Dialogue Health Technologies Inc.
Business Continuity Plan

REVISIONS

Version	Date	Revised by Revision Summary Approved by	Review Date
1.0	2017	- Alexis Smirnov	October 12th, 2017
1.1	2020	Taïna Inamukozi Jean-Nicolas Guillemette	September 30th, 2020
1.2	2021	Taïna Inamukozi Jean-Nicolas Guillemette	December 3rd, 2021
1.3 2022 Annabelle Nicolas	- Formatting, structure, content changes and additions - Business Impact Analysis and Risk Assessment revision		
1.4 2023 Aiham Zawahreh Complete revision based on 2021 version	Minor changes to incorporate Sunlife Reporting requirements for major outages (section SWAT TEAM) Nathalie Delisle	Aiham Zawahreh November 21st, 2022	October 6th 2023

TABLE OF CONTENTS

OVERVIEW

This Business Continuity and Disaster Recovery Plan ("BCP") provides framework for the following processes:
(i) how Dialogue Health Technologies Inc. ("Dialogue", the "Company" or "we") will ensure that its critical business functions, the health and safety of its employees and important assets are maintained during any significant business disruption ("SBD") that may arise on account of a force majeure event; and
(ii) the required steps that Dialogue shall follow to keep functioning during a crisis or disaster.

For the purposes of this BCP, a force majeure event includes any unforeseeable and irresistible event, including external causes with the same characteristics, such as an act of God, fire or explosion, conditions of war, act of military authority, terrorist attacks, outages/blackouts, rebellion or civil disobedience, new pandemic events or other impediment beyond its control,

and other internal causes such as any violence against staff, fraud, malicious or other sabotage act by one of our employees or contractors.

SCOPE OF THE BCP

This policy applies to employees, contractors, consultants, temporaries, and other workers at Dialogue, including all personnel affiliated with third parties.

The scope of this BCP includes:

1. Describing Dialogue's general activities and policy in case of a SBD;
2. Assessing risks to the business which may cause this BCP to be initiated; 3. Listing the critical business functions and their priority order in recovery/continuity; 4. Developing procedures for initiating and deactivating the BCP;
5. Electing alternate business sites & remote work conditions;
6. Summarizing communication procedures with various stakeholders; and
7. Delegating authority and responsibility.

It is important to note that Dialogue's Data Security Incident Response Plan covers our recovery and mitigation strategies in the event of a data security breach or threat while the BCP covers recovery and mitigation strategies for all other risks identified to data security.

BUSINESS DESCRIPTION

Dialogue provides access to virtual health and wellness services to employers, associations, insurers and other organizations (collectively "Clients") for use by their employees, customers, participants and/or members ("Users") respectively. The Users and their families (if applicable), collectively defined as "Members", are all eligible to use these services, for a fee paid by the Clients. The services are provided by medical personnel employed or contracted by Dialogue through the virtual healthcare system on a Dialogue-owned technology platform. Through the virtual care service, Members have access to an Integrated Health Platform, which can include one or many of the following services: Primary Care, Mental Health (stress management and wellbeing), Employee Assistance Program, iCBT program, Wellness and potential for new programs/services to be added in the future.

Such Services consist of:
(i) virtual consultations provided to the Users with the relevant professionals working for Dialogue; and
(ii) the necessary or recommended follow-up services, which include issuance of care/coaching plans, prescriptions, referrals to other specialists or appropriate resources and updates of the medical records of the Users as managed by Dialogue.

The Services and the Platform are accessible through our application available on mobile devices or through a web browser (the "App").

Dialogue uses cloud-based technology and Internet to provide its Services and most of the healthcare professionals, other professionals, counselors, and care/case coordinators providing Services to our Users through the Platform are working remotely.

COMPANY POLICY

Dialogue policy is to respond to a Significant Business Disruption by ensuring the following steps are followed:
i) Safeguarding our personnel's lives and Company's property
ii) Making a financial and operational assessment on the risks and feasibility of continuing our Services
iii) Protecting all of the Company's records and books,
iv) Protecting the confidentiality, integrity and availability of the Users data from activation to the deactivation of the BCP
v) Quickly recovering and resuming operations

In the event that we determine we are unable to continue to provide our Services, we will assure prompt communication with our Users, customers, employees and contractors in compliance with our contractual and legal obligations. Notably, all Users requesting healthcare consultations

will be redirected to a physical point of care location if they cannot be assessed or treated through a virtual appointment.

