Resilience and Incident Response Plan

Governance & Ownership

Owner: Key Account Manager (Head of Operations)
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 standard 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.

Purpose

This document defines Genesys' practical and proportionate approach to incident response, business continuity, disaster recovery, and backup and restore. It exists to enable timely response, clear decision making, restoration of critical services, and continued delivery of essential business activities.

Scope

Applies to employees, contractors, management, systems, cloud and hosted infrastructure, business and client data, and third parties that materially support operations. The plan covers four linked disciplines: incident response, business continuity, disaster recovery, and backup and restore.

Principles

- Controls are proportionate to size and risk.
- Material incidents are handled in a structured and timely way.
- Critical systems and data must be recoverable within practical timeframes.
- Roles and escalation paths must be clear.
- Lessons learned drive improvement.

Roles and Responsibilities

Director
Overall accountability for resilience, approval of major decisions, and client or regulator communication where required.

Information Officer
Overall responsibility for data protection and regulatory liaison; approves external notifications.

Deputy Information Officer
Supports the Information Officer, manages internal communications, and coordinates follow up actions.

Operational Lead Incident Coordinator
Coordinates response actions, records decisions, engages internal and external parties, and tracks status through containment, recovery, and closure.

Technical Support Personnel Service Providers
Investigate technical issues, implement containment and recovery actions, restore systems, and validate integrity.

All Staff & Contractors
Report suspected incidents promptly, follow continuity instructions, protect information assets, and cooperate with response and recovery activities.

Incident Response

What counts as an incident

Examples include unauthorised access, malware or ransomware, service disruption, data loss or corruption, and material vendor or infrastructure failure.

Reporting

Report incidents immediately to the Incident Coordinator, Information Officer, or Deputy Information Officer by phone, WhatsApp, or email. If unavailable, notify the developer on call.

Response stages

- **Identify and report** — confirm the event, capture logs and evidence, and classify severity.
- **Assess and classify** — determine affected assets and likely business impact.
- **Contain** — take reasonable actions to limit spread or exposure.
- **Eradicate and remediate** — remove threats, patch, reset credentials, or block malicious actors.
- **Recover** — restore services from clean sources or backups and validate functionality.
- **Review** — document lessons learned and update controls and this plan.

Escalation and notification

Management must be informed of material incidents. Where contract, law, or client commitments require notification, the organisation will assess obligations and respond within applicable timeframes. **Where client data or services are affected, Genesys will notify clients without undue delay and in accordance with contractual requirements.** External specialist support may be engaged where needed.

Business Continuity & Disaster Recovery

Continuity priorities

1. Maintain internal and client communication.
2. Preserve access to critical platforms and data.
3. Use manual or alternative processes where systems are unavailable.
4. Prioritise restoration of client-facing activities.

Continuity approach

Given the remote operating model, continuity may include alternate devices, remote working from unaffected locations, cloud collaboration platforms, prioritisation of essential tasks, and use of third-party provider support.

Disaster recovery objectives

- **Guideline RTO (time to restore services):** 4 – 8 hours
- **Guideline RPO (maximum tolerable data loss):** less than 24 hours for critical data.

Management will prioritise restoration based on service criticality, client impact, and data sensitivity.

Business Continuity & Service Restoration Objectives

Our Business Continuity and Resilience framework is aligned with the service levels defined in the client's SLA. The following Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) reflect our operational commitments for restoring service availability and data integrity across the three disruption tiers.

Notes:

- Each enterprise client is hosted on its own dedicated server, ensuring isolation and preventing multi tenant blast radius
- Hetzner typically provisions replacement bare metal servers within 20–40 minutes, enabling rapid initiation of restore procedures
- Cloudflare continues to serve static assets and provide DDoS/WAF protection during backend outages, reducing perceived downtime for end users

Tier 1 – Full Service Outage

Indicator: The service is completely unavailable; authorised users cannot access the platform.

Business Continuity Objectives

- **RTO:** < 8 hours
  We commit to restoring full platform availability by the next business day, consistent with the SLA's required resolution time.

- **RPO:** < 24 hours
  Data can be restored from daily backups and point-in-time recovery mechanisms.

