Incident Response & Breach Notification Policy

Policy for Security Incident Handling and Regulatory Breach Notification

Governance & Ownership

Policy Owner: Key Account Manager (Head of Operations)
Executive Sponsor: Company Director
Reviewer: Key Account Manager (Head of Operations)
Legal Review: External Legal Counsel (if applicable)
Approved By: Company Director

Version & Review Control

Version	Effective Date	Review Frequency	Next Review Date
1.0	March 2026	Annually	March 2027

Document Classification

Classification: Internal Use Only

Confidentiality Statement

This policy is the property of Genesys Creative Systems. It is intended for internal use only and may not be distributed, reproduced, or disclosed to any external party without the prior written approval of the Head of Operations or Company Director.

Introduction

This Incident Response and Breach Notification Policy establishes Genesys Creative Systems' approach to identifying, reporting, responding to, and recovering from information security incidents.

The policy supports the protection of information assets and ensures that incidents are managed in a timely and effective manner, in accordance with applicable legal and regulatory requirements, including POPIA.

Purpose & Scope

The purpose of this policy is to:

- Define a structured approach for the identification, reporting, and management of information security incidents
- Ensure compliance with applicable breach notification requirements, including POPIA Section 22
- Minimise the impact of incidents on business operations, systems, and data

Scope includes:

- All employees, contractors, and third-party service providers who access or process information on behalf of Genesys Creative Systems
- All systems, applications, cloud services, and infrastructure used by Genesys Creative Systems or its service providers
- All information security incidents, including those involving personal information, client data, or business systems

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA Section 22: mandatory notification of security compromises to the Information Regulator and affected individuals.
- Companies Act (2008): accountability for IT governance.
- King IV: oversight of technology and IT risk.

Best Practice References:

- NIST SP 800-61r2 – Computer Security Incident Handling Guide.
- ISO/IEC 27035 – Information Security Incident Management.

Policy Requirements

Incident Identification & Reporting

All employees, contractors, and service providers must promptly report any suspected or actual information security incidents.

- Suspected incidents must be reported as soon as possible through defined internal channels (e.g. email, messaging, or direct escalation)
- Incidents may include, but are not limited to: unauthorised access, data loss, phishing, system compromise, or suspicious activity
- All reported incidents must be logged and tracked for follow-up

Incident Classification

Incidents must be assessed and classified based on their impact and severity:

- Security Event: Any observable occurrence within a system or network (e.g. failed login attempt)
- Security Incident: An event that may compromise the confidentiality, integrity, or availability of systems or information
- Personal Data Breach: A security incident involving the unauthorised access, disclosure, alteration, or loss of personal information
- Major Incident / Breach: An incident that significantly impacts business operations, systems, or involves sensitive or regulated data requiring escalation or notification

Incident Response Lifecycle

Genesys Creative Systems must follow a structured approach to managing incidents:

1. Identification – Detect and report suspected incidents immediately, including any suspected compromise of personal information
2. Containment – Limit the impact by isolating affected systems or access
3. Eradication – Remove the root cause (e.g. malicious activity, vulnerabilities)
4. Recovery – Restore systems and services to normal operation
5. Notification – Notify relevant parties where required
6. Lessons Learned – Review the incident and improve controls

Incident Management & Coordination

Incidents must be managed in a coordinated and controlled manner:

- Responsibility for managing incidents must be assigned to an appropriate individual (e.g. Operational Lead)
- Relevant internal stakeholders and service providers must be engaged where required

- Actions taken during incident response should be documented where feasible
- External support (e.g. hosting providers or developers) may be engaged to assist with investigation and remediation

Regulatory & Breach Notification

Where personal information is involved, breach notification must be handled in accordance with applicable legal requirements:

- Any incident involving personal information must be assessed to determine whether it constitutes a notifiable data breach
- Where required, the Information Regulator must be notified as soon as reasonably possible in accordance with POPIA
- Affected individuals must be notified where there is a risk of harm or where required by law
- Notifications should include: Nature of the incident, Type of data affected, Potential impact, Steps taken to mitigate the risk, Contact details for further information
- Where appropriate, Genesys Creative Systems should aim to provide timely initial notification, followed by updates as more information becomes available

Evidence Handling

Information relating to incidents, including personal information, must be preserved to support investigation and reporting:

- Relevant logs, records, and supporting information should be retained where feasible
- Evidence should be handled in a manner that preserves its integrity
- Access to incident-related information must be restricted to authorised individuals

Post-Incident Review

Following significant incidents, a review should be conducted to identify improvements:

- Root causes should be analysed and documented
- Lessons learned should be used to improve processes, controls, and awareness
- Relevant policies, procedures, or configurations should be updated where necessary

Roles & Responsibilities

- Company Director: Ultimate accountability for information security governance, risk management, and compliance.
- Key Account Manager (Head of Operations): Responsible for the day-to-day implementation, enforcement, and coordination of information security controls and policies. Ensures that security practices are embedded in business operations.
- Technology Service Providers (Internal or External): Responsible for the technical implementation, configuration, maintenance, and support of systems and security controls, including cloud platforms, hosted environments, and custom-developed

applications. This includes managing security configurations, applying updates, and supporting incident response where required.

- Employees & Contractors: Must comply with all information security policies, procedures, and controls. Responsible for protecting company information, using systems securely, and reporting any suspected security incidents.
- Third-Party Service Providers: Must comply with Genesys Creative Systems' security requirements as defined in contracts and agreements. Responsible for protecting any systems or data they access or process on behalf of the organisation.

Exceptions

Exceptions to this policy must be documented, justified, and approved by the Head of Operations. All exceptions shall be recorded in the Risk Register. High-risk exceptions require escalation to the Company Director.

Consequences of Non-Compliance

Non-compliance with this policy may result in disciplinary action (employees), termination of contract (vendors/contractors), and potential reporting to regulatory authorities under POPIA.

Monitoring & Enforcement

Genesys Creative Systems must monitor the effectiveness of its incident response processes to ensure that security incidents are identified, managed, and resolved in a timely and appropriate manner.

- Security incidents and potential breaches must be monitored and tracked to ensure appropriate response and resolution
- Incidents involving personal information must be reviewed to determine whether notification obligations apply
- Lessons learned from incidents should be used to improve security controls and response processes
- Where applicable, third-party service providers must support incident response activities and provide relevant information or assistance

Where non-compliance or gaps are identified:

- Corrective actions must be implemented to address weaknesses in incident detection, response, or communication
- Additional controls, training, or oversight may be introduced to improve response capability
- Significant issues may be escalated to management for oversight and decision-making

Acknowledgement

All employees and contractors are required to:

- Read and understand this policy

- Comply with its requirements
- Acknowledge adherence as part of onboarding and ongoing employment obligations

This policy is made available via the organisation's internal document repository.

Oversight & Review

This policy will be reviewed annually by the Head of Operations and updated as required to reflect changes in regulation, technology, or organisational needs.

Document Control & Version History

Version	Date	Owner	Reviewer	Approved By	Next Review Date
1.0	March 2026	Key Account Manager (Head of Operations)	Key Account Manager (Head of Operations)	Company Director	March 2027

Version History

Version	Date	Description of Changes	Author	Reviewer
1.0	March 2026	Initial version aligned with POPIA and best practices (ISO, NIST)	Key Account Manager (Head of Operations)	Key Account Manager (Head of Operations)