fitabase

NOTICE

This document was written and produced by:

Small Steps Labs LLC

4705 35TH STREET, SAN DIEGO, CA 92116

Cybersecurity Operations

REVISION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
7/29/2021	1.0	Draft	L Trotter II
12/15/2021	1.0	Approved\Final	CISO

Table of Contents

Introduction

Small Steps Labs LLC, which shall hereafter be referred to as “Fitabase,“ is committed to ensuring that the cybersecurity program is designed, implemented, and communicated to the workforce (employees, contractors, and vendors) consistently. The cybersecurity program, roles, responsibilities, regulations, and operations are part of our commitment to deliver services with integrity.

Scope

The business environment analysis applies to all entities included in the organizational chart of Fitabase, which individually may be referred to as "workforce." Entities currently included are employees, contractors, and vendors. This document applies to all Fitabase information systems, entities, and departments used to deliver services unless otherwise stated.

Roles and Responsibilities

The following stakeholders have specific responsibilities based on the needs of Fitabase. The **Chief Information Security Officer (CISO)** has been assigned with the following responsibilities.

- Identifying and communicating the organization’s role in the supply chain.
- Identifying and communicating the organization’s place in critical infrastructure and its industry.
- Prioritizing, establishing, and communicating organizational mission, objectives, and activities.
- Determining the organization's dependencies and critical functions to deliver critical services.
- Determining contingency requirements to support delivery of critical services.

Identify: Business Environment (Id.Be)

Fitabase’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Id.Be-1 Communicate Role in Supply Chain

The dependence on products, systems, and services from vendors, and the importance of the relationships with those providers, present an increasing level of

supply chain risks. It is important that Fitabase understands who their customers are and who their vendors are in order of importance. By identifying customers and vendors the organization can better align contingency and incident response activities to ensure minimal interruptions to services in the event of a security incident. Fitabase's customers and vendors shall be identified to the following specifications:

- Document existing and new customers in order of importance;
  - Review this document annually and update accordingly.
- Document existing and new vendors in order of importance. (i.e., which services\products does the organization rely on the most;
  - Review this document annually and update accordingly.
- Develop procedures to communicate with primary vendors\customers in incident response strategy.

ID.BE-2 ROLE IN CRITICAL INFRASTRUCTURE

The requirement for defining critical infrastructure and key resources is based on global and national laws, and regulations. Based on the services provided Fitabase has identified the organization as the following along with the applicable resources for communication:

- The organization manages fitness data however this data is not considered electronic protected health information (ePHI)

ID.BE-3 ORGANIZATIONAL PRIORITIES

Data protection requirements are derived from the mission and business needs defined by organizational stakeholders, the processes designed to meet those needs, and the risk management strategy. Data protection requirements determine the adequate controls for information systems. Inherent to defining protection is an understanding of the adverse impact that could result if a compromise or breach of information occurs. Fitabase has defined the mission and business processes as follows:

- **Our mission** at Fitabase is to enable researchers to use the latest tools, devices, and apps to further our collective knowledge. We are dedicated to making it as easy as possible for researchers to deploy the "new tools of wellness" to measure, track, and engage their participants.
- **Business Processes:** Administration, Operations, Information Technology, Information Security, Customer Service, Infrastructure, Performance Management, and Sales.

ID.BE-4 IDENTIFY CRITICAL FUNCTIONS

Critical information systems, functions, or services require significant protections. The identification of critical systems and functions considers laws, regulations, and system functionality requirements. The operational environment of a system may impact the criticality, including the connections to and dependencies on cyber-physical systems, inter-connected systems, devices, and outsourced IT services. Information system and function criticality are assessed in terms of the impact to a system or function failure on the missions that are supported by the system. Fitabase has identified the following critical functions within the organization:

- Web App Service
- Background Data Processing Services
- 3rd Party Integration Connectors

ID.BE-5 CONTINGENCY REQUIREMENTS

Contingency planning for information systems is part of an overall program for achieving continuity of operations for the mission and business functions. Contingency planning addresses system restoration and implementation of alternative processes when systems are compromised or breached. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Fitabase has identified the following primary systems for the contingency strategy:

- Web App Service
    - downtime requirements 1hr.
    - Backup requirement: Time point restore using previous code deployment snapshots and Azure SQL timepoint data recovery allowing for data snapshots within the past 90 days.
- Background Data Processing Services
    - Downtime Requirements: 1hr
    - Backup requirement: Time point restore using previous code deployment snapshots and Azure SQL timepoint data recovery allowing for data snapshots within the past 90 days.
- 3rd Party Integration Connectors
    - Downtime Requirements: 15 minutes.
    - Mitigation efforts and coordination with our 3rd party partners (Fitbit, Garmin, Dexcom and BodyTrace).

Right to Modify

Fitabase reserves the right to modify this Business Environment Analysis at any time. Changes and modifications will be effective when approved and redistributed.

Enforcement

Sanctions for violations of this policy shall be enforced by the CISO in accordance with the sanctions policy.