Business Continuity and Disaster Recovery Plan

Business Continuity and Disaster Recovery (BC/DR) Plan

Policy Owner: Trevor DeVore

Effective Date: Mar 24, 2026

Purpose

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

In the event of a loss of availability of a hosting service provider, the CTO will determine an appropriate response strategy.

General requirements

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the ScreenSteps, Inc. 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.

Communications and escalation

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

Communications shall take place over approved channels such as Slack, email.

Key communication contacts are maintained in this list: Slack

Roles and responsibilities

Role	Responsibility
CTO	The CTO shall lead BC/DR efforts to mitigate losses and restore customer facing web applications. The CTO, in conjunction with the Head of Customer Support, shall be responsible for leading efforts to maintain continuity of ScreenSteps, Inc. services to customers during a disaster.
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 and the IT Manager.
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 Customer Support	The Head of Customer Support, in conjunction with 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.
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.

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 AWS availability commitments and SLAs
IT Operations	Critical data is backed up to 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 ScreenSteps, Inc. web application affecting the AWS us-east region.

Version history

Version	Date	Description	Author	Approver
4.0	Mar 24, 2026	Version 4.0	Trevor DeVore	Trevor DeVore
3.0	Jan 29, 2025	Version 3.0	Danielle Steed	Jeremy Brown
2.0	Sep 11, 2023	Version 2.0	Trevor DeVore	Jeremy Brown
1.0	Sep 11, 2022	Version 1.0	Trevor DeVore	Jeremy Brown

Appendix A - Business continuity procedures by scenario

Business Continuity Scenarios

Primary Production Region Offline

- CRM, Telephony, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT possibly unaffected
- Remote Staff unaffected (US)

Procedure:

1. Shift production to DR region
2. Notify Customer Base what happened

DR Region Offline (power and/or network)

- CRM, Telephony, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT possibly affected
- Web application unavailable
- Remote Staff unaffected (US)

Procedure:

1. Notify Customer Base that web application is offline
2. Normal operations continue

SaaS Tools Down

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

Procedure:
Telephony Down

1. Notify Customer Base to use Support Portal or Email
2. Support Staff use Mobile Phones and/or Land Lines as needed

Email Down (Gmail/Corp Email)

1. Support Staff manually manage 'case' related communications

CRM Down

1. Notify Customer Base that CRM is down

Video Conferencing/ScreenShare Down (Zoom)

1. Support Staff utilize alternate service as needed

Appendix B - RTOs/RPOs

Rank	Asset	Affected Assets	Business Impact	Users	Owners	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Comments / Gaps
1	AWS Data Centers	Web application	Core services	All	Engineering	6 hours	10 min	
	Google Workspace	Network	Core services	All	Engineering			
	Home Office ISP Networks	Network		IT Ops, Development	N/A			
	Subcontractor Networks	Network		Development	N/A			
	Third Party Networks	Network		Sales	N/A			
	Company Laptops	Hardware		All	IT Ops			
	Personal Mobile Device	Hardware						