Access Management Procedure

Governance & Ownership

Owner: Key Account Manager (Head of Head of Operations)
Approved By: Company Director

Version & Review Control

Version	Effective Date	Review Frequency	Next Review Date
1.2	March 2026	Annually	March 2027

Document Classification

Classification: Internal Use Only

Confidentiality Statement

This standard 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 Head of Operations or Company Director.

Purpose

This procedure defines how access to systems, applications, and data is requested, approved, provisioned, reviewed, and removed. It ensures that access is controlled, auditable, and aligned with business needs and the principle of least privilege.

Scope

This procedure applies to:

- All employees, contractors, and third parties
- All systems, applications, cloud platforms, and SaaS services
- All access to personal information, business data, and administrative functions

Roles & Responsibilities

Role	Responsibility
Director	Provides oversight, approves privileged access, and escalates high-risk exceptions. (currently Google Workspace Admin; to be delegated)
Head of Operations	Coordinates access requests, maintains access records, and ensures compliance with this procedure.
Developers / Technical Resources	Provision accounts in Google Workspace and other systems; manage technical access; support revocation. (with Director and Head of Head of Operations assistance where required)
Third-Party Providers	Access only what is authorised; comply with contractual and security requirements.

Given the small team size, access management responsibilities may be performed directly by the Head of Operations or Technical Lead, with Director oversight for privileged access

Access Principles

- Access must be based on job role (RBAC).
- Access must follow the principle of least privilege.
- Access must be approved before being granted.
- Access must be reviewed periodically.
- Access must be removed when no longer required.

Joiners (Access Provisioning)

Request

- Access requests are raised by the hiring team or Head of Operations.
- Requests are submitted via email to Head of Operations and, where needed, the technical team.

Approval

- Head of Operations approves standard access.
- Company Director approves privileged or administrative access.
- Approval is based on role, business need, and system sensitivity.

Provisioning

- Accounts are created in **Google Workspace**, the authoritative identity provider.
- Additional systems (hosting, apps, third-party tools) are provisioned by the technical team.
- Access is recorded by the Head of Operations, as part of the access provisioning workflow.
- MFA is supported through Google Workspace and is required by policy. Enforcement settings are managed in the Google Admin Console.

Movers (Access Changes)

- Role changes are communicated to Head of Operations.
- Head of Operations reviews existing access and identifies required changes.
- Google Workspace access is updated by the Technical Lead or Head of Operations, depending on delegated admin rights. The technical team will make updates to other systems.
- Any increase in privilege requires Director approval.
- Access is recorded by the Head of Operations, as part of the access change workflow.

Leavers (Access Removal)

Notification

- The Head of Operations must be notified of termination or contract end.
- The Head of Operations informs the Technical Lead immediately so that Google Workspace and application access can be removed.

Timeframe

- Access must be removed **immediately** or within **24 hours** of departure.

Deactivation

- Google Workspace account is suspended or deleted.
- Access to email, Drive, and integrated apps is revoked instantly.
- Access to hosting platforms, admin consoles, and third-party systems is removed.
- Shared credentials or API keys are rotated if applicable.

Recordkeeping

- Offboarding actions are logged by the Head of Operations.

Access Reviews (Recertification)

Frequency

- Access reviews are performed **quarterly**.

Scope

- All user accounts
- Privileged/admin accounts
- Third-party access
- Service accounts

Process

- Head of Operations exports user lists from Google Workspace and other systems.
- Head of Operations must review whether access remains appropriate.
- Head of Operations removes or adjusts access where no longer required.
- Exceptions are escalated to the Director.

Evidence

- Review results are documented and stored securely for audit.

Privileged Access

- Admin access is limited to authorised individuals approved by the Director.
- Separate admin accounts are used where supported.
- Privileged actions are logged through Google Workspace and system logs.
- Privileged access is reviewed quarterly.

Third-Party Access

- Third-party access must be approved by Head of Operations and the Director.
- Access is time-bound and limited to required systems.
- Access is reviewed during contract renewal or quarterly.
- Access is revoked immediately when no longer required.

Authentication Controls

- MFA is supported and required by policy. Enforcement is enabled in Google Workspace and will apply to all users from 01 April.
- Google Workspace enforces strong password requirements for all internal users.
- Password managers are recommended.
- Accounts are protected by Google Workspace security controls (lockout, phishing protection, etc.).

Escalation

Escalate to the Company Director if:

- Unauthorised access is suspected
- Access removal is delayed
- Privileged access conflicts arise
- A system owner refuses or delays access revocation

Documentation & Recordkeeping

- Access requests, approvals, changes, and removals must be documented.
- Access review evidence must be retained for audit.
- Records are stored securely by Head of Operations.

Related Documents

- Access Control & Identity Management Policy
- Incident Response Procedure
- Vendor / Third-Party Policy

Document Control & Version History

Version	Date	Owner	Approved By	Next Review Date
1.0	March 2026	Key Account Manager (Head of Operations)	Company Director	March 2027

Version History

Version	Date	Description of Changes	Author	Approver
1.0	March 2026	Initial version	Key Account Manager (Head of Operations)	Company Director
1.2	March 2026	Google Workspace confirmed as central Identity Provider	Key Account Manager (Head of Operations)	Company Director