Security Awareness & Training Policy

Policy Framework for Staff Security Awareness and Training Initiatives

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 Security Awareness & Training Policy establishes Genesys Creative Systems' requirements for educating employees, contractors, and relevant third-party personnel on their security and privacy responsibilities. The programme ensures ongoing competence to protect personal information and company assets, enable secure remote work, and reduce the likelihood and impact of security incidents.

Purpose & Scope

The purpose of this policy is to define the scope, content, frequency, and governance of Genesys Creative Systems' security awareness and training programme.

Scope includes:

- All employees and long-term contractors ("staff").
- Short-term contractors and third-party operator personnel who access Genesys Creative Systems' technology systems or data.
- All systems and platforms used to process personal information or confidential business data.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- Protection of Personal Information Act (POPIA) – Section 19 (security safeguards), Section 22 (breach notification).
- Companies Act (2008) – accountability of directors.
- King IV – governance of IT and information.
- Labour Law – employee obligations and disciplinary processes.

Best Practice References:

- ISO/IEC 27001 & 27002 (A.6, A.7 awareness; A.12 operations; A.16 incident management).
- NIST Cybersecurity Framework v2 (ID, PR.AT – Awareness & Training; RS – Response).
- NIS2 Directive & GDPR (as international best practice for accountability and breach handling).

Policy Requirements

Security Awareness Programme

Genesys Creative Systems must maintain a security awareness and training programme to ensure that employees and contractors understand their responsibilities in protecting information and systems.

The programme must be proportionate to the size and nature of the organisation and focus on practical, real-world risks.

Onboarding & Induction Training

All new employees and contractors must complete security awareness training as part of onboarding, which must include:

- Overview of the Information Security Policy and Acceptable Use requirements
- Basic privacy and data protection principles (including POPIA)
- Identification of phishing and social engineering attacks
- Incident reporting processes and escalation channels

Where relevant, role-specific guidance should be provided based on job function.

Ongoing Awareness & Refresher Training

Security awareness must be reinforced on an ongoing basis through:

- Annual refresher training covering updates to policies, threats, and procedures
- Periodic awareness communications (e.g. emails, team briefings, reminders)
- Reinforcement of key principles such as least privilege and secure data handling

Training content should be updated to reflect emerging threats and organisational changes.

Phishing Awareness & Testing

To assess and improve user awareness:

- Periodic phishing simulations may be conducted
- Results should be used to identify areas for improvement and guide future training

Role-Based Training

Where applicable, role-specific security training must be provided based on responsibilities, including:

- Developers: Secure coding practices, common vulnerabilities (e.g. OWASP Top 10), and secure handling of secrets
- Operations / Cloud: Secure configuration, logging and monitoring, backup and recovery practices
- Customer-facing roles**:** Secure handling of personal information and verification procedures
- Vendor / third-party management: Due diligence and risk awareness
- Management / Executives: Accountability, incident response decision-making, and regulatory considerations

Training Content Requirements

Security awareness training must, at a minimum, cover:

- Data protection and privacy principles (including POPIA requirements)
- Data classification and secure handling practices
- Access control, authentication (including MFA), and password security
- Email and communication security, including phishing awareness
- Identification and reporting of security incidents
- Secure use of systems and devices

Responsibility for Participation

All employees and contractors are responsible for:

- Participating in required training
- Applying security practices in their daily activities
- Reporting suspected security incidents promptly

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 participation in security awareness activities and take appropriate action to ensure that employees and contractors understand and comply with security requirements.

- Participation in onboarding and periodic training should be tracked where feasible
- Awareness activities (e.g. communications, briefings, reminders) should be conducted periodically to reinforce key security principles
- Phishing simulations or similar exercises may be used to assess awareness and identify areas for improvement
- Feedback from incidents, near misses, or observed behaviour should be used to improve training content and focus areas

Where non-compliance is identified:

- Individuals may be required to complete additional training or awareness activities

- Repeated or significant non-compliance may be escalated to management for further action

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)