It is important to note that Dialogue's scope of practice does not include the replacement of any urgent care and thus, all Users in need of urgent medical care, in the presence of a significant business disruption or not, are always redirected to the nearest in-person clinic or emergency room.

DEFINITIONS

BCP (Business Continuity Plan) : A Business Continuity Plan provides a framework, guidance, and concept of operations to support businesses to continue and/or rapidly restore their critical business functions in the event of a disruption to normal operations.

RTO (Recovery Time Objective) : Maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs

RPO (Recovery Point Objective) : Maximum acceptable amount of data loss after an unplanned data-loss incident, expressed as an amount of time.

SLA (Service Level Agreement) : A service level agreement is a contract between a service provider and a customer, defining the types and standards of services to be offered.

CONDITIONS OF THE BCP

The following BCP is conditional in that the following conditions must be met in order for the BCP to be initiated:
(i) An event or series of events occurs which causes a SBD to critical business function operations or mission-critical systems; OR
(ii) An event or series of events occurs which causes our employees and contractors' inability to use workspaces and work facilities.

PLAN LOCATION AND ACCESS

Dialogue will maintain copies of its BCP, the annual reviews, and the changes that have been made to it for inspection upon specific request or as provided in our agreements with our customers. An electronic copy of our plan is located on a secured Google drive folder and therefore multiple times mirrored on Google servers and our employees' hard drives as well.

CRITICAL BUSINESS FUNCTIONS

As per Dialogue's business description and objectives, the critical business functions of Dialogue are the following:

1. Offer our Users continuous access to consultations with our professionals via the platform ("Critical Business Function 1");
2. Offer the consultations' follow-up services to Users (issuance of care/coaching plans, prescriptions, referrals, medical record updating, User support as needed) through the Platform ("Critical Business Function 2").

In case of an SBD, ensuring continuity of our critical business functions implies us ensuring the following:

1. Optimal availability of our employees and contractors (e.g. our personnel) to consult with Users; and
2. Maintenance of our mission critical systems as necessary for Dialogue to provide the consultations services and the follow-up services;

It is understood that in case of an SBD, priority will be given to Critical Business Function 1, i.e. provide consultation to our Users and Critical Business Function 2 will resume as soon as possible once Critical Business Function 1 is up and running again.

MISSION-CRITICAL SYSTEMS

Dialogue's mission-critical systems are those that ensure our ability to provide our Services.

More specifically, these systems are the following:

For Critical Business Function 1:

1. Dialogue Care Platform (i.e. the Platform) through which our consultation services are provided;
2. The HR Admin console by which our customers are able to manage eligibility of the Users to receive our services (as well as addition or deletion of Users as required); 3. Our infrastructure services that support the Platform and the App.
4. Call Center hosted by Bell
5. Microsoft Azure platform
6. PowerBI for the visualization and access to data

For Critical Business Function 2:

1. Dialogue Care Platform (i.e. the Platform) through which our follow-up services are provided;
2. The HR Admin console by which our customers are able to manage eligibility of the Users to receive our services (as well as addition or deletion of Users as required); 3. Our infrastructure services that support the Platform and the App;
4. The Input Health system that enables our healthcare professionals to maintain the electronic medical records of each User, issue prescriptions and referrals.Call Center

hosted by Bell

5. Microsoft Azure platform
6. PowerBI for the visualization and access to data

Systems 1, 2 and 3 are located off-site and hosted in a data center operated by a leading Cloud Infrastructure Provider (AWS). To learn more about AWS business continuity management, please see:
https://aws.amazon.com/compliance/data-center/controls/

Three mission-critical systems (The Care Platform, HR Admin Console and Infrastructure Service that support the platform and the app) benefit from the redundancy of AWS (Amazon Web Services) that has three redundant data centers within the Canada Central region.

