Secure Software Development & Change Management Policy

Policy for Secure Development, Testing, and Change Management

Governance & Ownership

- Policy Owner: Head of Operations
- Executive Sponsor: Company Director
- Reviewer: Operations Manager
- 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 Secure Software Development & Change Management Policy establishes Genesys Creative Systems' requirements for secure coding, application development, system changes, and software release management. It ensures that all changes to Genesys Creative Systems' IT environment are authorised, tested, documented, and compliant with security and regulatory requirements.

Purpose & Scope

The purpose of this policy is to:

- Ensure software developed or deployed by Genesys Creative Systems meets security and compliance requirements.
- Prevent unauthorised, insecure, or disruptive changes to systems.
- Ensure accountability through proper approval, documentation, and rollback procedures.

Scope includes:

- All internally developed applications and websites
- All configuration changes to Genesys Creative Systems-managed systems, databases, and cloud platforms.
- Software acquired from vendors that requires integration or customisation.
- Developers, contractors, and third-party service providers working on Genesys Creative Systems projects.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA – Section 19: requires safeguards to protect personal information processed through software systems.
- Companies Act (2008) – director accountability for IT governance.
- King IV – governance of technology and IT-related decision-making.

Best Practice References:

- ISO/IEC 27001 Annex A.12 & A.14 – secure development, system acquisition, and change management.
- ISO/IEC 27034 – Application Security.
- NIST Cybersecurity Framework v2.0 – PR.IP (Protective Technology), DE.CM (Detection).
- NIST SP 800-218 (SSDF) – Secure Software Development Framework.
- OWASP ASVS & Top 10 – application security best practices.
- NIS2 Directive – secure-by-design principle.

Policy Requirements

Secure Software Development

Genesys Creative Systems must ensure that software is developed and maintained in a secure manner to reduce the risk of vulnerabilities and protect data and systems.

- Secure coding practices must be followed, including mitigation of common vulnerabilities (e.g. OWASP Top 10)
- Code must be reviewed prior to deployment into production environments
- Security testing must be performed on critical systems where feasible, including static and/or dynamic analysis
- Sensitive information (e.g. credentials, encryption keys) must not be hardcoded in source code
- Third-party libraries and dependencies must be reviewed for known vulnerabilities and updated regularly
- Developers must be made aware of secure development practices and receive periodic training where feasible

Change Management

All changes to systems, applications, and infrastructure must be controlled to minimise risk and ensure system stability.

- Changes must be requested, documented, and approved prior to implementation
- Changes must include consideration of risks and potential impacts
- Where feasible, changes must be tested prior to implementation (e.g. in a staging or test environment)
- Emergency changes must be documented, justified, and reviewed after implementation
- Changes must be traceable to an identified individual
- Records of changes and approvals must be retained for audit and operational purposes

Release & Deployment Management

Deployments to production environments must be managed in a controlled and auditable manner.

- Production deployments must follow an approved and documented process
- Where feasible, automated deployment mechanisms (e.g. CI/CD pipelines) should include appropriate checks for security and quality
- New releases should be tested to minimise disruption to services
- Version control systems must be used to manage and track source code changes
- Deployment activities must be logged and auditable

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 compliance with secure development and change management requirements to ensure that systems are developed, modified, and deployed in a controlled and secure manner.

- Development and change activities must be traceable through version control systems, change records, and deployment logs
- Code reviews, testing activities, and approvals should be evidenced where applicable
- Changes to production systems must be monitored to ensure they follow the defined change management process
- Where feasible, logging and monitoring mechanisms should be used to detect unauthorised or unapproved changes

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)


enesys
CREATIVE SYSTEMS