Acceptable Use Policy (AUP)

Policy for Responsible Use of Genesys Creative Systems Technology, Networks, and Services

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 Acceptable Use Policy (AUP) establishes the requirements for the responsible use of Genesys Creative Systems' systems, networks, cloud platforms, and services.

This policy ensures that employees, contractors, and third parties use Genesys Creative Systems resources in a secure, ethical, and lawful manner, aligned with regulatory and organisational obligations.

Purpose & Scope

The purpose of this policy is to:

- Promote the secure and responsible use of company systems and data
- Reduce the risk of security incidents, data loss, and misuse of resources
- Ensure that users understand their responsibilities when accessing company systems

Scope includes:

- All employees, contractors, and third-party service providers
- All devices used to access company systems or data (including personal devices where applicable)
- All systems, applications, cloud services, and communication platforms used for business purposes

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA – Section 19: requires security safeguards to protect personal information.
- Companies Act (2008): director accountability for governance and IT use.
- King IV: ethical and responsible use of technology.

Best Practice References:

- ISO/IEC 27001 Annex A.8 – asset use and user responsibilities.
- NIST Cybersecurity Framework v2.0 – PR.AC (Access Control).

Policy Requirements

General Use of Systems

Company systems and services must be used responsibly and primarily for authorised business purposes.

- Limited personal use is permitted where it does not interfere with work duties, security, or compliance requirements
- Users must act in a professional and responsible manner when using company systems and services
- All use of systems must comply with applicable laws, regulations, and company policies

Acceptable Use of Communication & Systems

Users must use company communication platforms and systems in a secure and appropriate manner.

- Email, messaging, and collaboration tools must be used professionally and must not be used to transmit inappropriate or harmful content
- Users must not access, download, or distribute illegal, offensive, or inappropriate material
- Company systems must not be used to introduce malicious software or unauthorised tools

Protection of Company Information

Users are responsible for protecting company and client information.

- Confidential or sensitive information must not be disclosed without authorisation
- Company information must only be accessed, stored, and shared using approved systems and platforms
- Personal or public cloud storage services must not be used to store company or client data unless explicitly approved
- Care must be taken when sharing information externally to ensure it is sent to authorised recipients only

Secure Use of Devices and Networks

Devices and network access must be used securely to prevent unauthorised access or data exposure.

- Users must not disable or bypass security controls on devices or systems
- Only approved or trusted software and applications may be installed or used for business purposes

- Public or unsecured networks must be used with caution, particularly when accessing sensitive systems or data
- Devices must be protected from unauthorised access and not left unattended in unsecured environments

Account and Access Responsibilities

Users are responsible for maintaining the security of their accounts and access credentials.

- Login credentials must not be shared or disclosed
- Users must not attempt to gain unauthorised access to systems or data
- Suspicious activity or potential security incidents must be reported promptly

Use of Artificial Intelligence (AI) Tools

The use of Artificial Intelligence (AI) tools (e.g. generative AI platforms) must be conducted in a secure and responsible manner.

- Company or client confidential information must not be entered into public AI tools unless explicitly approved
- AI tools must not be used to process personal information unless appropriate safeguards and approvals are in place
- Outputs generated by AI tools must be reviewed and validated before use in business activities
- AI tools must not be used to generate or distribute misleading, harmful, or inappropriate content
- Only approved AI tools or services should be used for business purposes where feasible

Prohibited Activities

The following activities are strictly prohibited:

- Use of company systems for unlawful or unauthorised purposes
- Accessing, downloading, or distributing illegal, offensive, discriminatory, or inappropriate content
- Introduction of malicious software, hacking tools, or unauthorised monitoring tools
- Installation or use of unauthorised applications, services, or tools (including shadow IT)
- Sharing of login credentials or enabling unauthorised access to systems or data
- Use of company systems for personal commercial gain or external business activities without approval

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 of its systems, devices, and services to ensure compliance with this policy and to protect company and client information.

- Use of company systems, applications, and communication platforms may be monitored where appropriate to detect misuse or security risks
- Security incidents, policy violations, or inappropriate use must be reported and investigated in accordance with incident response processes
- Use of unauthorised tools or services (including AI tools) should be identified and addressed where feasible
- User behaviour and adherence to this policy should be reinforced through ongoing awareness and communication

Where non-compliance or misuse is identified:

- Access to systems or services may be restricted or removed where necessary to mitigate risk
- Corrective actions (e.g. removal of unauthorised software, guidance to users) must be implemented
- Repeated or significant violations may be escalated to management for further action

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)