Secure Data Retention & Disposal Policy

Policy for the Management, Retention, and Secure Disposal of Genesys Creative Systems Information Assets

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 Secure Data Retention & Disposal Policy establishes requirements for the retention, storage, and secure disposal of Genesys Creative Systems' information assets. The policy ensures compliance with legal, regulatory, and contractual requirements while reducing the risk of data breaches and unauthorised disclosures.

Purpose & Scope

The purpose of this policy is to:

- Ensure that information is retained only for as long as necessary to fulfil its intended purpose
- Support compliance with applicable legal and regulatory requirements (including POPIA)
- Reduce the risk of unauthorised access, data breaches, or unnecessary data exposure
- Ensure that information is securely destroyed when no longer required.

Scope includes:

- All employees, contractors, and third parties who process Genesys Creative Systems data.
- Electronic and paper-based information under Genesys Creative Systems' control.
- Data stored on company devices, servers, cloud services, or with third-party vendors.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA Section 14: personal information may not be retained longer than necessary for its lawful purpose.
- Companies Act (2008): defines retention requirements for statutory records.

Best Practice References:

- ISO/IEC 27001 Annex A.11.2.7 – secure disposal of media.
- ISO/IEC 27018 – protection of personal data in the cloud.
- NIST SP 800-88 – Guidelines for Media Sanitisation.

Policy Requirements

Data Handling Principles

Genesys Creative Systems must ensure that information is handled in a secure and responsible manner throughout its lifecycle, including creation, storage, use, retention, and disposal.

- Information must be handled in accordance with its sensitivity and business purpose
- Access to data must be restricted based on the principle of least privilege
- Personal information must be processed in accordance with applicable data protection requirements (e.g. POPIA)
- Data subject to legal holds or investigations must not be deleted until authorised

Data Retention

Information must be retained only for as long as necessary to fulfil business, legal, and regulatory requirements, and in alignment with the purpose for which it was collected.

- Personal information must be retained only for the duration required to fulfil the original purpose and lawful basis for processing
- Financial records must be retained for a minimum of 7 years in accordance with applicable legislation
- Employment-related records must be retained for an appropriate period following termination (e.g. 5 years)
- Client and project records should be retained for a defined period (e.g. 5 years post-contract), unless longer retention is required
- Marketing and campaign data must not be retained beyond its useful lifecycle (e.g. 12 months) unless renewed consent or another lawful basis is established
- Information subject to legal, regulatory, or investigation requirements must not be deleted until appropriate clearance is obtained

Data Subjects Rights Consideration

Personal information must be deleted or anonymised where retention is no longer necessary, or where a valid request for deletion is received and no legal basis for retention exists.

Secure Disposal

Information must be securely disposed of when no longer required, to prevent unauthorised access or reconstruction.

- Paper records must be securely destroyed (e.g. shredding or equivalent methods)
- Electronic data must be securely erased using appropriate methods to prevent recovery

- Removable media must be securely wiped or physically destroyed where appropriate
- Data stored in cloud services must be deleted in accordance with provider capabilities and contractual agreements
- Where feasible, confirmation of secure deletion should be obtained for sensitive or critical data

Third-Party Data Handling & Disposal

Where third parties process or store data on behalf of Genesys Creative Systems:

- Vendors must comply with defined data retention and disposal requirements
- Vendors must securely delete or return data upon request or contract termination
- Where appropriate, vendors should provide written confirmation of secure data destruction

Exceptions & Legal Holds

- Information required for legal, regulatory, or investigative purposes must not be deleted until authorised
- Any exceptions to defined retention periods must be justified and approved

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.

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 data retention and disposal requirements to ensure that information is retained only as long as necessary and securely disposed of when no longer required.

- Data retention practices should be reviewed periodically to ensure alignment with business, legal, and regulatory requirements
- Data stores (e.g. cloud platforms, applications, and shared repositories) should be reviewed to identify information that is no longer required
- Disposal activities should be performed and documented where feasible, particularly for sensitive or personal information
- Where third parties process or store data, their compliance with retention and disposal requirements should be monitored through ongoing engagement and contractual controls

Where non-compliance or risks are identified:

- Data that exceeds defined retention periods must be reviewed and securely disposed of where appropriate
- Corrective actions must be implemented to address gaps in retention or disposal practices
- 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)