Operational Notes

- Incident response begins same day.
- Priority is restoring platform access and ensuring no data loss beyond the defined RPO.
- This tier triggers the highest internal escalation level.

Tier 2 – Critical Disruption

Indicator: A critical function is unavailable, preventing same-day content creation or dispatch.

Business Continuity Objectives

- **RTO:** < 8 hours
  Critical functionality must be restored by the next business day (AUS), matching the SLA requirement.
- **RPO:** < 24 hours
  Data required for content creation and dispatch must be recoverable within the same RPO window as Tier 1.

Operational Notes

- Same-day response with engineering escalation.
- Restoration focuses on the specific critical subsystem rather than full platform recovery.
- Communication with the client follows the same cadence as Tier 1.

Tier 3 – Minor Disruption

Indicator: The service is operational, but a fault negatively impacts productivity.

Business Continuity Objectives

- **RTO:** < 48 hours
  Minor issues are resolved within two business days, consistent with the SLA's "next day +1" response expectation.
- **RPO:** Not typically applicable
  Minor disruptions generally do not involve data loss or rollback.

Operational Notes

- Prioritised after Tier 1 and Tier 2 incidents.
- Fixes may be deployed in the next scheduled maintenance window unless impact escalates.

Summary of RTO/RPO Commitments

SLA Tier	Description	RTO	RPO
Tier 1	Full outage	**< 8 hours**	**< 24 hours**
Tier 2	Critical disruption	**< 8 hours**	**< 24 hours**
Tier 3	Minor disruption	**< 48 hours**	Not typically applicable

---

Backup & Recovery

Recovery dependencies

Hosting and infrastructure services, system images and deployment artefacts, database and application backups, identity and access controls, and third-party communications.

Backup requirements

- Backups must cover data and configurations necessary for recovery of critical services.
- Backups must be encrypted in transit and at rest.
- Backup frequency must align to operational need; daily backups are standard.
- Retention: 30 days as a baseline unless contractual requirements dictate otherwise.
- Backup storage should avoid single points of failure and restrict access to authorised personnel only.

Restore expectations

Restore activities must be controlled, validated for integrity and usability, and confirmed free from known compromise before returning to service.

Testing and Maintenance

Records and evidence

Maintain incident logs, recovery actions, backup records, restore test outcomes, service provider communications, and post-incident improvement actions.

Testing

- Conduct at least one resilience test annually. Tests may be tabletop exercises, restore tests, or walkthroughs of recovery actions.
- Restore tests must be performed at least annually and results documented.

Review and improvement

- Review this plan annually and after material incidents or major changes.
- Update contact lists, escalation paths, and dependency information as required.
- Document lessons learned and assign owners for remediation actions.

Exceptions

Any material exception to this standard must be approved by management, documented with rationale, and reviewed within a defined timeframe.

Appendices

Appendix A Practical Response Reference

Scenario	Initial response	Typical recovery focus
Suspected account compromise	Disable or reset affected access, review recent activity, notify management if material	Restore secure access, validate logs, assess exposure
Hosting or infrastructure outage	Confirm provider status, assess business impact, invoke continuity workarounds	Provision replacement server, restore Docker volumes and MariaDB from Cloudflare R2, rebuild containers, validate application and data integrity
Data corruption or deletion	Stop further changes where practical, determine affected scope	Recover from backup, validate integrity and completeness
Malware or ransomware suspicion	Isolate affected device or system, engage technical support, preserve evidence	Eradicate threat, rebuild or restore safely, confirm clean state

Appendix B Contact List

- **Information Officer:** Matt Spicer — matt@genesys.co.za / +27 83 720 1311
- **Deputy Information Officer:** Fran Schroeder — fran@Genesys.co.za / +27 61 454 9462
- **Incident Coordinator:** Fran Schroeder — fran@Genesys.co.za / +27 61 454 9462
- **Developer on Call:** Dane Matthews dane@themodernweb.co / +27 82 069 7504

Document Control & Version History

Version	Date	Owner	Approved By	Next Review Date
1.0	March 2026	Key Account Manager (Head of Operations)	Company Director	March 2027

Version History

Version	Date	Description of Changes	Author	Approver
1.0	March 2026	Initial version	Key Account Manager (Head of Operations)	Company Director