Information Security Policy

Document Log

Version	Date	Name	Changes
1.0	08.08.2023	Sergey Kapustinskiy	Initial Document
1.1	15.06.2024	Sergey Kapustinskiy	Added Information security objectives chapter

Table of Contents

- Table of Contents
- 1 Introduction
- 2 Regulatory Compliance
- 3 Scope of Compliance
- 4 Policy Applicability
- 5 Information Security Objectives
- 6 Roles and Responsibilities
    - 6.1 Head of IS Responsibilities
    - 6.2 IT Services Responsibilities
    - 6.3 Users Responsibilities
    - 6.4 Role Assignment

1 Introduction

This document set up Organization's information security requirements for all employees. Organization's management has committed to these policies to protect information utilized by Organization in attaining its business goals. All employees are required to adhere to the policies described within this document.

2 Regulatory Compliance

During normal course of compliance and reporting activities Organization will ensure that proper scoping of compliant PCI operations and reporting are in effect.

3 Scope of Compliance

This Information Security Policy applies to all "system components." System components are defined as any network component, server, or application that is included in or connected to the company's information environment. The company information environment is that part of the network that possesses company information. For example, the following types of systems would be in scope for compliance within any environment:

- Systems storing company information
- Systems processing company information
- Network devices transporting or directing company information traffic
- Devices that create media containing company information
- Support systems

4 Policy Applicability

All employees, contractors, vendors and third-parties that use, maintain or handle Organization information assets must follow this policy.

5 Information Security Objectives

Based on the requirements and issues set out in this document, the following major objectives are set for information security:

- Ensuring compliance with applicable information security regulations and expectations of interested parties;
- Ensuring cyber resilience and process continuity;
- Identifying information security risks and reducing them to an acceptable level.

6 Roles and Responsibilities

6.1 Head of IS Responsibilities

Head of Information Security is responsible for coordinating and overseeing Organization's compliance with policies and procedures regarding the confidentiality, integrity and security of its information assets.

Head of Information Security will work closely with the other Organization managers and staff involved in securing the company's information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed.

Successfully securing Organization information systems requires that Head of Information Security consistently adhere to a shared vision for security. Head of Information Security works as well with system managers, administrators and users to develop security policies, standards and procedures to help protect the assets of the Organization. Head of Information Security is dedicated to security planning, education and awareness.

Specific responsibilities of Head of Information Security include:

- Make high-level decisions pertaining to the information security policies and their content. Approve exceptions to these policies in advance on a case-by-case basis.
- On an annual basis, coordinate a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- At least annually review the Information Security policies and procedures to maintain adequacy in light of emergent business requirements or security threats.
- Make sure that third parties, with whom company information is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the company information which they process.
- Assure that connections to third parties are managed per PCI requirements via the relationship procedures
- Complete tasks as required by the periodic Operational Security Procedures.
- Disseminating Organization information security policies and acceptable use guidance, and other user policies to all relevant system users, including vendors, contractors and business partners.
- Ensure background checks are carried out on potential employees who will have access to systems, networks, or data, for example background, pre-employment, criminal, or reference checks.
- Working on disseminating security awareness information to system users.
- Working to administer sanctions and disciplinary action relative to violations of Information Security Policy.
- Create new information security policies and procedures when needs arise. Maintain and update existing information security policies and procedures. Review the policy on an annual basis and assist management with the approval process.
- Act as a central coordinating role for implementation of the Information Security Policies.
- Maintain and distribute incident response and escalation procedures.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Review logs daily. Follow up on any exceptions identified.
- Restrict and monitor access to sensitive areas. Ensure appropriate physical controls are in place where sensitive cardholder information is present.

6.2 IT Services Responsibilities

IT Services are the direct link between information security policies and the network, systems and data. IT Services responsibilities include:

- Applying Organization information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Assisting Head of Information Security with monitoring and controlling all access to Organization data.
- Maintain an up to date network diagram.
- Completing tasks as required by the Periodic Operational Security Procedures.

6.3 Users Responsibilities

Each user of Organization computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all Organization information system users:

- Understand what the consequences of their actions are with regard to computing security practices and act accordingly.
- Embrace the "Security is everyone's responsibility" philosophy to assist Organization in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Read and be aware at least annually with the Security Awareness and Acceptable Use Policies

6.4 Role Assignment

Organization uses role-based access control (RBAC) to restrict data resource access to unauthorized subjects. All personnel are assigned appropriate roles before they can exercise permissions and access data resources. Each role is connected to data resource access needs and a level of privilege.

Roles are based on individual personnel's job classification and function. All privileged user IDs are granted the least privilege necessary to perform job responsibilities. IT Services is responsible for assigning roles with corresponding level of privilege and provides documented approval for each role.