

Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: CTO

Effective Date: September 12, 2022

Purpose

The purpose of this business continuity plan is to prepare ScreenSteps 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 ScreenSteps IT systems that are business critical. This policy applies to all employees of ScreenSteps and to all relevant external parties, including but not limited to ScreenSteps 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., AWS, Chargebee, etc.)
- The Perimeter 81 VPN is unavailable

In the event of a loss of availability of a hosting service provider, the CTO will confer with the engineering team 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 an employee's workspace (i.e. home), 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 an employee's workspace (i.e. home) becomes unavailable due to a disaster, they have the option to work from any safe location when their situation stabilizes.

Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting employee workspaces or operations.

Communications shall take place over any available regular channels including Slack, email, or phone.

Contact information for key contacts can be found in the Slack > People & user groups section.

Roles and Responsibilities

Role	Responsibility
CTO	The CTO 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 and the IT Manager.
Departmental Heads or Managers	Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue working from alternative locations.
Director of Customer Success	The Director of Customer Success, 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.
CTO	The CTO shall be responsible for leading efforts to maintain continuity of services to customers during a disaster.
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.

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

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer Product Service Delivery	Rely on AWS, Elastic Cloud availability commitments and SLAs. Rely on other related 3rd party vendor commitments.

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 an employee workspace or a critical service goes down.

Version	Date	Description	Author	Approved by
1.0	07-Sep-2022	First Version	Jeremy Brown and Trevor DeVore	Jeremy Brown

Appendix A – Business Continuity Procedures by Scenario

Business Continuity Scenarios

Employee Home Workspace Offline (power and/or network)

- Employee is only person affected

Procedure:

1. If workspace is offline for > 30 minutes then notify manager in Slack
2. If workspace is offline > 4 hours then discuss options with manager in Slack

On-call Employee Workspace Offline (power and/or network)

- Employee is unable to respond to monitoring events and raised alarms

Procedure:

1. Notify manager or management at earliest ability and ensure a transfer of responsibility

SaaS Tools Down

- CRM, Telephony, Video Conferencing/Screen Share, or Corp Email may be affected
- Customer Support may be unable to process new or existing cases
- Remote Staff may not be able to communicate with other staff through Slack

Procedures:

1. If Zendesk is down consider directing support@screensteps.com to a Google Group where employees can respond to new enquiries. Once Zendesk is back up then move the history of any communications back into Zendesk.
2. Contact other staff via whichever channel is still available (i.e. Slack, telephone, or email)

Telephony Down

1. Notify Customer Base via a banner on screensteps.com to use Support Portal or Email

Email Down (Gmail/Corp Email)

1. Sales should consider calling contacts directly or creating tickets in Zendesk and directing the person to use the Zendesk support portal
2. Direct customers to use the customer support portal to send us responses
3. Depending on severity IT can reconfigure MX records in Cloudflare so that Cloudflare handles email address. support@screensteps.com could then be routed to support@bluemango.zendesk.com so that support could continue to interface with customers.

Video Conferencing/ScreenShare Down (Zoom)

1. Support Staff utilize alternate service as needed