



## Breathe Life

### System and Organization Controls SOC 3<sup>®</sup> Report

Report on Breathe Life's system relevant to security throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020.

November 18<sup>th</sup>, 2020 - **CONFIDENTIAL**

# Table of contents

Section 1 – Independent Service Auditor’s Report	1
Section 2 – Statement by Breathe Life Service Organization	4
Section 3 – Breathe Life System Description	5

# Section 1 – Independent Service Auditor’s Report

## Independent Service Auditor's Report

### To: Breathe Life Service Organization

#### Scope

We have been engaged to report on Breathe Life's accompanying statement titled "Statement by Management of Breathe Life Service Organization" ("statement") that the controls within Breathe Life's system ("system") were effective throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020, to provide reasonable assurance that Breathe Life's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

#### Service Organization's Responsibilities

Breathe Life is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Breathe Life's service commitments and system requirements were achieved. Breathe Life has also provided the accompanying statement about the effectiveness of controls within the system. When preparing its statement, Breathe Life is responsible for selecting, and identifying in its statement, the applicable trust services criteria and for having a reasonable basis for its statement by performing an assessment of the effectiveness of the controls within the system.

#### Our Independence and Quality Control

We have complied with the relevant rules of professional conduct and code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies Canadian Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

#### Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on whether management's statement that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements (CSAE) 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, published in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether management's statement is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our reasonable assurance engagement included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Breathe Life's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Breathe Life's service commitments and system requirements based on the applicable trust services criteria
- Performing such other procedures as we considered necessary in the circumstances.

### **Inherent Limitations**

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become ineffective because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### **Opinion**

In our opinion, management's statement that the controls within Breathe Life's system were effective throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020, to provide reasonable assurance that Breathe Life's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte LLP

*Deloitte LLP*<sub>1</sub>

Samantha Welscheid

Partner, Deloitte  
Montreal, Quebec, Canada  
November 18<sup>th</sup>, 2020

---

<sup>1</sup> CPA auditor, public accountancy permit No. A129441

# Section 2 – Statement by Management of Breathe Life Service Organization

## Statement by Management of Breathe Life Service Organization

We are responsible for designing, implementing, operating, and maintaining effective controls within Breathe Life Service Organization’s (Breathe Life’s) system (“system”) throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020, to provide reasonable assurance that Breathe Life’s service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our statement.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020, to provide reasonable assurance that Breathe Life’s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Breathe Life’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 3.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We confirm that the controls within the system were effective throughout the period August 1<sup>st</sup>, 2019 to July 31<sup>st</sup>, 2020, to provide reasonable assurance that Breathe Life’s service commitments and system requirements were achieved based on the applicable trust services criteria.



**Ian Jeffrey**  
Chief Executive Officer  
Breathe Life

November 18<sup>th</sup>, 2020

# Section 3 – Breathe Life system Description

## Company Overview

Breathe Life Inc. was founded in 2017 by Ian Jeffrey, Sebastien Malherbe, Jean-Nicholas Hould, and Arach Tchoupani. They had the vision to make financial security accessible to everyone. To achieve this, they set about building a digital distribution platform for the life insurance industry. Breathe Life Inc. is headquartered in Montreal, Quebec, Canada.

## Description of Services

Breathe Life provides life insurers with a modern end-to-end platform that increases the speed of policy delivery and reduces operational costs for the distribution of financial security products. The omnichannel platform allows carriers to distribute their products through an advisor, directly online, or anywhere in between.

## Internal Controls

Breathe Life's internal controls are encompassed in a set of policies and procedures, with oversight by its Executive Management Team ("EMT") and other personnel, in order to provide reasonable assurance regarding the achievement of its objectives.

### Executive Management Team

Breathe Life's Chief Executive Officer (CEO) manages Breathe Life's activities on a daily basis with assistance from the EMT, representing all functions of the business. The CEO assigns authority and responsibility for operating activities, and establishes reporting relationships and authorization hierarchies.

### Organizational Structure and Assignment of Authority and Responsibility

Breathe Life's organization and distribution of responsibilities and authority provide the framework within which its activities for achieving company-wide objectives are planned, executed, controlled, and monitored.

Led by the EMT, Breathe Life's organization includes General Admin, Engineering, Product, Data, Sales, Client Success, and Marketing.

## Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of Breathe Life's internal controls system. The purpose of Breathe Life's risk assessment process is to identify, assess, and manage risks that can potentially affect Breathe Life's ability to operate and provide reliable services to its clients and customers.

Breathe Life maintains an Information Security Policy which is communicated to staff to ensure that individuals utilizing Breathe Life resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

## Control Activities - Organizational Controls

The people who make up part of the Breathe Life team are the most critical element of the company. This section describes the controls related to aspects of human resources management.

### Recruitment

Formal job descriptions exist for all positions. These documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.

Candidates are screened, interviewed, and given technical tests by HR, team members from that specific environment, and the EMT. As part of the hiring process, background checks are performed including pre-employment, education, financial and/or criminal verifications.

