

Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: Alex Iglesias

Effective Date: July 7th, 2023

Purpose

The purpose of this business continuity plan is to prepare Finsweet in the event of 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 Finsweet IT systems that are business critical. This policy applies to all employees of Finsweet and to all relevant external parties, including but not limited to Finsweet consultants and contractors.

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

- Loss of availability for a production hosting service provider

In the event of a loss of availability of a hosting service provider, the CEO will confer with the Finsweet Security Officer (FSO) to determine an appropriate response strategy.

Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of Finsweet IT systems, 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](#).

Alternate Work Facilities

If the work facility of any employees, contractors, or any third-parties of Finsweet becomes unavailable due to a disaster, the individual shall work remotely from another location, which is safe.

Communications and Escalation

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

Communications shall take place over any available regular channels including email, Slack, Google Meet, or WhatsApp.

Key contacts shall be maintained on the on-call schedule and key contacts:

<https://www.notion.so/finsweet/deecf64b83dc41d8829a6e05a9ec4a3c?v=5b1f0ae850c4480aa39577f0721fa489&pvs=4>

Roles and Responsibilities

Role	Responsibility
CEO	The CEO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.
Finsweet Security Officer (FSO)	The FSO shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems. In addition, they shall be responsible for leading efforts to maintain continuity of Finsweet services to customers during a disaster.
Human Resources Officer (HRO)	The HRO shall be responsible for internal communications to employees as well as any action needed to maintain physical health and safety of the workforce.
Department 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 the FSO and HRO.

Continuity of Critical Services

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

Recovery Time Objectives (RTO) and Recovery Point Objects (RPO) can be found in Appendix B.

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

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on the provider's availability commitments and SLAs
IT Operations	Critical data is backed up and operations resumed from alternate locations.
Email	Utilize Gmail and its distributed nature, rely on Google's standard service level agreements.
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 the Finsweet services or a natural disaster (i.e., severe weather, regional power outage, earthquake) affecting the larger portion of the company.

Version	Date	Description	Author	Approved by
1.0	07-Jul-2023	Submit for approval	Alex Iglesias	Joe Krug
1.1	06-Jul-2024	Submit for approval	Rohan Ganachari	Alex Iglesias
1.2	25-Apr-2025	Submit for approval	Rohan Ganachari	Alex Iglesias

Appendix A - Business Continuity Procedures by Scenario

Business Continuity Scenarios

Cloud providers Down

- Cloud providers (Cloudflare, Google Cloud, Vercel, Webflow) affected
- CRM, Slack, Notion, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT unaffected
- Remote Staff unaffected

Procedure:

1. Notify all stakeholders
2. Subscribe to updates on the affected cloud provider's status page and proactive monitoring

SaaS Tools Down

- Cloud providers unaffected
- CRM, Slack, Notion, Video Conferencing/Screen Share, or Corp Email Affected
- SUPPORT partially affected (no new cases, manual triage required)
- Remote Staff unaffected

Procedures:

Slack Down

1. Notify Customer Base to use Email
2. Support Staff use Mobile Phones as needed

Email Down (Gmail/Corp Email)

1. Support Staff manually manage 'case' related communications
2. Support Staff use alternate email accounts as needed (Hotmail)

Notion Down

1. Subscribe to updates on <https://status.notion.so/> and proactive monitoring
2. Notify all stakeholders
3. Support Staff use alternate tools as needed

CRM Down

1. Notify Customer Base that CRM is down
2. Activate 'Spreadsheet' Case Tracking (Airtable)

Video Conferencing/ScreenShare Down (Google Meet)

1. Support Staff utilize alternate service as needed

Disaster Event at remote-worker location

- Cloud providers unaffected
- CRM, Slack, Notion, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT offline
- Remote Staff unaffected (variable impact)

Procedure:

1. Alert stakeholders of impaired functions & potential delays
2. Notify team and Customer Base
3. Reassign tasks & responsibilities

Appendix B - RTOs/RPOs

Rank	Asset	Affected Assets	Business Impact	Users	Owners	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Comments / Gaps
1	Google Datacenters	Site	Core services	All	Engineering	24 hours	24 hours	

1	Cloudflare	Network	Core services	All	Engineering	24 hours	-	
2	Google Cloud	Network	Core services	SaaS	Engineering	24 hours	24 hours	
2	Github	Network	Core services	All	Engineering	24 hours	24 hours	
3	Home Office ISP Networks	Network	Core services	All	N/A	48 hours	-	
3	Notion	Network	Core services	Agency	Agency	48 hours	-	
4	Vercel	Network	Core services	SaaS	Engineering	24 hours	-	
4	Personal Mobile Device	Hardware	Inability to access services with 2FA	All	Self	48 hours	-	