Cloud Security Policy

Policy for Secure Use of Cloud Services and Technologies

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 Cloud Security Policy establishes the requirements for securely adopting, managing, and using cloud services at Genesys Creative Systems. As a cloud-first company, Genesys Creative Systems relies on SaaS, PaaS, and IaaS solutions to support its business operations. This policy ensures that cloud services are configured, managed, and used in compliance with regulatory requirements and industry best practices.

Purpose & Scope

The purpose of this policy is to:

- Define security requirements for the selection and use of cloud service providers.
- Clarify responsibilities under the shared responsibility model.
- Ensure encryption, authentication, and monitoring are consistently applied.
- Protect personal and business data stored or processed in the cloud.

Scope includes:

- All cloud services used for business purposes (SaaS, PaaS, IaaS).
- Employees, contractors, and third parties accessing Genesys Creative Systems cloud environments.
- Any data, systems, or services hosted in third-party cloud infrastructure.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA Section 19: requires security safeguards when processing personal information.
- POPIA Section 21: operator agreements when third parties process personal information.
- Companies Act (2008): accountability for IT governance.
- King IV: oversight of IT risk and cloud adoption.

Best Practice References:

- ISO/IEC 27017 – cloud-specific information security controls.
- ISO/IEC 27018 – protection of personal data in cloud computing.
- Cloud Security Alliance (CSA) Cloud Controls Matrix.
- NIST Cybersecurity Framework v2.0 – cloud implementation guidance.

Policy Requirements

Cloud Security Controls

Genesys Creative Systems must ensure that cloud services are selected, configured, and managed in a secure manner to protect systems and data.

- Cloud service providers should demonstrate appropriate security practices, such as recognised certifications (e.g. ISO 27001, SOC 2), where available
- Data must be protected through encryption in transit and at rest where supported
- Multi-Factor Authentication (MFA) must be enabled for administrative and privileged access
- Access to cloud services must follow the principles of least privilege and role-based access control (RBAC)
- Cloud services must support logging and monitoring capabilities appropriate to the level of risk
- Providers must notify Genesys Creative Systems of security incidents in accordance with contractual obligations

Cloud Service Usage & Approval

The use of cloud services must be controlled to reduce risk and prevent unauthorised systems from being introduced.

- All cloud services must be reviewed and approved prior to use
- Unauthorised or unapproved cloud services (shadow IT) must not be used for business purposes
- Cloud services must be assessed for security, privacy, and business suitability prior to procurement
- Personal information must be stored and processed in accordance with applicable data protection requirements (e.g. POPIA)

Shared Responsibility Model

Responsibilities for cloud security must be clearly understood and managed between Genesys Creative Systems and cloud service providers.

- Cloud service providers are responsible for the security of the underlying infrastructure and platform services
- Genesys Creative Systems is responsible for the secure configuration and use of cloud services, including identity management, access control, and monitoring
- Responsibilities must be clearly defined in agreements with providers
- Any identified security gaps must be addressed prior to production use

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 use and security of cloud services to ensure that they are configured and managed in accordance with this policy.

- Cloud environments should be monitored through available logging and audit capabilities where feasible
- Access to cloud systems must be reviewed periodically to ensure it remains appropriate and aligned to business needs
- Configuration and security settings should be reviewed periodically to identify misconfigurations or risks
- Any security incidents or suspicious activity within cloud services must be investigated and managed in accordance with incident response processes

Where non-compliance or security weaknesses are identified:

- Issues must be addressed through appropriate corrective actions and configuration updates

- Access may be restricted or removed where necessary to mitigate risk
- 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)
