
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
7/21/2021	1.0	Draft	L Trotter II
12/20/2021	1.0	Final	L Trotter II & Aaron Coleman

Table of Contents

Introduction 5

Scope 5

ID.GV-1 Cybersecurity Program 5

- Cybersecurity Framework 5
- Centralized Management 6
- Program Management (PM) 6

Security Controls 7

- Access Control (AC) 7
- Security Awareness Training (AT) 7
- Audit Logging (AU) 7
- Configuration Management (CM) 8
- Identification and Authentication (IA) 8
- Incident Response (IR) 8
- Maintenance (MA) 8
- Media Protection (MP) 8
- Personnel Security (PS) 9
- Physical Security (PE) 9
- Planning (PL) 9
- System and Information Integrity (SI) 9

ID.GV-2 Roles and Responsibilities 9

ID.GV-3 Legal and Regulatory Requirements 10

ID.GV-4 Risk Management 10

- Risk Assessment (RA) 10
- Supply Chain Risk Management (SR) 11
- Security Assessment (CA) 11
- Contingency Planning (CP) 11

Definitions 11

RIGHT TO MODIFY 12
ENFORCEMENT 12

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 Cybersecurity Policy 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.

ID.GV-1 CYBERSECURITY PROGRAM

The Fitabase cybersecurity policy defines the framework and strategy used to align organizational goals with laws, regulations, responsibilities, policy, and security controls. The following sections of this document provides specifics of the legal, operational, and management expectations of the workforce and information systems within the organization.

CYBERSECURITY FRAMEWORK

To ensure a consistent and repeatable process Fitabase has implemented the National Institute of Standards Cybersecurity Framework (NIST CSF). The NIST CSF is compiled of standards, guidelines, and practices for reducing cyber risks to critical infrastructure. This provides a formal methodology to implement security controls, create a holistic view, identify risk, and determine program maturity level.

Core

The ‘core’ of the framework is a set of cybersecurity activities and outcomes consisting of three parts: Functions, Categories, and Subcategories. The five high level functions: Identify, Protect, Detect, Respond, and Recover contain categories to meet cybersecurity objectives that cover governance, technical, and physical security with a focus on business outcomes. Subcategories provide detailed implementation tasks.

- **Identify** - Develop an organization wide understanding to manage cybersecurity risk to systems, people, assets, and data.

- **Protect** - Develop and implement appropriate safeguards to ensure delivery of services.
- **Detect** - Develop and implement appropriate activities to identify cybersecurity events in real time.
- **Respond** - Develop and implement response procedures to act on cybersecurity incidents.
- **Recover** - Develop and implement a strategy to maintain resilience and to restore services that were impaired due to a cybersecurity incident.

Centralized Management

Fitabase has a centralized cybersecurity management structure. The CISO is responsible for establishing and monitoring all security controls throughout Fitabase. The CEO serves are the CISO.

Program Management (PM)

Fitabase has developed its cybersecurity program by identifying the best practices to protect information systems based on the business model. The program consists of governance, technical, and physical controls to protect the confidentiality, integrity, and availability of information systems. Controls are a combination of policy, secure architecture, and operational practices using the defense in depth strategy to protect systems. The CISO is responsible for developing an organization-wide cybersecurity program plan that:

- Provides overview of the requirements for the program and a description of the program management and security controls in place; and plans for meeting those requirements.
- Identifies the assignment of roles, responsibilities, management commitment, and legal requirements.
- Is approved by Executive Management.

SECURITY CONTROLS

The security controls listed in the table are the primary controls also referred to the 'common controls' that must be implemented throughout the organization. Security controls must involve aspects of policy, processes, and technical implementations for operations.

ID	FAMILY	ID	FAMILY
AC	Access Control	**PE**	Physical and Environmental Protection
AT	Awareness and Training	**PL**	Planning
AU	Audit and Accountability	**PM**	Program Management
CA	Assessment, Authorization, and Monitoring	**PS**	Personnel Security
CM	Configuration Management	**PT**	PII Processing and Transparency
CP	Contingency Planning	**RA**	Risk Assessment
IA	Identification and Authentication	**SA**	System and Services Acquisition
IR	Incident Response	**SC**	System and Communications Protection
MA	Maintenance	**SI**	System and Information Integrity
MP	Media Protection	**SR**	Supply Chain Risk Management

Table 1 – NIST Security Control Families

ACCESS CONTROL (AC)

Information systems must regulate who or what can access resources whether physical or logical within the organization. Unauthorized access shall be mitigated by implementing the specifications provided in the Access Control Standard.

SECURITY AWARENESS TRAINING (AT)

Organizations face new threats consistently and attack methods vary due to industry. The workforce shall be formally trained about relevant threats, organizational policy, regulation, and incident response procedures through periodic reminders and annually security awareness training as specified in the Security Awareness Training Standard.

AUDIT LOGGING (AU)

Audit Logging is a necessary process to monitor information systems for anomalies, intrusion attempts, and indications of compromise. Logs also are necessary for organizational and law enforcement investigations. Logs shall be configured to record system events for all information systems as specified in the Anomalies and Events Standard.

CONFIGURATION MANAGEMENT (CM)

Information systems pose vulnerabilities when deployed in the environment with default configurations. Attackers look for default settings to exploit to gain unauthorized access to information resources. Systems shall be configured to reduce the attack surface for all information systems as specified in the Configuration Management Standard.

IDENTIFICATION AND AUTHENTICATION (IA)

To prevent the misuse of information systems whether malicious or accidental they must allow access only to unique and authorized users. This is especially important when dealing with sensitive data. Unique identifiers and authentication controls shall be configured for the workforce and all information systems as specified in the Access Control Standard.

