Access Control & Identity Management Policy

Policy for Managing User Identities, Authentication, and Access Rights

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 Access Control and Identity Management Policy defines Genesys Creative Systems' approach to managing user identities and controlling access to systems, applications, and data.

The policy ensures that access is granted only to authorised individuals and is aligned to business requirements and the principle of least privilege.

Purpose & Scope

The purpose of this policy is to:

- Ensure that access to systems and data is restricted to authorised users
- Establish controls for user account lifecycle management, authentication, and authorisation
- Reduce the risk of unauthorised access and misuse of information

Scope includes:

- All employees, contractors, and third-party service providers who access Genesys Creative Systems' systems or data
- All systems, applications, cloud platforms, and SaaS services used by Genesys Creative Systems
- All types of accounts, including user accounts, privileged accounts, service accounts, and API access

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- Protection of Personal Information Act (POPIA) – Section 19 (security safeguards).
- Companies Act (2008) – accountability of directors.
- King IV – governance of technology and access management.

Best Practice References:

- ISO/IEC 27001 & 27002 (Annex A.9 – access control).
- NIST Cybersecurity Framework v2.0 – PR.AC (Access Control).
- NIS2 Directive & GDPR – best practice for access logging and accountability.

Policy Requirements

Identity & Account Management

All users must be uniquely identifiable and managed through controlled account processes.

- Each user must have a unique account; shared accounts are not permitted except where required for technical purposes (e.g. service accounts)
- User accounts must be created, modified, and removed through a controlled process
- Access must be linked to an identifiable individual at all times
- Default credentials must be changed prior to use

Access Provisioning (Joiner–Mover–Leaver)

Access to systems must be managed throughout the user lifecycle.

- Access must be granted based on job role and business requirements (role-based access control)
- Access must be limited to the minimum necessary (least privilege), particularly for systems containing personal or sensitive information
- New access must be approved prior to provisioning
- Access must be updated or removed when roles or responsibilities change
- Access must be revoked promptly upon termination of employment or contract

Authentication & Credential Security

Strong authentication controls must be implemented to protect access to systems and data.

- Passwords must not be stored in plain text and should be managed using approved tools (e.g. password managers)
- Passwords must be a minimum of 12 characters in length and should be sufficiently complex or use passphrases
- Passwords must not be reused across multiple systems or services
- Passwords must not be shared or stored in plain text
- Passwords should be stored using approved tools (e.g. password managers)
- Multi-Factor Authentication (MFA) must be enabled for privileged access and remote access
- Accounts should be protected against brute-force attacks (e.g. lockout after repeated failed attempts)
- Authentication controls must be appropriate to the sensitivity of the system and data being accessed

- Single Sign-On (SSO) or federation should be used where supported

Privileged Access Management

Privileged access must be strictly controlled and monitored.

- Administrative access must be limited to authorised individuals only
- Privileged accounts should be separate from standard user accounts
- Use of privileged access should be minimised and controlled
- Privileged activities should be logged where supported
- Privileged access to systems containing sensitive or personal information must be strictly limited and controlled

Service Accounts & API Access

Service accounts and non-human access must be securely managed.

- Service accounts and API access must be restricted to defined purposes
- Credentials must be protected and not embedded in code or exposed in plain text
- Access keys and secrets should be rotated periodically or upon suspected compromise
- Usage of service accounts should be monitored where feasible

Access Reviews

Access rights must be reviewed periodically to ensure continued appropriateness.

- Access to systems and applications must be reviewed periodically to ensure continued appropriateness, with frequency based on risk and system criticality
- Access to systems containing personal or sensitive information must be subject to additional scrutiny
- Privileged access must be reviewed more frequently or with additional oversight
- Access that is no longer required must be removed promptly
- Inactive or orphaned accounts must be identified and disabled where appropriate

Third-Party Access

Access provided to third parties must be controlled and limited.

- Third-party access must be approved, documented, and limited to required systems and data
- Access should be time-bound and reviewed periodically

- Third-party access to systems containing personal information must be limited, controlled, and aligned with contractual agreements
- Third-party access must be removed when no longer required

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 access control practices to ensure that access to systems and data remains appropriate and aligned with business requirements.

- User access rights should be reviewed periodically to ensure they remain appropriate, with frequency based on risk and system criticality
- Privileged access should be subject to additional oversight and review
- Account lifecycle activities (e.g. provisioning, changes, and revocation) should be monitored to ensure they are performed correctly and in a timely manner

- Authentication events and access to sensitive or personal data should be monitored through available logging and reporting mechanisms where feasible

Where non-compliance or risks are identified:

- Access rights must be updated or removed where they are no longer required
- Accounts that are inactive, orphaned, or no longer valid must be disabled or removed
- Access to systems or data 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)