Vendor & Third-Party Risk Management Policy

Policy for Managing Risks Associated with Vendors and Third-Party Operators

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 Vendor & Third-Party Risk Management Policy establishes Genesys Creative Systems' requirements for identifying, assessing, and managing risks associated with external vendors, service providers, and operators who access or process Genesys Creative Systems' data, systems, or services. The policy ensures that third-party engagements align with Genesys Creative Systems' security, privacy, and regulatory obligations.

Purpose & Scope

The purpose of this policy is to minimise risks arising from third-party relationships and to enforce consistent vendor due diligence and monitoring.

Scope includes:

- All third-party service providers, operators, contractors, or vendors who access Genesys Creative Systems data or systems.
- Cloud providers, SaaS applications, and hosting partners.
- Outsourced business process or IT service providers.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA – Section 21: operators (third parties) must have written agreements ensuring compliance.
- Companies Act (2008) – director accountability for third-party risk.
- King IV – governance of outsourcing, supplier oversight, and risk.

Best Practice References:

- ISO/IEC 27036 – Information Security in Supplier Relationships.
- ISO/IEC 27001 Annex A.15 – supplier relationships.
- NIST Cybersecurity Framework v2.0 – ID.SC (Supply Chain Risk Management).
- NIS2 Directive – supply-chain transparency and accountability.

Policy Requirements

Vendor Risk Management

Genesys Creative Systems must manage risks associated with vendors and third-party service providers to ensure the protection of systems, data, and business operations.

- Where feasible, vendors must undergo a risk assessment prior to engagement
- Contracts must include appropriate security, privacy, and regulatory compliance requirements
- POPIA-compliant Operator Agreements must be in place for all third parties processing personal information
- Vendors must provide reasonable evidence of security controls where applicable
- Access to systems and data must be restricted based on the principle of least privilege
- Critical or high-risk vendors may be subject to periodic performance and security reviews
- Exit requirements must be defined, including the secure return or deletion of data

Third-Party Processing of Personal Information (Operators)

Where vendors process personal information on behalf of Genesys Creative Systems:

- A written agreement must be in place defining data protection responsibilities (Operator Agreement)
- Vendors must only process personal information for authorised purposes
- Vendors must implement appropriate technical and organisational measures to protect personal information
- Vendors must notify Genesys Creative Systems without undue delay in the event of a data breach
- Vendors must not transfer or disclose personal information without authorisation

Vendor Onboarding & Due Diligence

Prior to engagement, appropriate due diligence must be performed based on the level of risk, including:

- Completion of a vendor due diligence questionnaire covering security, privacy, compliance, and operational considerations
- High-risk vendors may be required to provide additional assurance (e.g. security attestations or certifications)
- The level of due diligence should be proportionate to the risk associated with the vendor

- Provision of relevant security documentation or attestations for high-risk vendors, where available

Ongoing Monitoring & Oversight

Vendors must be subject to ongoing oversight to ensure continued compliance with security and contractual obligations:

- Vendors should be reviewed periodically, with frequency based on risk (e.g. annually for critical vendors)
- Security incidents involving vendors must be reported and managed in accordance with agreed timelines
- Non-compliance must be addressed through remediation plans, and may result in contract review or termination
- Service agreements may include defined security and incident response expectations

Vendor Exit & Offboarding

Upon termination of a vendor relationship, appropriate controls must be applied to protect Genesys Creative Systems' data and assets:

- All data processed or stored on behalf of Genesys Creative Systems remains its property
- Vendors must return all data in a secure and usable format upon request or contract termination
- Vendors must securely delete all data from systems, backups, and devices following confirmation of successful transfer
- Where feasible, vendors should provide written confirmation of secure data deletion
- Access to systems must be revoked promptly, including accounts, credentials, and API access
- Any company-owned assets, documentation, or intellectual property must be returned prior to contract closure
- Vendors must support transition and handover activities where required
- Confidentiality and data protection obligations must remain in effect after contract termination

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

- Vendor risk management will be reviewed quarterly by the Head of Operations.
- Critical vendors will undergo annual reassessment.
- Non-compliance may lead to contract suspension or termination.

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)