System 4 (Critical Business Function 2) is provided by supplier Input Health, who has a Disaster Recovery Plan in place in case of an SBD. Input Health' Business Continuity and Disaster Recovery measures include an off-site data storage facility with fully mirrored key business processes.

System 5, (Critical Business Function 1 and 2) Azure SQL Database is a fully managed relational database with built-in regional high availability and turnkey geo-replication to any Azure region.

https://azure.microsoft.com/en-us/support/legal/sla/azure-sql-database/v1_8/

System 6 (Critical Business Function 1 and 2) Power BI, guarantees at least 99.9% availability of Power BI Embedded for users to execute API calls and embed reports.

https://azure.microsoft.com/en-us/support/legal/sla/power-bi-embedded/v1_1/

For Systems 5 and 6, database backup processes and recovery procedures exist and are tested annually by our IT partner Optima.

PLAN ACTIVATION PROCEDURES

In the event of an SBD, Dialogue Business Continuity Team (BCT) will be in charge of the activation of this BCP. The BCT will be responsible for:

1. Responding immediately to the potential SBD and calling the emergency services, as required, depending on the situation;
2. Assessing the extent of the SBD and its impact on the critical business functions of Dialogue;
3. Deciding which elements of the BCP shall be activated;
4. Creating a SWAT team that will assist the BCT, if needed;
5. Advising all personnel that the BCP plan has been activated and advising on the next steps by means of this instruction sheet;
6. Ensuring continuity of the critical business functions as per the Recovery Objectives set forth below;
7. Preparing any necessary procedures; and
8. As soon as required, beginning the deactivation procedures.

SBD ALERT

Depending on the nature of the SBD, either one of the Dialogue personnel discovering the SBD will call a member of the BCT in the order listed below or the BCT will activate the plan as soon as the SBD occurs.

BUSINESS CONTINUITY TEAM

- Jean-Nicolas Guillemette (Chief Operations Officer)
- Alexis Smirnov (Chief Technology Officer)
- Jaclyn Rappaport (Director of Primary Care Operations)
- Nathalie Delisle (General Counsel)

If the above people are not available, try:

- Cherif Habib (CEO)
- Dayna Murray (Director of MH, EAP, iCBT Operations)
- John McCalla (Vice President Engineering)

SWAT TEAM

The BCT may set up a dedicated SWAT team, with relevant members and stakeholders to outline objectives and key results. Project managers may be nominated in order to coordinate and carry out the initiatives. A clear internal and/or external communication plan may be created using the appropriate channels. A plan may be outlined for the return to normal followed by a post-mortem exercise.

The SWAT team is responsible for determining the need to inform Sun Life of major SBD. For SBD that extends beyond Dialogue's RTO (4hr), Sun life needs to be informed within 48hrs of the incident detection.

Sun Life contacts

- Ayoub Jivraj (ayoub.jivraj@sunlife.com) is the AVP within the Canadian business technology support team who oversees system outage incidents.
- Ali Kassam (ali.kassam@sunlife.com), from corporate technology team oversees the reporting of incidents to OSFI

ALTERNATE BUSINESS SITE

The alternate business site will consist of relocation to remote work that will be used in the event of an SBD that inhibits the continuation of the critical business functions at the original business site. This strategy includes relocation to remote work during both short-term and long-term disruptions affecting Critical Business Function #1,2 or both.

In the event that the SBD impacts our main office only (i.e. Location #1, Appendix A), we may also decide to relocate some of our operations and establish a command center (notably for our Business Continuity Team) at the Alternate Office Location (Appendix A. However, we mostly rely on remote work and we have the capacity to do so, therefore, the probability that this will occur is low.

It should be noted that approximately 90% of our personnel providing Dialogue's services work remotely, therefore these transitions should be relatively seamless.

ALTERNATE BUSINESS SITE DETAILS

When it comes to an SBD that may affect our offices or personnel:

1. Our personnel, not already working remotely, will be notified by one member of the BCT

that they are directed to initiate remote work procedures. Personnel will cease normal business activities and begin preparations to move home to begin remote work. In the case that there is no immediate threat or danger to health and safety, employees will wrap up what they are doing, adapt to remote work and will gather their personal belongings and necessary items from work that they are approved to bring home.

