Data Protection & Encryption Policy

Policy Protecting Data at Rest, In Transit, and During Disposal

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 Data Security and Encryption Policy defines Genesys Creative Systems' approach to protecting information through appropriate security controls, including encryption of data at rest and in transit.

The policy supports the protection of personal and business information in accordance with applicable data protection requirements, including POPIA.

Purpose & Scope

The purpose of this policy is to ensure that sensitive and personal information is protected against unauthorised access, disclosure, or alteration through the use of appropriate encryption and security controls.

Scope includes:

- All personal and business information processed by Genesys Creative Systems
- Data stored on devices, cloud platforms, and third-party services
- Data transmitted across internal, public, or third-party networks
- Backups, archives, and removable media

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- Protection of Personal Information Act (POPIA) – Section 19 (security safeguards), Section 14 (retention & disposal).
- Companies Act (2008) – accountability of directors.
- King IV – governance of technology and information assets.

Best Practice References:

- ISO/IEC 27001 & 27002 (Annex A.8, A.10 – data protection, encryption).
- NIST Cybersecurity Framework v2.0 – PR.DS (Data Security).
- NIS2 Directive & GDPR – as best practice for breach prevention and encryption standards.

Policy Requirements

Data Protection Controls

Genesys Creative Systems must implement appropriate controls to protect sensitive and personal information.

- Sensitive and personal information should be protected using encryption where supported
- Access to data must be restricted based on the principle of least privilege
- Backups must be protected and secured appropriately
- Removable media must be used only where necessary and protected where applicable
- Industry-standard encryption protocols (e.g. AES-256, TLS 1.2 or higher) should be used where supported

Encryption of Data at Rest

- Data stored on devices, cloud platforms, and storage systems should be encrypted where supported
- Full disk encryption must be enabled on user devices where feasible
- Cloud service providers should provide encryption capabilities for stored data

Encryption of Data in Transit

- Data transmitted over networks must be protected using secure protocols (e.g. HTTPS, TLS)
- Unsecured or legacy protocols must not be used for transmitting sensitive information

Key and Credential Protection

- Access to systems and sensitive data must be protected using strong authentication mechanisms
- Credentials and secrets must not be stored in plain text
- Access to sensitive configuration or secrets must be restricted to authorised individuals

Third-Party and Cloud Security

- Cloud and third-party providers must implement appropriate security controls, including encryption where applicable
- Providers should demonstrate recognised security practices or certifications where available

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 implementation of data protection and encryption controls to ensure that sensitive and personal information is adequately protected.

- Data protection practices should be reviewed periodically to ensure that encryption and security controls are applied where appropriate
- Systems and services should be reviewed to confirm that secure configurations (e.g. encrypted storage, secure communication protocols) are in place where supported
- Access to sensitive data and systems should be reviewed periodically to ensure appropriate controls are maintained
- Where third-party or cloud providers are used, their security capabilities (including encryption) should be monitored through ongoing engagement and contractual oversight

Where non-compliance or risks are identified:

- Appropriate corrective actions must be implemented to address gaps in encryption or data protection controls
- Access to systems or data may be restricted where necessary to mitigate identified risks
- 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)
