Business Continuity & Disaster Recovery Policy

Policy for Ensuring Operational Resilience and Disaster Recovery

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 Business Continuity and Disaster Recovery (BCDR) Policy defines Genesys Creative Systems' approach to maintaining the continuity of critical business operations and restoring systems and services following a disruption.

The policy ensures that Genesys Creative Systems can respond to and recover from incidents in a controlled and timely manner, reducing the impact on service delivery and information assets.

Purpose & Scope

The purpose of this policy is to:

- Minimise the impact of disruptions on business operations and service delivery
- Ensure that critical systems and services can be restored within a reasonable timeframe
- Support the protection and recovery of company and client data

Scope includes:

- All business functions and services considered critical to Genesys Creative Systems' operations
- All systems, applications, and cloud platforms supporting business services
- All employees, contractors, and third-party service providers involved in service delivery or recovery activities.

Regulatory Drivers & References

Regulatory Drivers (South Africa):

- POPIA – Section 19: requires safeguards to protect personal information during disruptions.
- Companies Act (2008) – director accountability for governance and risk management.
- King IV – principle of resilience, sustainability, and risk management.

Best Practice References:

- ISO/IEC 22301 – Business Continuity Management Systems.
- ISO/IEC 27001 Annex A.17 – Information Security Continuity.
- NIST Cybersecurity Framework v2.0 – RS (Response), RC (Recovery).
- NIS2 Directive – best practice for resilience and operational continuity.

Policy Requirements

Business Continuity Planning

Genesys Creative Systems must identify and prioritise critical business services and ensure that appropriate measures are in place to maintain or restore operations during a disruption.

- Critical business processes and services must be identified and documented
- Key dependencies (e.g. systems, cloud services, third-party providers) must be understood
- Recovery objectives, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), should be defined where appropriate
- Continuity strategies should consider remote working, alternative processes, and use of cloud-based services
- Roles and responsibilities for continuity and recovery activities must be defined

Backup & Data Recovery

Data must be protected through appropriate backup and recovery mechanisms to support business continuity.

- Critical data must be backed up regularly using secure and reliable methods
- Backups must be protected (e.g. encrypted where supported) and stored in a manner that supports recovery
- Backup restoration should be tested periodically to ensure data can be recovered successfully
- Backup processes should align with defined recovery objectives where applicable

Disaster Recovery (IT Systems)

Systems and services must be capable of being restored following a disruption.

- Critical systems and applications must have defined recovery approaches
- Cloud-based services should be configured to provide resilience and availability where supported (e.g. redundancy, failover capabilities)
- Recovery procedures should be documented at a level appropriate to the organisation
- Disaster recovery considerations should include scenarios such as system failure, data loss, cyber incidents, and service provider outages

Third-Party and Cloud Resilience

Where services are dependent on third-party providers:

- Providers must demonstrate appropriate resilience and continuity capabilities
- Dependencies on third-party services must be understood and considered in continuity planning
- Alternative arrangements or contingency approaches should be considered where feasible

Testing & Awareness

Business continuity and recovery arrangements must be validated and understood.

- Continuity and recovery processes should be tested periodically, where feasible
- Lessons learned from testing or incidents should be used to improve resilience
- Employees and relevant parties should be aware of their roles during a disruption

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 the effectiveness of its business continuity and disaster recovery arrangements to ensure that critical services and systems can be restored in a timely manner.

- Business continuity and recovery arrangements should be reviewed periodically to ensure they remain appropriate and aligned to business needs
- Backup processes should be monitored to ensure they are functioning as expected and supporting recovery requirements
- Backup restoration and recovery activities should be tested periodically, where feasible, to confirm that data and systems can be recovered
- Dependencies on cloud and third-party providers should be reviewed to ensure continued availability and resilience

Where gaps or weaknesses are identified:

- Corrective actions must be implemented to improve continuity and recovery capabilities
- Recovery processes, configurations, or documentation should be updated as required
- Significant issues may be escalated to management for oversight and decision-making

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)