INCIDENT RESPONSE (IR)

When responding to incidents whether its system health, an attack, or other incidents the approach must be organized and repeatable. Incidents must be handled in a timely manner to limit further damage. An incident response plan shall be developed and distributed for incident handling. This information can be found in the Incident Response Plan.

MAINTENANCE (MA)

Governing information system, data center, and office maintenance applies to all types of services to systems conducted internally or by vendors. Maintenance includes fire suppression systems, data centers, and peripherals such as scanners and printers. Information necessary for maintenance records include date and time, service description, etc. Information system, data center, and office maintenance shall be conducted annually if applicable.

MEDIA PROTECTION (MP)

Protecting proprietary information is a priority for Fitabase. These different types of information can be stored on removable media devices intentionally and unintentionally. Media protection controls shall be communicated to the workforce to prevent data loss and intrusion for all information systems in the Acceptable Use Policy.

Personnel Security (PS)

Establishing the business security requirements when hiring, terminating, and sanctioning workforce members is essential to protecting Fitabase's information systems. Personnel security controls shall be implemented to reduce disruption due to inadequate employee screening and processes as specified in the Personnel Security Standard.

Physical Security (PE)

Physical access controls are necessary for data center access, personal and organizational information systems. Access should only be allowed to workforce members and third parties approved by Fitabase. Physical security controls shall be implemented to protect information systems as specified in the Physical Security Standard.

Planning (PL)

Security plans are scoped the information systems logically separated (boundary) by firewalls. Information systems within logical boundaries should contain an overview of the security requirements along with the adequate controls required. Security plans describe the intended application of each selected control in the context of the system with a sufficient level of detail to correctly implement. All information systems shall be inventoried with a list of security controls required for those systems based on the criticality of the data that is transmitted, stored, or processed.

System and Information Integrity (SI)

Information systems must be updated, monitored, and tested to protect the integrity of the system. System information controls shall be implemented to protect the integrity of the data and information system as specified in the Continuous Monitoring Standard.

ID.GV-2 Roles and Responsibilities

The following cybersecurity program stakeholders have specific responsibilities based on the needs of Fitabase .

Executive Management has been assigned the following responsibilities:

- Designating the Chief Information Security Officer (CISO).
- Staying informed, supporting, and communicating the importance of the cybersecurity program to the organization.

The **Chief Information Security Officer (CISO)** has been assigned the following responsibilities:

- Ensuring the cybersecurity program is developed, documented, and implemented to provide adequate security for all information systems, networks, and data that support organizational objectives.
- Developing and maintaining cybersecurity policies, standards, procedures, and controls to address organizational requirements.
- Ensuring compliance with regulatory requirements.
- Protecting the cybersecurity program plan from unauthorized disclosure and modification.
- Ensuring protections have been implemented based on risk tolerance in regards with the potential of unauthorized access, use, disclosure, disruption, modification, or destruction of information collected, and maintained by or on behalf of Fitabase .
- Reviewing and updating the organization-wide cybersecurity program plan annually; to address organizational changes and problems identified during the organization's life cycle.
- Reporting on the effectiveness of the cybersecurity program.

ID.GV-3 LEGAL AND REGULATORY REQUIREMENTS

To improve cybersecurity programs the government mandates regulatory requirements that include best practices based on industry and data the organization manages. Fitabase manages fitness data that do not contain any health or personally identifiable information.

ID.GV-4 RISK MANAGEMENT

The cybersecurity program is a collection of governance, technical, and physical security controls to reduce risk. These controls are implemented by following a repeatable process to perform the following functions: 1) identify assets, 2) categorize assets, 3) implement controls, 4) assess controls, and 5) monitor controls throughout the system life cycle.

RISK ASSESSMENT (RA)

Information system risk must be identified during its operational lifecycle. Risks are identified by vulnerability scans, assessments, and third-party notifications. Risk assessments shall be conducted to identify the threats, vulnerabilities, and likelihood of exploitation for information systems as specified in the Risk Management Strategy.

SUPPLY CHAIN RISK MANAGEMENT (SR)

The dependence on products, systems, and services from vendors can increase the level of risk to the organization. Vulnerabilities that may increase security or privacy risks include lack of access controls, tampering, theft, insertion of malicious software and hardware, lack of communication, and poor procedures in the supply chain. Supply chain risk management controls shall be implemented to reduce the risk of third-party weaknesses as specified in the Supply Chain Risk Management Strategy.

SECURITY ASSESSMENT (CA)

Information system controls need to be assessed for efficiency throughout the organization's lifecycle. Assessments shall be conducted to determine the gaps in the administrative, technical, and physical security controls as specified in the Security Assessment Standard.

CONTINGENCY PLANNING (CP)

Information systems require redundancy should problems occur at primary sites to maintain minimal interruption. For this reason, information systems shall be architected to maintain redundancy to prevent service interruption as specified in the Contingency Planning Strategy.

DEFINITIONS

Centralized Management - in centralized information systems governing, the information resources and decisions regarding their acquisition and control are concentrated in one business unit that provides IT services to the entire organization.

Cybersecurity Framework - process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities.

Program Management - overview of the security requirements for an organization-wide cybersecurity program and describes the program management security controls and common security controls in place or planned for meeting those requirements.

Security Categorization – the process of determining the security category for information or an information system based on the business impact of threats.

Right to Modify

Fitabase reserves the right to modify this Cybersecurity Policy 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.