2. Personnel will begin remote work from home.
3. BCT will check in (directly or via delegates) and make sure every employee has made it safely home.
4. BCT will ensure continuity of the consultations services established at the employees' homes; and
5. BCT will ensure continuity of the follow-up services established at the employees' homes.

As mentioned above, all personnel working from our offices will transition to home offices for daily business. We will maintain security and business continuity by:

a) Implementing employee remote work procedures; and
b) Ensuring that all employees follow the Talent and Culture Policy and any policies or procedures it references in regards to remote work

The following considerations must be addressed when implementing remote work procedures:

i) Physical and information security of the employees home office setup
ii) Access to critical equipment and supplies, or can be prepared with essential equipment

and supplies within 12 hours of the BCP activation,
iii) Ability to receive replacement equipment and required redundant power supplies, peripherals, etc, up to 24 hours after reporting a damaged, lost or non-serviceable piece of equipment
iv) Access to critical dependencies for relevant business processes (email, CRM, etc.) v) Employee health, social, mental wellbeing and comfort while in remote working conditions.

We rely on cloud services in order to maintain our mission critical systems, thus a redundancy and failover plan for cloud services by region will be established with AWS and Input Health, as necessary.

Alternate mission critical systems processes will be achieved by:

a) Relying on automatic backup;
b) Creating snapshots of environments; and
c) Syncing to an alternate region with AWS and Input Health.

BUSINESS CONTINUITY SCENARIOS

The following scenarios were determined to have the highest risk scores during the Risk Assessment and Business Impact Analysis exercises. Resolution processes for each risk are summarized below:

Telecommunication Network Outage/Power Outage

Resolution Process/Risk Prevention:

- The BCT and/or SWAT team will assure prompt communication with clients and partners to advise them of the situation
- An on-call notification will be sent out by the Service Level Specialist on duty in order to contact employees with different service providers to manage the demand on the Care Platform.
- The Care Platform will remain accessible to members who still have service and/or internet as the Care Platform benefits from the redundancy of AWS (Amazon Web Services) that has three redundant data centers within the Canada Central region.
- Due to the unpredictable nature of internet and power outages, it is impossible to know when access to the internet or phone services will be available again therefore we place our emphasis on communication and ensuring our clients and partners are kept informed every step of the way

Cyber-attack, Breach of Confidentiality

Resolution Process/Risk Prevention:

- Suppliers of mission critical systems with highest security standards, periodical security assessments, encryption at rest and on transit.
- Cyber and Security awareness training mandatory for all staff to complete annually
- Privacy training provided to all staff
- Dialogue's Data Security Incident Response Plan will be activated.

Fraud, sabotage or other malicious acts by one employee

Resolution Process/Risk Prevention:

- System restrictions and access restrictions in place, in addition to activity monitoring to prevent such an event from occuring
- Dialogue's Data Security Incident Response Plan will be activated

Simultaneous resignation or loss of key staff

Resolution Process/Risk Prevention:

- Designated successors and succession plans for key staff such as: Directors, VP, Officers
- Robust talent development programs in place

Information Technology issues (Hardware Failure, Lost/Corrupted Data, Application Failure)

Resolution Process/Risk Prevention:

- AWS and Inputhealth, both suppliers of our mission critical systems have their own BCP's which provide redundant updates and weekly checks to ensure back-up system is intact with backup systems being located off-site and fully mirrored.

Regulatory Change Disclaimer: Our Legal and Government Relations teams closely and consistently monitor policy/regulatory trends in order to advise the business on potential policy/regulatory changes and their anticipated impacts on its operations. These teams report to the regulatory SWAT team, which consists of Dialogue's executive team, along with Dialogue's Medical Director, to inform the development of risk mitigation strategies and determine the opportunities for risk disclosure.

