Logging, Monitoring & Audit Policy

Policy for Security Logging, Continuous Monitoring, and Audit Readiness

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 Logging, Monitoring & Audit Policy defines Genesys Creative Systems' requirements for logging security-relevant events, monitoring systems for anomalies, and maintaining audit trails to support compliance and forensic investigations. The policy ensures the company can detect, respond to, and recover from security incidents effectively.

Purpose & Scope

The purpose of this policy is to establish consistent logging and monitoring practices that ensure visibility into Genesys Creative Systems' systems, applications, and networks.

Scope includes:

- All production systems, applications, and infrastructure components.
- All cloud platforms and SaaS solutions where Genesys Creative Systems data is stored or processed.
- Employee, contractor, and third-party operator activity where access to company data or systems is involved.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA – Section 19: enforce security safeguards to detect unauthorised access.
- Companies Act (2008) – director accountability.
- King IV – principle of oversight, accountability, and IT governance.

Best Practice References:

- ISO/IEC 27001 Annex A.12 & A.18 – logging and monitoring, evidence collection.
- ISO/IEC 27002 – control objectives for event logging and protection.
- NIST Cybersecurity Framework v2.0 – DE.CM (Detection & Monitoring), RS.AN (Analysis).
- NIS2 Directive – supply-chain monitoring and transparency.

Policy Requirements

Logging Requirements

Genesys Creative Systems must ensure that appropriate logging is enabled on systems and services to support security monitoring, incident investigation, and operational oversight.

- Security-relevant events should be logged where supported, including authentication, access, changes, and privileged activities
- Logs should include sufficient detail to support investigation (e.g. timestamp, user or account identifier, and event description)
- Systems should use consistent and reliable time sources where feasible
- Logs must be protected against unauthorised access, modification, or deletion
- Access to logs must be restricted to authorised individuals only
- Logs should be retained for a defined period (e.g. at least 90 days), or longer where required by contractual or regulatory obligations

Monitoring & Alerting

Systems and services must be monitored to detect potential security incidents or unauthorised activity.

- Available platform-native monitoring and alerting capabilities should be used where feasible (e.g. cloud platform logs, application logs)
- Alerts should be configured for significant or suspicious events where supported
- Monitoring activities should be proportionate to the level of risk and criticality of the system
- Third-party service providers should provide appropriate visibility or reporting where they host or process Genesys Creative Systems data

Audit & Evidence Management

Logging and monitoring information must be sufficient to support audit, investigation, and compliance requirements.

- Logs and audit trails should be maintained to support investigation of incidents and demonstrate compliance where required
- Relevant evidence should be preserved in a manner that maintains its integrity where feasible
- Access to logs and audit information must be controlled and limited to authorised individuals
- Where required by clients or regulatory obligations, additional evidence or reporting may be provided

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 logging and alerting activities to ensure that security-relevant events are identified and acted upon in a timely manner.

- Logs should be reviewed periodically, where feasible, to identify unusual or suspicious activity
- Alerts generated by systems or services should be investigated and addressed appropriately
- Monitoring practices should be aligned to the level of risk and criticality of systems and services
- Logging and monitoring capabilities should be reviewed periodically to ensure they remain effective and relevant

Where gaps or issues are identified:

- Logging or monitoring configurations must be updated to improve visibility and coverage
- Identified incidents or suspicious activities must be investigated and managed in accordance with incident response processes
- Access to systems or services may be restricted where necessary to mitigate identified risks
- 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)