Cybersecurity in FRHC

FREEDOM
HOLDING CORP.

2024

Introduction

FRHC is building a technology ecosystem to provide a more productive and effective client experience. We believe we need to secure our clients' data and protect them from relevant threats—our core responsibility to provide a trusting relationship within our ecosystem. We use a risk-based approach for our initiatives and weave it into our technology development strategy.

General Organizational of Information Security Management in the Freedom Holding Corp. (further - Company):

01 The Company's information security management system (ISMS) is formed using a risk-based approach to ensure the continuity of business processes, as well as the confidentiality, integrity, and availability of information that we process.

02 In accordance with our Information Security Policy the Board of Directors approves strategic internal information security documentation.

03 The Chief Executive Officer (CEO) is responsible for organizing ISMS processes and ensuring the allocation of necessary resources.

04 The Chief Technology Officer (CTO) is responsible for delegates responsibilities for ISMS processes and organizes identification, assessment, and treatment of IT&IS risks. He is also overseeing our Information Security team, which consists of Centralized FRHC Information Security Team and our subsidiaries Information Security Teams.

05 The CTO and Chief Risk Officer (CRO) both periodically report to the Risk Committee of the board of directors including on cybersecurity initiatives, notable incidents, and cybersecurity risks.

Information Security Principles Used by the Company:

06 The company is guided by efficiency, proper level of motivation, risk-oriented approach, comprehensiveness, multi-level protection, compliance with legal requirements, corporate responsibility, minimization of powers, separation of duty, secure architecture, and awareness.

07 We continually evaluate our application and infrastructure environment, including penetration testing, to reduce security risks to an acceptable level.

Description of Information Security Risk Management:

08 Cybersecurity is a critical component of the risk management program, with the CTO leading cybersecurity risk management improvement initiatives as part of the FRHC Technology Strategy.

09 The company employs a variety of preventative and detective tools designed to monitor, block, and provide alerts regarding suspicious activity.

10 The overall cybersecurity risk management objective is to reduce frequency or minimize the impacts of threat events that could lead to penetration, disruption, or misuse of information systems.

11 Personnel responsible for risk management activities are made aware of their responsibilities, including when changes are made to the risk management process.

12 The type, maturity, and formalization of risk management process in our subsidiaries is informed by the level of anticipated threats and their impacts associated with each organization.

Description of Information Security Incident Management Processes:

13 The company maintains an IT and cybersecurity incident management process that provides a framework for responding to actual or potential cybersecurity incidents.

14 The cybersecurity incident management process facilitates coordination across multiple areas of the organization including our Board members and subsidiaries.

15 We have internal policies and procedures and commitments to notify interested parties about incidents related to their sensitive information.

16 Personnel responsible for incident response activities are made aware of their responsibilities, including when changes are made to the incident response process

17 The type, maturity, and formalization of incident management process in our subsidiaries is informed by the level of anticipated threats and their impacts associated with each organization. The process might include business recovery and business continuity procedures, data backup processes, and playbooks for response to specific common or high impact attack scenarios.

Description of the Company's Data Protection Principles:

The Information Security Policy was developed in accordance with the international standard ISO27001:2022 and the requirements of applicable legislation. We are consistently involving our data protection practices and implement leading data protection standards.

18

The scope of the policy includes all FRHC business processes, all information processed by FRHC, information systems and software, their support tools (equipment), including those located on the territory of other companies, as well as all users of information systems and FRHC personnel, any third parties which processing company`s information.

19

We collect, process and transfer data of our clients in compliance with the applicable regulatory requirements and within the constraints of stated purposes.

20

Our FRHC Technology Strategy also include data protection stream which consist of variety of initiatives, like inventory and categorization of data and especially personal data, standardization of data processing and protection processes, periodic analysis and audit of data protection controls, implementation data protection roles in our companies, correct data processing consents collection, ongoing monitoring and management of related to data protection risks in our companies as well as applicable third parties. All these initiatives are implemented considering human rights.

21