DATA BREACH RESPONSE PLAN

Plan Version: 1.0 Effective Date: 4 June 2025 Last Updated: 4 June 2025

1. Purpose and Scope

This Data Breach Response Plan ("the Plan") outlines the procedures for preparing for, detecting, responding to, and recovering from any suspected or actual data breach involving personal information processed by Insight Intel. Its purpose is to minimize harm to data subjects, mitigate operational impact, ensure compliance with legal and regulatory obligations (especially POPIA), and preserve the trust and reputation of Insight Intel.
This Plan applies to all personal information (including special personal information and unique identifiers) processed by Insight Intel, regardless of its format, location (on-site or cloud), or the individuals involved (employees, contractors, third-party operators).

2. Definition of a Data Breach

A "data breach" (or "security compromise" as per POPIA) refers to any incident where there is a reasonable belief that the integrity, confidentiality, or availability of personal information has been compromised. This includes, but is not limited to:

- Loss or accidental destruction of personal information.
- Unauthorised access to or acquisition of personal information.
- Unlawful disclosure of personal information.
- Cyber-attacks (e.g., ransomware, phishing leading to credentials compromise, malware).
- Physical theft of devices (laptops, USBs) containing unencrypted personal information.
- Accidental disclosure (e.g., sending an email with personal data to the wrong recipient).

3. Data Breach Response Team (DBRT) & Roles

A dedicated Data Breach Response Team (DBRT) is established to lead the response efforts.

- Information Officer: Anemi van Schalkwyk
  - Responsibilities: Overall strategic oversight, final decision-making authority for notifications, liaison with legal counsel, Information Regulator, and executive management.
- Legal & Compliance Lead: Brits Law
  - Responsibilities: Legal assessment of the breach, regulatory notification requirements, drafting breach notifications, advising on data subject rights, managing external legal counsel.
- IT/Technical Lead: IT Manager
  - Responsibilities: Technical investigation, containment, eradication, recovery, forensic analysis, implementing security enhancements, liaison with external cybersecurity experts.
- Communications Lead: Communication Officer
  - Responsibilities: Drafting internal and external communications (excluding formal legal notifications), managing media inquiries (if applicable), reputation management.

Contact Information for DBRT (Internal):

- Anemi van Schalkwyk: +27 79 590 4083, anemi@insightintel.co.za

External Contacts (Pre-approved):

- Legal Counsel: Brits Law, Anrich van Stryp, +27 12 140 3495, anrich@britslaw.com

4. Phases of Data Breach Response

This Plan is structured into six phases:

Phase 1: Preparation (BEFORE a Breach)

- Policy & Plan Development: Maintain and regularly review this Data Breach Response Plan, the Data Handling & Processing Policy, and the Information Security Policy.
- DBRT Establishment: Define roles, responsibilities, and contact details for the DBRT.
- Training: Conduct mandatory, regular data protection and breach response training for all employees, especially DBRT members.
- Technical Readiness: Implement and maintain robust security measures (encryption, access controls, monitoring systems, backups). Ensure incident detection and logging capabilities.
- External Contacts: Identify and establish relationships with external legal, forensic, and PR support.
- Tabletop Exercises: Conduct periodic simulated breach exercises with the DBRT to test the plan's effectiveness and identify gaps.
- Asset Inventory: Maintain an up-to-date inventory of all systems, applications, and locations where personal information is stored.

Phase 2: Detection & Assessment (IMMEDIATE RESPONSE)

- Identification: Any employee who suspects or detects a data breach (e.g., unusual system activity, lost device, suspicious email, external notification) MUST immediately report it to the Information Officer.
- Initial Triage (Information Officer):
    - Verify the report.
    - Assess the apparent scope and nature of the suspected breach (e.g., what data, what systems, who is affected).
    - Convene the DBRT immediately.
- Initial Assessment (DBRT):
    - Confirm the Breach: Determine if a security compromise has indeed occurred.
    - Categorize: Classify the type of breach (e.g., unauthorized access, loss, destruction).
    - Preliminary Impact Assessment: Identify the type of personal information involved (e.g., names, contact details, special personal information, unique identifiers), the number of data subjects potentially affected, and the potential severity of harm.

