
fitabase

NOTICE

This document contains information protected by copyright. Only Small Steps Labs LLC "Fitabase" may photocopy or reproduce any part of this document for training or use by the Small Steps Labs workforce. Any other reproduction of this document or part of this document is prohibited unless Small Steps Labs has provided prior written consent.

The Information in this document is subject to change without notice.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Information in this document may be confidential or proprietary to Small Steps Labs.

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
12/20/2021	1.0	Final	L Trotter II & Aaron Coleman

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 Security Awareness Training Standard 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 **Chief Information Security Officer (CISO)** has been assigned the following responsibilities:

- Manage the development, documentation, implementation, and monitoring of the security awareness training standard document.
- Ensure compliance with regulatory requirements.
- Review and update the security awareness training standard as needed or annually; to address organizational and regulatory changes identified during the business lifecycle.

Pr.At-1 Security Awareness Training

Security Awareness Training for all new and existing Fitabase workforce members shall be required to increase awareness and protect information systems. Fitabase shall provide content that includes a basic understanding of the need for cybersecurity, expectations to maintain secure operations, and how to respond to security incidents. Periodic security training shall be administered to workforce members throughout the year according to the following:

- As part of the training for new hires and at least once annually thereafter.
- In addition to annual training, educational awareness materials shall be delivered in the form of emails, meetings, or paper documents.
- Re-train individuals who fall victim to attacks with lessons learned incorporated in training.

- Keep training records for 6 years.

Training Topics

The following topics shall be provided to the workforce to deliver the proper Security and Privacy training. The underlined topics are required.

Security and Privacy

The purpose of this training is to provide workforce members a general overview of security and privacy in the workplace.

Social Engineering

The purpose of social engineering training is to educate workforce members about the psychological manipulation techniques attackers use via phone calls, phishing emails, and other social interactions to divulge information.

Incident Notification

The purpose of incident notification training is to educate workforce members about the process for reporting malicious, accidental, and suspicious incidents within Fitabase. Some examples include malware identification, mishandling sensitive information, and observing workforce members misusing resources.

PR.AT-2 Staff Training

When selecting content, the following topics shall be included:

- Phishing
- Social Engineering
- Incident Notification (process for reporting security incidents)

PR.AT-3 Vendor Training

Vendors refers to external third parties providing services\products on behalf of Fitabase. Vendors include contractors, cloud providers, and other businesses that provide system development, information technology services, testing or assessment services, outsourced applications, and network\security management, etc. Fitabase shall ensure vendor requirements by implementing the following:

- Explicitly include the following security requirements in acquisition contracts;

    - Vendors are required to review the Acceptable Use and Cybersecurity Policies.
    - Vendors are required to take security awareness training upon hire within 30 days.
- Phishing
- Social Engineering
- Incident Notification

Right to Modify

Fitabase reserves the right to modify this Security Awareness Training Standard 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.