SWIFT COMPLY

Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: Brent Heeringa

Effective Date: 2021-04-23

Purpose

The purpose of this business continuity plan is to prepare SwiftComply in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Scope

All SwiftComply IT systems that are business critical. This policy applies to all employees of SwiftComply and to all relevant external parties, including but not limited to SwiftComply consultants and contractors.

The following scenarios are excluded from the BC/DR plan scope:

- Loss of availability for a production hosting service provider (i.e., GCP)

In the event of a loss of availability of a hosting service provider, the Head of Engineering will confer with the CEO, senior management and engineering staff to determine an appropriate response strategy.

1. Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the SwiftComply office, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Incident Response Plan.

SWIFT COMPLY

2. Alternate Work Facilities

If a SwiftComply office becomes unavailable due to a disaster, all staff shall work remotely from their homes or any safe location.

3. Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting SwiftComply facilities or operations.

Communications shall take place over any available regular channels including Google Meet, Slack, Email, Phone.

Key contacts shall be maintained on the on-call schedule and key contacts: https://docs.google.com/document/d/18kqKTPcHqgOPsx3pxxLLRmb81TqQSMgxZSkS3xs1E18/edit?usp=sharing

4. Roles and Responsibilities

Role	Responsibility
Head of Engineering	The Head of Engineering shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems.
Departmental Heads	Each department head shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions. Departmental heads shall communicate regularly with executive staff.
Managers	Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue working from alternative locations.
Head of Services	The Head of Services, in conjunction with the CEO and CFO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.
CEO	The CEO shall be responsible for internal communications to employees as well as any action needed to maintain physical health and safety of the workforce.

SWIFT COMPLY

5. Continuity of Critical Services

Procedures for maintaining continuity of critical services in a disaster can be found in Appendix A.

Strategy for maintaining continuity of services can be seen in the following table:

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on GCP availability commitments and SLAs
IT Operations	Rely on GCP availability commitments and SLAs. Development work is distributed to each dev's machine and not reliant on each other.
Email	Utilize Gmail and its distributed nature, rely on Google's standard service level agreements.
Support	All systems (Intercom) are vendor-hosted SaaS applications.
Finance, Legal and HR	All systems are vendor-hosted SaaS applications.
Sales and Marketing	All systems are vendor-hosted SaaS applications.

Plan Activation

This BC/DR shall be automatically activated in the event of the loss or unavailability of a region in GCP where SwiftComply's platform is hosted.

Version	Date	Description	Author	Approved by
1.0	2021-04-23	First Version	Brian Clapper	Mick O'Dwyer
2.0	2025-10-15	Update VP of Engineering to Head of Engineering and VP of Customer Success to Head of Services	Brent Heeringa	Mick O'Dwyer

SWIFT COMPLY

Appendix A – Business Continuity Procedures by Scenario

Business Continuity Scenarios

GCP Primary Availability Zone Offline

- Primary DB offline
- Half of production infrastructure offline (redundant)
- UAT services offline
- Staff unaffected (US)

Procedure:

1. Failover to replica DB
2. Notify Customer Base that services may be degraded
3. Normal operations continue

GCP Region Offline

- City 3 services offline

Procedures:

Temporary Outage

1. Notify Customer Base that services are down temporarily
2. When region is back up verify stability of all services and notify customers

Prolonged or Permanent Outage

1. Restore Production DB from daily backup
2. Restore other services from latest production code snapshot
3. Notify Customer Base a restore was done, inform them of the restore point and that work done after that time until now is likely lost

Intercom (support) Offline

- City 3 support down until intercom recovers

Procedures:

1. Alter the support@swiftcomply.com mailing group to add in individual customer success users as required, so that emails to the group still go to Intercom as well as individual email accounts
2. If possible provide an in-app notification that phone support is down temporarily