Phase 3: Containment & Eradication (STOP THE BLEEDING)

- Isolate: Immediately isolate affected systems or networks to prevent further unauthorized access or spread of the breach. (e.g., disconnect devices, disable compromised accounts).
- Stop the Cause: Identify and eliminate the root cause of the breach (e.g., patch vulnerabilities, remove malware, change compromised credentials).
- Preserve Evidence: Securely collect and preserve all relevant logs, images, and other forensic evidence for investigation.
- Document Actions: Meticulously document all steps taken during containment.

Phase 4: Recovery & Remediation (RESTORE & STRENGTHEN)

- System Restoration: Restore affected systems and data from secure, uncompromised backups.
- Integrity Verification: Verify the integrity and security of restored systems before bringing them back online.
- Vulnerability Remediation: Implement permanent fixes for the vulnerabilities exploited during the breach.
- Enhanced Security: Consider implementing additional security controls identified as necessary during the breach analysis.
- Monitor: Implement enhanced monitoring to detect any recurrence of the breach activity.

Phase 5: Notification (COMMUNICATE RESPONSIBLY)

- Legal Assessment (Legal & Compliance Lead): Determine the specific notification requirements based on POPIA and any other applicable laws (e.g., if international data subjects are involved).
    - POPIA Requirement: You must notify the Information Regulator and affected data subjects "as soon as reasonably possible" after the discovery of a security compromise. This is typically

interpreted as within 72 hours if possible, though POPIA does not specify an exact timeframe other than "as soon as reasonably possible."

- Notification to Information Regulator:
  - When: As soon as reasonably possible after discovery.
  - Content: Nature of the breach, categories of information involved, likely consequences, measures taken, proposed measures to address the breach, and mitigating effects.
  - Method: Via official channels provided by the Information Regulator (e.g., dedicated online portal or email).
- Notification to Affected Data Subjects:
  - When: As soon as reasonably possible after discovery, if there is a reasonable belief that personal information has been accessed or acquired by an unauthorised person.
  - Content (as per POPIA Section 22④):
    - Description of the compromise.
    - Description of the likely consequences of the compromise.
    - Description of the measures taken or proposed to be taken by Insight Intel to address the compromise.
    - Recommendation of measures to be taken by the data subject to mitigate the possible adverse effects.
    - If known, the identity of the unauthorised person who may have accessed or acquired the personal information.
  - Method: Direct communication where possible (e.g., email, SMS, postal mail). If direct communication is not feasible (e.g., too many data subjects or no contact details), indirect methods may be considered (e.g., website notice, public announcement, but always consult with the Information Regulator first).
- Client Notification: Inform affected clients whose data or data subjects' information was involved, as per contractual obligations and professional courtesy.
- Internal Communication: Inform relevant internal stakeholders (e.g., executive management) about the breach and response progress.

Phase 6: Post-Breach Review & Learnings (CONTINUOUS IMPROVEMENT)

- Lessons Learned Session: Convene the DBRT and relevant stakeholders for a comprehensive review meeting after the breach is fully resolved.
  - What happened?
  - How did the Plan perform?
  - What went well? What could be improved?
  - Was the cause fully eradicated?
  - Were all legal obligations met?
- Root Cause Analysis: Conduct a thorough investigation to identify the definitive root cause of the breach.
- Action Plan: Develop and implement an action plan based on lessons learned to strengthen security controls, update policies and procedures, and enhance training.
- Documentation: Prepare a final incident report detailing the entire breach lifecycle, findings, and remediation actions.

5. Documentation & Record-Keeping

Accurate and thorough documentation is critical at every stage of the breach response. All actions, decisions, communications, and evidence must be logged and maintained, including:

- Date and time of discovery.
- Nature and scope of the breach.
- Personal information affected.
- All DBRT activities, decisions, and rationale.
- Communications with the Information Regulator, data subjects, and clients.
- Forensic analysis reports.
- Remediation steps taken.
- Post-breach review findings.