Mentorloop
4 Regent Street
North Richmond, Vic 3000
Australia

Mentorloop Business Continuity & Disaster Recovery Plan

Introduction

Distribution List

This distribution list ensures availability of and access to this document at all times in case of a critical incident and should be regularly audited and updated where necessary.

#	Format	Location
1	Google Doc	Google Doc, Mentorloop Google Drive (visible to all staff)
2	PDF	CTO's laptop
3	PDF	CEO's laptop
4	Physical print	Mentorloop Office

Related Documents

Title
Mentorloop Risk Management Process
Mentorloop Risk Register

Objectives

The objectives of this document are to:

- Identify the activities critical to the stable operation of the organisation
    - Audit the resources (human, equipment, knowledge or other) required to maintain these business activities
    - Analyse the impact on the business of these activities ceasing to function or being significantly impaired
- Develop a considered, planned and tested response to an incident that impairs the functioning of any of these critical business activities, including:
    - The circumstances in which an incident response plan should be invoked
    - Identify which staff members have the authority to declare an incident and invoke a response

        - Identify the team that will be required to implement the incident response plan
        - Establish a communications plan for an incident response scenario
- Develop a clearly documented process for recovering regular operation of critical business activities after an incident, including:
    - Outlining strategies to ensure an effective and expedient recovery
    - Setting reasonable objectives for the timeframe in which recovery should take place
    - A step-by-step checklist to ensure that a successful recovery can be confirmed to have taken place
- Ensure that the details of this plan are kept up to date, tested regularly and reevaluated for effectiveness.

Business Impact Analysis

Critical Business Activities

These critical business activities should be developed, revised and updated in accordance with the Mentorloop Risk Management Process.

Summary of critical business activities

#	Title
1	Regular operation of the Mentorloop application
2	Customer support
3	Sales

1. Regular operation of the Mentorloop application

Description of activity: The Mentorloop application must remain online and operational in order for our customers to use it in accordance with their expectations and requirements. They maintain a mode of regular operation in order to be used by our clients in accordance with their expectations and for us to meet our contractual obligations to them.

Potential outcomes if this activity cannot be provided:

- Breach of SLAs
- Risk of client churn
- Reputational damage
- Loss of revenue

Maximum time activity could be unavailable before losses incurred: three business days. If the application was offline for more than two business days our clients could reasonably expect to be compensated.

Dependency on external services and providers:

- Network and server infrastructure hosting (Amazon Web Services)
- Database hosting (MongoDB Inc)

Priority: Critical

2. Customer support

Description of activity: Mentorloop support team must be contactable by our customers and able to provide support to them in a reasonable timeframe.

Potential outcomes if this activity cannot be provided:

- Risk of client churn
- Reputational damage
- Lost of revenue

Maximum time activity could be unavailable before losses incurred: One business day.

Dependency on external services and providers:

- Email (Google)

Priority: High

3. Sales

Description of activity: Mentorloop is dependent upon walking potential customers through a demonstration of the application to help them determine whether it is suitable for their needs. If the sales team were unable to conduct demonstrations we could expect a downturn in revenue.

Potential outcomes if this activity cannot be provided:

- Loss of revenue

Maximum time activity could be unavailable before losses incurred: One week.

Dependency on external services and providers:

- Network and server infrastructure hosting (Amazon Web Services)
- Database hosting (MongoDB Inc)

Priority: Medium

Incident Response Plan

Activation

This Incident Response Plan should be enacted in the event of any major disruption of the Critical Business Activities listed in the Business Impact Analysis.

It can be activated by any of the following Mentorloop roles: CEO, COO, CTO.

Upon activation, members of the Crisis Management Team should be contacted immediately and notified of the incident and any required details or context. The team should determine as a whole which individuals are required to enact the response, based on the roles and responsibilities outlined in the *Crisis Management Team Roles and Responsibilities.*

Crisis Management Team

Crisis Management Team Roles and Responsibilities

Role	Responsibilities

CEO	- Ensure the business continuity plan has been activated
	- Oversee broader implementation of the response and recovery
	- Communicate with key stakeholders as required
	- Keep key staff informed of changes to the situation
	- Oversee implementation of response and recovery as it pertains to office and facilities
	  - Analysis of impact
	  - Evaluation and implementation of appropriate disaster recovery processes

CTO	- Oversee implementation of response and recovery as it pertains to IT systems and infrastructure
	  - Analysis of impact
	  - Evaluation and implementation of appropriate disaster recovery processes
	  - Keep management informed of any changes to the situation
	- Managing additional engineering resources and support required to enact recovery

Head of Customer Success	- Internal communications with customer success team - External communications with affected customers - Managing additional customer support resources required to enact recovery

Key Contacts

Contact List (Internal)

Name	Contact Number	Role
Lucy Lloyd	+61 418 477 361	CEO
Heidi Holmes	+61 409 966 209	COO
Tracy Powell	+61 432 293 259	CTO

Disaster Recovery Plan

Degradation or loss of regular application operation

Scenario: One or more of the Mentorloop web application environments are unavailable or the quality of service is degraded.

Possible Causes:

- Server failure
- Database failure
- Network layer failure

Impact: Critical business activity #1.

Plan of action:

- Maintain a log of actions taken, including by whom and when.
- Identify the point of failure
    - *Application server instances, database instances, network layer*
- Identify the scope of the damage
    - *Has a single instance gone offline, or is an entire AWS region unavailable?*
- Evaluate potential recovery options
    - *Can the affected component be fixed, ie, server restart?*
    - *Can the affected component be replaced, ie, deploy a new server?*
    - *Do we need to implement a contingency, ie, deploy a new server in a different availability zone*
    - *Do we simply have to wait for a dependency on an external provider, ie, AWS region comes back online*
- Pull a team to enact the recovery option
- Notify management of the selected recovery option, including:

    - Estimated time to recovery
    - Potential side effects or unintended or undesirable outcomes (cost, loss of data)
    - Maintain communications and provide updates in the event of any changes
- Upon completion of recovery, complete an analysis of root cause and effectiveness of response, to be provided to management.

Recovery time objective: < 3 hours

Unavailability of office or facilities

Scenario: The Melbourne office is unable to be used or vital services (ie, power, network connectivity) are degraded or unavailable.

Possible Causes:

- Natural disaster
- Hardware failure
- Network outage

Impact: Critical business activities #2 and #3.

Plan of action:

- Maintain a log of actions taken, including by whom and when
- Identify root cause
- Assess expected time to recover
- If necessary, implement remote work procedures
- Notify internal stakeholders
- Coordinate communications with affected external stakeholders

Recovery time objective: < 2 business days.

Notifications

Program coordinators and admins of affected customers will be notified via email as deemed appropriate by the Crisis Management Team. Notifications will be sent within 3 hours of acknowledgement for an ongoing incident. Other notifications may be sent at resolution of the incident and throughout the incident investigation at Mentorloop's discretion. Participants may also be notified at Mentorloop's discretion.

Test, evaluate, maintain.

This document is to be reviewed regularly as part of the Mentorloop Risk Management Process. Each of the scenarios in the Disaster Recovery Plan are to be tested twice yearly.