Information Security Policy

Overarching Policy for Information and Technology Governance

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 Information Security Policy defines Genesys Creative Systems' overall approach to protecting its information assets, systems, and services.

The policy establishes the organisation's commitment to maintaining the confidentiality, integrity, and availability of information and ensuring that security risks are managed appropriately.

Purpose

The purpose of this Information Security Policy is to:

- Establish a consistent and risk-based approach to information security
- Protect company and client information from unauthorised access, disclosure, or loss
- Define the governance framework for information security within Genesys Creative Systems
- Support compliance with applicable legal, regulatory, and contractual requirements (including POPIA)

Scope

This policy applies to:

- All employees, contractors, and third parties with access to Genesys Creative Systems' information and systems.
- All technology platforms, cloud services, and websites managed by Genesys Creative Systems.
- All information assets, including personal information, financial data, intellectual property, and operational records.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA (Act 4 of 2013), Sections 19 and 22
- King IV Report on Corporate Governance
- Companies Act (2008)
- Labour Law requirements (employee conduct)

Best Practice References

- NIST Cybersecurity Framework v2 (2024)
- ISO/IEC 27001 & 27002
- GDPR (international privacy benchmark)

- NIS2 Directive (EU 2022/2555 – best practice for governance & incident response)

Policy Requirements

Genesys Creative Systems commits to safeguarding the confidentiality, integrity, and availability of all information assets. This Information Security Policy provides the umbrella for all supporting information security policies, which cover access, encryption, remote workforce, vendor management, and other domains. Security practices shall be proactive, risk-based, and aligned with legal obligations under POPIA, GDPR and other international standards

Information Security Principles

Genesys Creative Systems must apply the following core principles:

- Least Privilege: Access to systems and data must be limited to what is necessary
- Defence in Depth: Multiple layers of security controls should be applied where appropriate
- Data Protection: Information must be protected throughout its lifecycle
- Accountability: Users are responsible for protecting company information and systems
- Risk-Based Approach: Security controls must be proportionate to the level of risk

Governance & Responsibilities

Information security is a shared responsibility across the organisation.

- The Company Director is ultimately accountable for information security
- The Head of Operations is responsible for implementing and overseeing security practices
- Employees, contractors, and third parties are responsible for complying with security policies and reporting incidents
- External service providers must meet agreed security requirements

Security Control Domains

Genesys Creative Systems must implement and maintain appropriate controls across key security domains, including:

- Access control and identity management
- Endpoint and device security
- Data protection and encryption
- Logging and monitoring
- Incident response and breach notification
- Business continuity and disaster recovery

- Acceptable use of systems and services

Risk Management

Information security risks must be identified, assessed, and managed appropriately.

- Security risks should be considered when implementing new systems, services, or processes
- Appropriate controls must be applied to reduce risks to acceptable levels
- Significant risks should be escalated to management

Compliance

Genesys Creative Systems must comply with applicable legal, regulatory, and contractual requirements.

- This includes compliance with POPIA and other relevant data protection obligations
- Security practices must align with client and partner requirements where applicable
- Non-compliance must be addressed through appropriate corrective actions

Policy Framework

This policy is supported by a set of related policies and standards, including but not limited to:

- Access Control and Identity Management Policy
- Endpoint and Device Security Policy
- Acceptable Use Policy
- Privacy and Data Protection Policy
- Data Retention and Disposal Policy
- Data Security and Encryption Policy
- Logging and Monitoring Policy
- Incident Response and Breach Notification Policy
- Business Continuity and Disaster Recovery Policy

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 compliance with this policy and its supporting policies to ensure that information security practices are effective and appropriate.

- Security practices and controls should be reviewed periodically to ensure continued effectiveness
- Compliance with supporting policies should be monitored and reinforced through ongoing activities and awareness
- Security incidents, risks, or policy violations must be identified and managed in accordance with defined processes

Where non-compliance or risks are identified:

- Corrective actions must be implemented to address identified gaps
- Access to systems or services may be restricted where necessary to mitigate risk
- Significant issues may be escalated to management for oversight and resolution

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)