RISK ASSESSMENT

Document can be found here

BUSINESS IMPACT ANALYSIS

Document can be found here

RECOVERY OBJECTIVES:

MISSION CRITICAL SYSTEMS:

The maximum length of time mission-critical systems can be down before the SBD impacts our business are as follows:

- For Systems 1, 2 and 3:
    - As these Systems support access to the Platform and App and thus to our Services, the maximum length of time these mission critical systems can be down is <4 hours (RTO) .
    - Unlike snapshot-based solutions that update target locations at distinct, infrequent intervals, AWS uses continuous data protection, enabling a Recovery Point Objective (RPO) of <5 minutes.

https://aws.amazon.com/blogs/storage/point-in-time-recovery-and-continuous-backup-for-amazon-rds-with-aws-backup/

- For System 4 (Input Health System - Critical Business Function 2):
    - The maximum length of time this system can be down is estimated to be < **four (4) hours**.

In case of any SBD affecting our mission-critical systems:

- Dialogue's Chief Technology Officer will liaise with AWS to establish a redundancy and failover plan as soon as possible following the SBD; and
- Dialogue's Chief Operations Officer will delegate or liaise with InputHealth to establish a redundancy and failover plan as soon as possible following the SBD.

OTHER SYSTEMS AND PERSONNEL PLANS:

In a disruption affecting our business district, city, or region, we will transfer our operations to personnel located outside of the affected area, and recover and resume business within **two (2) hours.** It has to be noted that in most of the provinces where we operate, our personnel, especially the professionals providing the consultations to our Users (Critical Business Function 1) can be found throughout the provinces, (i.e. they are not concentrated in large urban centers), thus reducing the risk of impact to our business when an SBD occurs in a specific area**.**

These recovery-time objectives are not hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day,

scope of disruption and status of critical infrastructure, particularly telecommunications, can affect actual recovery times. Recovery refers to the capacity of Dialogue resuming all activities after a wide-scale disruption. It is also important to note that all Dialogue Services are provided via the Internet and thus Dialogue will not be able to provide any services should the Internet be down for all Canadian Internet Providers.

DATA BACK-UP AND RECOVERY (HARD COPY AND ELECTRONIC)

Dialogue maintains its primary hard copy books and records at its office location in Montreal, to the exception of any Company incorporation documents and other corporate documents which are maintained by our external counsels at their offices located in Montreal. Hard copies of incorporation and corporate documents are held at the Dialogue Australia / eHH Registered Office at 31 Clements Street, Russell Lea, NSW 2046 Australia. Hard copies of notarial deeds and communications with authorities are held at the Dialogue Germany Office at Ohmstrasse 11, 80802 Munich, Bavaria, Germany.

In addition, Dialogue mission critical systems are managed by AWS RDS, which has automatic backup as described in AWS documentation (https://aws.amazon.com/rds/faqs/), and by Input Health, which has a backup strategy for each of its key business processes.

Backup copies of books, records and all other business documents (including any electronic records) are stored in Google GSuite, which also has automatic managed backups (https://support.google.com/a/answer/7376096).

Dialogue's Chief Technology Officer, with the help of Dialogue's Compliance Manager and legal counsel, are responsible for the maintenance of these books, records and any backup copies of said books,records and all other necessary documents.

In the event of an internal or external SBD that causes the loss of our paper records, we will recover them from our external counsels physically, or recover them electronically through Google G Suite back-up.

ALTERNATE COMMUNICATIONS BETWEEN DIALOGUE AND ITS CUSTOMERS, ITS SUPPLIERS, EMPLOYEES AND CONTRACTORS

CUSTOMERS AND SUPPLIERS

We now communicate with our customers and Users using our Platform, phone, email and fax. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by email but the Platform or Internet is unavailable, we will call them on the telephone and

follow up where a record is needed with a paper copy in the mail.

EMPLOYEES AND CONTRACTORS

We now communicate with our employees and contractors using phone, email, Slack, in-person communication, and various other tools. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. We will also employ a call tree so that senior management can reach all employees quickly during an SBD.

PLAN DEACTIVATION PROCEDURES

This section is the process in which business returns to normal or a state of permanence. The end result of permanence may not look exactly like before the plan activation. The goal of the deactivation is to re-establish the full capability of the business to a state in which resources are focused on growth and proactivity rather than survival.

