Synthetic Users Business Continuity Plans (BCP)

Version: 1.1

Effective Date: 29th April 2025

Approved By: Kwame Ferreira, CEO

Owner: Kwame Ferreira, CEO (CEO)

---

1. Purpose and Scope

Purpose:

To ensure the continued operation of critical business functions and rapid service recovery in the event of a major disruption, minimizing impact to customers, partners, and employees.

Scope:

This plan applies to all Synthetic Users business units and covers:

- SaaS platform operations and hosting infrastructure
- Customer support and success functions
- IT and cybersecurity systems
- Finance, billing, and legal operations
- HR and employee management processes

---

2. Ownership and Maintenance

- **BCP Owner:** Kwame Ferreira, CEO (CEO)
- **Review Frequency:** Bi-annually or immediately following a significant incident or organizational change

- **Change Management:** Updates are logged in the BCP Change Register, reviewed by the BCMT, and approved by the CEO

3. Business Continuity Management Team (BCMT)

Role	Name	Responsibility
Leader	Kwame Ferreira (CEO)	Overall coordination, activation/deactivation authority
Technology & Infrastructure	Artur Ventura (CTO)	Cloud recovery, backups, system restoration
Finance & Legal	Zumbi Ferreira (CFO)	Financial continuity, legal compliance, insurance
HR & Communications	HR Director	Employee safety, internal comms, wellbeing
Client Support & Relations	Customer Success Manager	Customer communication, support continuity

4. Critical Business Functions and Priorities

Function	Description	Priority	RTO	RPO	MTD
SaaS Operations	Core product availability and hosting	1	2 hours	15 minutes	8 hours
IT Infrastructure & Security	Data protection, encryption, and access systems	1	2 hours	15 minutes	8 hours
Customer Support	Communication with clients and ticket	2	4 hours	1 hour	24 hours

	resolution				
Finance & Billing	Payment processing, payroll, and vendor management	3	12 hours	4 hours	48 hours
Human Resources	Staff communication and administration	4	24 hours	12 hours	72 hours

5. Risk Assessment and Impact Analysis

Risk Categories:

- Cloud or hosting platform outage
- Cybersecurity breach or ransomware attack
- Loss of key personnel
- Natural disasters or regional power failures
- Pandemic or large-scale health event
- Legal or regulatory disruption

Each risk is evaluated for **likelihood, impact, and recovery complexity**, and tracked in the **Risk Register**.

6. Recovery Strategies

Technology and Infrastructure

- Redundant infrastructure hosted across multiple AWS regions (EU and US)
- Automated daily backups (AES-256 encrypted) with 30-day retention
- Recovery Time Objective (RTO): 2 hours
- Recovery Point Objective (RPO): 15 minutes

- AWS disaster recovery features (multi-AZ replication and snapshots)

Customer Support Services

- Remote-ready support team with cloud ticketing and communication tools (email, chat, Slack)
- Backup email notification list for service updates during outages

Finance and Billing

- Cloud-based systems (e.g., Stripe, Xero) with data redundancy and offline access capability

Human Resources

- Remote work infrastructure for all employees
- Crisis communication channel (Slack + email)
- Employee assistance and wellbeing program

---

7. Incident Response and Plan Activation

7.1 Detection and Assessment

- BCMT monitors alerts and internal reports for operational disruption.
- Initial assessment determines severity, affected systems, and potential downtime.

7.2 Activation Criteria

- Triggered when any Priority 1 or 2 function is disrupted beyond its RTO.
- The BCMT Leader authorizes activation and coordinates communication.

7.3 Communication Plan

- **Internal:**

    - Notify all employees via Slack and email.
    - Daily updates to management during active recovery.
- **External:**
    - Client and partner notifications coordinated by the Customer Success Manager.
    - Public updates via website status page or direct communication if required.

7.4 Recovery Procedures

- Recovery follows predefined steps in the **Recovery Procedures Appendix** for each function.
- Each recovery phase is logged in the **Incident Log** (system recovery time, decisions, contacts).

7.5 Deactivation

- BCMT Leader deactivates the plan once normal operations are restored and verified.

---

8. Training and Testing

- **Annual BCP training** for all BCMT members and department heads.
- **Bi-annual simulations** covering scenarios such as cloud outage, ransomware, and data loss.
- Post-test reviews identify improvements and update the plan accordingly.

---

9. Change Management

- Updates triggered by infrastructure changes, new dependencies, or after incident reviews.
- All revisions recorded with date, author, and summary of changes.
- Archived versions retained for three years for audit purposes.

---

10. Post-Incident Review

- Conducted within 10 business days after plan deactivation.
- Includes lessons learned, timeline analysis, and system hardening recommendations.
- Results documented in the **Post-Incident Review Report** and incorporated into future BCP updates.

11. Client Exit, Portability, and Interoperability

11.1 Data Portability

- All customer data can be exported in standard, machine-readable formats (JSON, CSV) via the platform's export functionality or API.
- Upon client request or contract termination, a full data export is provided within 30 calendar days.

11.2 Interoperability

- Synthetic Users exposes a documented REST API for integration with client systems.
- SSO integration supports SAML 2.0 and OpenID Connect, ensuring compatibility with client identity providers.
- Data formats and schemas are documented and versioned.

11.3 Exit Plan

In the event of contract termination or service transition:

1. **Notification:** Client provides written notice per the terms of the Master Service Agreement.
2. **Data Export:** Full export of all client data is made available within 30 calendar days of termination.
3. **Data Deletion:** Following export confirmation, all client data is securely deleted per the Data Deletion and Retention Policy, including backups within 90 days.

4. **Access Revocation:** All client user accounts and API credentials are deactivated on the termination date.
5. **Transition Support:** Reasonable transition assistance is provided during the notice period to support migration to an alternative service.
6. **Confirmation:** Written confirmation of data deletion is provided to the client upon completion.