Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: Neil Cameron

Effective Date: 1 May 2023

Purpose

The purpose of this business continuity plan is to prepare Make and Grow ltd 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 Make and Grow ltd IT systems that are business critical. This policy applies to all employees of Make and Grow ltd and to all relevant external parties, including but not limited to Make and Grow ltd 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. Heroku)
- Loss of availability of Make and Grow ltd satellite offices (these will be considered incidents)

In the event of a loss of availability of a hosting service provider, the CTO will confer with the senior engineers and the CEO 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 the Make and Grow ltd 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.

Alternate Work Facilities

If the Make and Grow ltd office becomes unavailable due to a disaster, all staff shall work remotely from their homes or any safe location.

Communications and Escalation

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

Communications shall take place over any available regular channels including Slack, Google Workspace and WhatsApp

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

Roles and Responsibilities

Role	Responsibility
CTO	The CTO shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems.
Function Leads	Each function lead 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.
Customer Success Lead	The CS Lead 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.
Engineering Lead	The Engineering Lead, in conjunction with the CS Lead shall be responsible for leading efforts to maintain continuity of Make and Grow ltd services to customers during a disaster.

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 Heroku / Salesforce availability commitments and SLAs
IT Operations	Not dependent on HQ. 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 Make and Grow ltd office, or a natural disaster (i.e., severe weather, regional power outage, earthquake) affecting the UK.

Version	Date	Description	Author	Approved by
1.0	1 May 2023	First Version	Neil Cameron	Jonny Burch

Appendix A - Business Continuity Procedures by Scenario

Business Continuity Scenarios

Hosting Provider Down (power and/or network)

- Production application offline

Procedure:

1. Notify Customer Base that service is disrupted
2. Contact Heroku support for status update
3. Ascertain whether issue is with Heroku or our own configuration
4. If issue is with Heroku
    1. Communicate with customer base
    2. Follow updates on twitter https://twitter.com/herokustatus
    3. Stand by for any configuration changes required
5. If issue is with our own configuration
    1. Assemble senior engineers in Google Meet
    2. Determine the nature of issue
    3. Work collaboratively to solve

SaaS Tools Down

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

Procedures:

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
2. Support Staff use alternate email accounts as needed (Hotmail)

CRM Down

1. Notify Customer Base that CRM is down
2. Activate ‘Spreadsheet' Case Tracking (Google Sheets)
3. Leverage ‘Production' Database for Entitlements, Case History, Configuration data.

Video Conferencing/ScreenShare Down (Google Meet)

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	Salesforce Data Centers	Site	Core services	All	Engineering	24 hours	24 hours	Assume worst case scenario of switching to another hosting provider.