The BCT will select and communicate the criteria, the timeline, and manner in which Dialogue deactivates the BCP plan. The deactivation of the plan will notably begin when the following criteria are met:

(i) The primary business site has been confirmed to be sufficient in terms of safety, environmental and physical security;

(ii) Critical business functions have been completely restored at the primary business site; and

(iii) Equipment, supplies and procurement capacity is able to support plan deactivation.

UPDATES AND ANNUAL REVIEW AND TESTING

Any person of the BCT has the authority to execute this BCP.

Dialogue will update this BCP whenever we have a material change to our operations, structure, business or location or there is any change in market conditions and legal/regulatory requirements. In addition, the BCT, with the help of our Compliance Manager will meet, review and test this BCP annually and will make all necessary updates, as needed.

A copy of the 2022 Test Report can be found here

DISCLOSURE OF THIS BCP

Attached is our written BCP disclosure statement we provide to our customers upon request. We can also provide a full copy of this BCP to our customers upon request.

SENIOR MANAGER APPROVAL

I have approved this Business Continuity and Disaster Recovery Plan as reasonably designed

to enable Dialogue to meet its obligations to customers, Users, employees and contractors in the event of an SBD.

_____

By : Nathalie Delisle
Title: General Counsel

APPENDICES

APPENDIX A

Office Location #1	Office Location #2
390 Notre-Dame West Street, #200, Montreal, QC, H2Y 1T	10 King Street East, Suite 900, Toronto, ON, M5C 1C3.

Alternate Office Location
Power Corporation of Canada 751 Victoria Square, Montreal, Quebec H2Y 2J3

Dialogue's Business Continuity Plan - Disclosure Statement

Dialogue Technologies Inc. ("Dialogue" or the "Company") has developed a Business Continuity Plan (BCP) on how we will respond to events that significantly disrupt our business. Since the timing and impact of disasters and disruptions is unpredictable, we will have to be flexible in responding to actual events as they occur. With that in mind, we are providing you with this information summary on our business continuity plan.

Contacting Us – If after a significant business disruption (SBD as defined in the BCP), you cannot contact us as you usually do, we will dedicate a special page for this emergency situation on our website at www.dialogue.co.

Our Business Continuity Plan – We plan to quickly recover and resume business operations after an SBD and respond by safeguarding our personnel's lives and Company's property, making a financial and operational assessment on the risks and feasibility of continuing our Services, protecting all of the Company's records, books and the confidentiality, integrity and availability of the data of our Users from activation to the deactivation of the BCP, and quickly recovering and resuming operations. Our business continuity plan is thus designed to permit our Company to resume its critical business functions as quickly as possible, given the scope and severity of the SBD.

Our business continuity plan thus notably addresses: data backup and recovery; our critical business functions, all mission critical systems; alternative communications with customers, suppliers, employees and contractors; alternate physical location of employees; and assuring our customers prompt communication if we are unable to continue our business.

Our IT suppliers back up our mission critical systems in a geographically separate area. While every emergency situation poses unique problems based on external factors, such as time of day and the severity of the SBD, we have been advised by our suppliers that they would generally be able to restore our own operations so that we can provide our Services within a matter of minutes. It should be noted that access to our Platform by Users or to our HR Admin Console by Clients may be delayed during this time, as well as the median wait time to speak with one of our case/care coordinators or professionals.

Varying Disruptions – SBD can vary in their scope, such as only our Company, a single building housing our Company, the business district where our Company is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our Company or a building housing our Company, we will transfer our operations to a local site when needed and expect to recover and resume business within a matter of minutes. In a disruption affecting our business district, city, or region, we will transfer our operations to a site outside of the affected area, and recover and resume business within **two (2) hours**. In either situation, we plan to

continue in business and notify you through our website www.dialogue.co. We will also provide you with our customer emergency number. If the SBD is so severe that it prevents us from remaining in business, we will assure prompt communications with our customers and users.

For more information – If you have questions about our business continuity planning, you can contact us at legal@dialogue.co.