA**IMAGE. It covers all forms of information security incidents, including but not limited to data breaches, cyberattacks, unauthorised access, insider threats, ransomware, and system disruptions.

In the event of an information security incident, **GEOTERRA**IMAGE commits to following a structured reporting and response process to ensure accountability, timely action, and ongoing improvement.

## DEFINITIONS

| | |
|---|---|
| EVENT | An identified occurrence within a system, service, or network that indicates a possible breach of security policy, or a situation relevant to the security of information or systems. |
| BREACH | A security incident that results in the confirmed compromise of systems or data. |
| THREAT | An unwanted incident that may result in harm to a system, organisation, or individual by exploiting a vulnerability. |
| VULNERABILITY | A weakness or gap in a system, process, control, or human factor that can be exploited by a threat to compromise the confidentiality, integrity, or availability of information or systems. |

## INCIDENT CLASSIFICATION AND SEVERITY

| | |
|---|---|
| LOW | Minor disruption with no sensitive data impact. |
| MEDIUM | Limited disruption or potential exposure of non-sensitive data. |
| HIGH | Significant disruption with potential compliance consequences. |
| CRITICAL | Major disruption, confirmed data breach, compliance impact. |

## INCIDENT RESPONSE PROCESS

The incident response lifecycle includes:

1. Incident Identification & Reporting - Identify and report incidents promptly
2. Initial Assessment - Classify, prioritise, and assign responsibility
3. Containment & Mitigation - Limit scope and prevent further damage
4. Investigation & Root Cause Analysis - Identify vulnerabilities, system weaknesses
5. Communication & Reporting – Communication and reporting to stakeholders and organisations
6. Recovery and Restoration - Remove vulnerabilities, restore systems and validate normal operations
7. Post-Incident Review - Conduct post-incident review and implement improvements
8. Documentation & Evidence – Maintain and make available upon request

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

## 1. INCIDENT IDENTIFICATION AND REPORTING

- Any staff member who becomes aware of a potential incident (data breach, system outage, unauthorized access, or suspected leak) must report it immediately to their line manager and the IT/Security team.
- The incident must be logged in the Incident Register with details of the date, time, person reporting, and description.

## 2. INITIAL ASSESSMENT

- The IT/Security team will conduct an immediate assessment to determine the severity, scope, and potential impact.
- Priority levels will be assigned (Low, Medium, High, Critical).

## 3. CONTAINMENT AND MITIGATION

- Immediate steps must be taken to contain the incident and prevent further damage (e.g., disabling accounts, isolating servers, revoking access tokens).
- Mitigation actions must be tracked and recorded.

## 4. INVESTIGATION & ROOT CAUSE ANALYSIS

- A root cause analysis must be performed to identify vulnerabilities, system weaknesses, or human errors that led to the incident.

## 5. COMMUNICATION AND REPORTING

- Notify relevant stakeholders (management, regulators, law enforcement, affected clients, and other third parties in line with legal obligations (If applicable under PAIA/POPIA) in line with compliance requirements.
- Communication must be clear, timely, and well-documented.
- Incident reports, escalation logs, and corrective actions to be maintained.

## 6. RECOVERY AND RESTORATION

- Systems or data impacted will be restored from Redstor-certified nightly backups.
- Verification will be conducted to ensure integrity and full functionality

## 7. POST-INCIDENT REVIEW AND CONTINUOUS IMPROVEMENT

- A lessons-learned review will be held with the team to identify improvements.
- Security policies, Sendmarc email controls, and access protocols will be updated as necessary

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

## 8. DOCUMENTATION & EVIDENCE

- All incidents must be fully documented in an Incident Register.
- Incident reports, escalation logs, and corrective actions to be maintained.
- Copies of reports, certificates, and remedial actions must be stored securely and made available to auditors or clients upon request.

| 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 SIGNATURES | | |
|---|---|---|
| **TITLE** | **NAME** | **EMAIL** |
| CEO | Corné Eloff | corne.eloff@geoterraimage.com |
| SIGNATURE | Corne Eloff Digitally signed by Corne Eloff Date: 2025.09.08 10:36:45 +02'00' | |

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

# INFORMATION SECURITY INCIDENT REPORT FORM

**Incident Number:** _____
**Date & Time of Incident:** _____
**Reported By (Name & Position):** _____
**Department / Project:** _____

---

**1. Incident Details**

- **Type of Incident:**
  - ☐ Data Breach
  - ☐ Unauthorized Access
  - ☐ System Outage
  - ☐ Malware / Virus / Ransomware
  - ☐ Loss/Theft of Device or Data
  - ☐ Other: _____
- **Description of Incident:**

---

- **Location / System Affected:**

---

**2. Initial Response**

- **Immediate Actions Taken (containment/mitigation):**

---

- **Reported To (IT/Security/Management):** _____

---

**3. Impact Assessment**

- **Severity Level:**
  - ☐ Critical
  - ☐ High
  - ☐ Medium
  - ☐ Low
- **Potential/Actual Impact:**
  - ☐ Data Loss
  - ☐ Service Downtime
  - ☐ Confidentiality Breach
  - ☐ Financial Loss
  - ☐ Reputational Risk
  - ☐ Other: _____

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

**4. Root Cause (if known):**

---

**5. Recovery Actions**

- **System/Data Restored from Backup?** ☐ Yes ☐ No
- **Date & Time of Recovery:** _____
- **Steps Taken to Ensure Integrity:**

---

**6. Follow-Up / Preventative Measures**

- **Corrective Actions Implemented:**
- **Policy/Procedure Updates Required:** ☐ Yes ☐ No
  If Yes, details: _____

---

**Reported By:** _____ (Signature & Date)

**Reviewed By (IT/Security):** _____

**Approved By (Management):** _____