### Onboarding

New employees are required to sign an Employment Agreement, which includes standard employment terms including requirements to conform with Breathe Life's standard policies and procedures. New employees and contractors must read, accept and sign the Information Security Policy and Code of Conduct confirming their understanding of the rules and internal procedures regarding security and ethics and their commitment to respect them.

The hiring manager or the HR Manager requests, through an online ticketing system, the creation of an employee account, which will be provisioned by a system administrator, according to the role of the new employee. Each role has a specific set of tools and services that the new hire is authorized to access.

### Offboarding

In the case of Non-voluntary offboarding (termination) the manager, the HR Manager and the employee meet, and the termination letter is delivered to the employee. The leaving employee / contractor is reminded of surviving requirements, such as non-competition and respecting intellectual property and confidentiality (extending to clients and customer information and data), which is already defined in the employee / contractor's contract. Office keys, hardware authentication device, laptop and computer accessories as per the Hardware Inventory list are collected and the system administrator disables the accesses immediately in the case of involuntary terminations or within 24 hours; and in the case of a voluntary termination of the employment contract, the offboarding checklist is completed at a mutually agreed date.

## Control Activities - Information security controls

### Physical Access

Breathe Life currently hosts its system in Google Cloud Platform data centers that are physically located in Canada for Canadian customers and in the US for US customers.

### Infrastructure

Infrastructure as Code (IaC) is used to configure and deploy the cloud infrastructure. The infrastructure configuration is stored and version-controlled in a human-readable declarative configuration file in our GitHub repository.

Database as a Service (DbaaS) is used for storing application data. A separate database, on a separate database instance, is created for each client. Databases are backed up on a frequent basis and failover configuration is also in place. Multiple layers of encryption are used to protect sensitive data, such as PHI.

## Monitoring

Breathe Life utilizes a variety of cloud-based monitoring and logging tools, such as Sumo Logic, Datadog, Sentry and StackDriver, to continuously monitor the applications and system infrastructure for security and availability vulnerabilities and performance issues and get notified in real-time in case of meaningful events.

## Antivirus and Threat Detection and Prevention

Employee workstations are equipped with a next-generation antivirus solution, which not only prevents known malware from being executed, but also detects and prevents unknown malware and attacks that exploit vulnerabilities through indicators of attacks and machine learning techniques.

## Vulnerability Management

A penetration test is conducted by an independent Security Assessment Vendor on an annual basis in order to identify vulnerabilities within the infrastructure or the applications developed by the engineering team. Automated and active vulnerability monitoring of third-party open source libraries is in place using Software Composition Analysis solutions, such as Snyk and GitHub security. Automated scanning of the application middleware which is contained within the Docker container images is also executed automatically every time a new Docker image is built and pushed to our images registry in our CI/CD pipeline.

## Network

Data flowing between the clients' device and our system is encrypted in transit using TLS. By default, ingress is blocked on the network from external traffic using firewall rules and only specific and valid endpoints are made available to external traffic using managed load balancers from Google Cloud.

## Authentication and Authorization

The system administrator role is limited to a small number of the most senior members of the Engineering team with the highest security qualifications. Internal and external user credentials adhere to established corporate standards for password length and complexity requirements. The principle of Least Privilege is followed, therefore permissions are provided on a need-to-know basis for individuals' accounts as well as for the service accounts that are running the systems.

## Incident Response

Breathe Life's Security Incident Response Plan describes the responsibilities of key individuals following a security incident. For high severity security incidents, a root cause analysis is also prepared and reviewed by the EMT and based on the analysis, relevant risk management data is updated to reflect the planned incident and problem resolution.

## Asset Management

The Information Security Policy includes sections on asset management and information classification to establish the level of confidentiality and classification of data and define clear rules and responsibility for the use of the information system and other information assets.

## Design and Planning

The onboarding of new clients requires several phases. Such as a kick-off meeting, roadmap creation, and then planning, design, and development. Breathe Life's development process follows the Scrum methodology. In the event of major IT projects, which are characterized by a new product entirely or a change to an existing product requiring a refactoring of the existing system architecture, confidentiality and security issues are analyzed through a threat modeling exercise.

## Software Development

Breathe Life has documented a Software Development Life Cycle (SDLC) Management policy which identifies multiple security measures that must be followed by the development team through every phase of the SDLC process.

## Information and Communication

### Internal Communication

As indicated previously, each new employee receives the Breathe Life Organization Chart, the Information Security Policy, the Code of Conduct, and the Team Handbook. These documents must be acknowledged by every employee, some on an annual basis. Each employee and contractor of Breathe Life is made aware of the security implications that revolve around their functions and actions. This process begins with providing individuals with the understanding and knowledge needed to help secure Breathe Life's system and its clients and customers and their data within established policies. A yearly Security awareness training includes the message that individuals can have a significant impact on the overall security of an organization.

### External Communication

Breathe Life has procedures in place that ensure its customers are notified of any major event, such as high severity security incidents or changes that affect system security or availability.

## Monitoring

A cross-functional Governance Risks and Control (GRC) team at Breathe Life, which comprise members of the EMT, HR and security, is responsible for assessing the effectiveness of the internal controls. This activity is done on a yearly basis and the assessment results are documented in our documents repository.