Endpoint & Device Security Policy

Policy for Securing Laptops, Desktops, and Mobile Devices

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 Endpoint and Device Security Policy defines Genesys Creative Systems' requirements for securing devices used to access, store, or process company information.

The policy ensures that endpoints, including laptops, mobile devices, and other user-accessible systems, are protected against unauthorised access, loss, or compromise.

Purpose & Scope

The purpose of this policy is to protect Genesys Creative Systems' information assets by establishing minimum security requirements for all devices used to access company systems and data.

Scope includes:

- All devices used by employees, contractors, and third parties to access or process Genesys Creative Systems information
- Company-issued devices, including laptops and any other managed endpoints
- Personally owned devices (BYOD) used to access company systems or data
- Mobile devices used for business purposes (e.g. email, applications, authentication)
- Removable media (e.g. USB drives, external storage devices)
- Devices used to access cloud services, applications, or remote environments

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- Protection of Personal Information Act (POPIA) – Section 19 (security safeguards).
- Companies Act (2008) – director accountability for governance failures.
- King IV – principle of responsible technology and IT governance.

Best Practice References:

- ISO/IEC 27001 & 27002 (Annex A.8, A.12 – asset and endpoint security).
- NIST Cybersecurity Framework v2.0 – PR.AC (Access Control), PR.DS (Data Security), DE.CM (Detection).
- NIS2 Directive (as global best practice).

Policy Requirements

Device Security Controls

All devices used to access or process Genesys Creative Systems information must meet minimum security requirements.

- Devices must be protected using full disk encryption where supported (e.g. BitLocker, FileVault)
- Anti-malware or endpoint protection software must be installed, enabled, and kept up to date
- Operating systems and applications must be kept up to date with security patches within a reasonable timeframe (e.g. critical updates prioritised)
- Local device firewalls must be enabled where supported
- Devices must be configured with strong authentication mechanisms (e.g. password or PIN with MFA for system access where applicable)
- Devices must automatically lock after a period of inactivity

Secure Use of Devices

Devices must be used in a manner that protects company information from unauthorised access or exposure.

- Devices must not be shared between users unless appropriately controlled
- Devices must not be left unattended in unsecured locations
- Public or untrusted networks should be used with caution, and access to sensitive systems should be protected (e.g. via secure connections)
- Only approved or trusted applications and software should be installed on devices used for business purposes

Loss, Theft, and Incident Reporting

Loss or compromise of devices must be reported and managed promptly.

- Lost or stolen devices must be reported as soon as possible
- Where feasible, remote lock or wipe capabilities should be used to protect data
- Appropriate actions must be taken to prevent unauthorised access to company systems (e.g. account suspension or credential reset)

Removable Media

The use of removable media must be controlled to prevent data leakage or malware introduction.

- Removable media should only be used where necessary

- Sensitive data stored on removable media must be encrypted
- Unknown or untrusted removable media must not be used

Bring Your Own Device (BYOD)

Personally owned devices used for business purposes must meet minimum security requirements.

- BYOD devices must comply with the same baseline security controls as company devices where feasible
- Access to company systems may be restricted if minimum security requirements are not met
- Company information must not be stored locally on personal devices unless necessary and appropriately protected

Mobile Device Security

Mobile devices used for business purposes must be secured to reduce the risk of data exposure.

- Mobile devices must be protected with a secure lock mechanism (e.g. PIN, password, or biometric authentication)
- Devices that are jailbroken or rooted must not be used to access company systems
- Where feasible, device-level security features (e.g. encryption, remote lock/wipe) should be enabled
- Access to company data on mobile devices should be limited to approved applications where possible

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 endpoint and device security requirements to ensure that devices used for business purposes are secure and appropriately managed.

- Device security practices should be reviewed periodically to ensure that minimum security controls (e.g. encryption, updates, and protection software) are in place where feasible
- Access to company systems may be reviewed to ensure that only compliant devices are used where possible
- User behaviour and device usage should be monitored through observation, incident reporting, and security awareness activities
- Loss, theft, or compromise of devices must be tracked and managed in accordance with incident response processes

Where non-compliance or risks are identified:

- Access to systems or data may be restricted or revoked until minimum security requirements are met
- Corrective actions (e.g. applying updates, enabling security controls) must be implemented where feasible
- Additional awareness or guidance may be provided to users where required
- Significant or repeated 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)