

General Information Security Policy V16.1

Business Process Management

Exported on 2025-09-30 18:31:34

Table of Contents

No table of contents entries found.

INFORMATION

		THE ENGLISH VERSION «SOFT CONSTRUCT» CJSC			
Document ID:					
Version:	16.1				
Process owner:	Information Security Department				
Document Classification:	Internal				
Effective Date:					
Applicable:	Company-Wide				
Version Control:					
Version No	Purpose/Change	Prepared by	Date Prepared	Approved by	Date Approved
16.1	Minor changes	Business Process Management		Ara Khachatryan / Chief Executive Officer	
16	Basic document	Business Process Management		Ara Khachatryan / Chief Executive Officer	01 Jul 2024

TABLE OF CONTENTS

- [Section 1: General provisions](#)
- [Section 2: Definitions](#)
- [Section 3: Policy description](#)
 - [Chapter 1: Company's Context and Information Security Management System \(ISMS\)](#)
 - [Chapter 2: The Company's ISMS Scope](#)
 - [Chapter 3: The Scope of ISO 27001 certification](#)
 - [Chapter 4: Information Security Objectives](#)
 - [Chapter 5: Connected companies](#)
 - [Chapter 6: Policy Review](#)

CONTENT**Section 1: General provisions**

The aim of the **General Information Security Policy** (hereinafter referred to as the Policy) is to define the purpose, direction, principles, and basic rules for information security management of the “SOFT CONSTRUCT” CJSC (hereinafter referred to as the Company).

The Information Security Department is responsible for ensuring this Policy.
The Policy and other supporting and related documentation of the Information Security Management System have been designed in accordance with the specification contained in ISO 27001:2022.

The Policy is applied to the entire Information Security Management System (ISMS).
Users of this document are all employees of the Company, as well as all external parties who have a role in the ISMS.

Information security preserves the availability, confidentiality, and integrity of physical and informational assets.

Section 2: Definitions

The following definitions and abbreviations are used in the Policy:

Availability	this means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and the Company must be able to detect and respond rapidly to incidents (such as viruses, hacker attacks other malware) that threaten the continued availability of assets, systems, and information. There must be appropriate business continuity plans.
Confidentiality	this involves ensuring that information is only accessible to those authorized to access it and therefore preventing both deliberate and accidental unauthorized access to the Company's information and its systems including its corporate network and website.
Information assets	the information assets include information printed or written on paper, transmitted by post or spoken in conversation, as well as information stored electronically on PCs, servers, web site(s), or any other digital media. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).
Integrity	this involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of either physical assets or electronic data. The Company must comply with all relevant data-related legislation in those jurisdictions within which it operates.
ISMS	the Information Security Management System, of which this policy and other supporting and related documentation is a part, and which has been designed in accordance with the specification contained in ISO27001:2022
Jira	a system for managing and controlling tasks and processes
Physical (assets)	the physical assets of the Company including but are not limited to computer hardware, data cabling, telephone systems.
Preserve	this means that management, all full time or part-time staff, subcontractors, consultants, and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Company's disciplinary policy.
Security breach	a security breach may result in an incident that will cause a breakdown in the availability, confidentiality, or integrity of the physical or electronic information assets of the Company.

Section 3: Policy description

Chapter 1: Company's Context and Information Security Management System (ISMS)

1.1 The Company's context includes those issues, which can influence the ISMS and the implementation of information security objectives.

1.2 The internal issues of The Company include but are not limited to

1.2.1 Governance, organization structure, roles, and accountabilities;

1.2.2 Standards, guidelines, policies, and procedures;

1.2.3 Information systems, information flows, and decision-making processes;

1.2.4 Relationship with, and perceptions and values of, internal stakeholders.

1.3 It is very important for the Company's ISMS to have a developed organizational structure and clearly defined job responsibilities of the Company's employees and management, in order to avoid incidents resulting from excessive rights.

1.4 The Company highly values the importance of employees' information security awareness, ensuring that the documented information security policies, procedures, and guides are always in place and available.

1.5 Social, political, legal, regulatory, technological, and competitive environments are external factors that have an influence on Company's information security.

1.6 The political situation in the country requires that the Company's Business Continuity Plan (BCP) consider the scenario of continuing the business operations even in a war situation.

1.7 According to the Law of the RA Ministry of Finance "Programs used to organize internet winning games in the territory of the Republic of Armenia should comply with the international and independent ISO/IEC standards of the 27,000 series."

1.8 The social factors and the strong competition in the industry, require that the Company meets the requirements of ISO 27001, gaining the confidence of its customers and partners.

1.9 External factors that also influence The Company's ISMS include the Company's interested parties:

1.9.1 Shareholders

1.9.2 Employees

1.9.3 Clients

1.9.4 Government agencies

1.9.5 Suppliers

1.9.6 Partners

1.10 All these parties expect the Company to practice secure information security governance.

1.11 The requirements of interested parties are documented in labor contracts, service-providing contracts, agreements, purchase specifications, and laws and regulations.

Chapter 2: The Company's ISMS Scope

2.1 The scope of the Company's ISMS applies to the processes of providing betting, bookmaking, online casino/online winning games services to its customers, and the development of programs for betting and gaming services. The ISMS scope covers the management of information and business activities that support these services.

2.2 The ISMS scope includes all Company's departments, staff, and assets that are part of these services. The physical boundary of the ISMS scope includes the Company operational address: RA, Yerevan, G. Hovsepyan 20 Street.

2.3 The ISMS scope doesn't include the premises of the Company's betting shops and the employees working there.

2.4 The scope certification is: Information Security Management System, related to developing, sales and servicing of on-line betting and gaming solutions.

Chapter 3: The Scope of ISO 27001 certification

3.1 The Board of directors and the management of Company which is engaged in Betting/Bookmaking, On-line Casino/Poker, and also other online Games with winning business, as well as the development of programs for online betting and gaming services, are committed to preserving the confidentiality, integrity, and availability of all the physical and not physical information assets throughout the Company in order to preserve its competitive edge, the profitability of the organization, legal, regulatory and contractual compliance, and commercial image and in order to detect and prevent information security risks. Information and information security requirements will continue to be aligned with organizational goals.

3.2 The Company's scope for ISO 27001 certification includes the information security of organizational legal, financial information, personal data of employees and clients, source code of the developed application and related information assets involved in the providing of Company's on-line betting and gaming services.

Chapter 4: Information Security Objectives

4.1 The overall objectives for the information security of the Company are the following:

- 4.1.1 ensure compliance with current laws, regulations, and guidelines.
- 4.1.2 ensure the confidentiality, integrity, and availability of the Company's information assets
- 4.1.3 ensure the disclosure and mitigation of information security risks
- 4.1.4 ensure the continuous improvement of the information security management system
- 4.1.5 establish controls for protecting the Company's information and information systems against any forms of harm and loss.
- 4.1.6 ensure that the Company is capable of continuing its activities even if major security incidents occur.
- 4.1.7 ensure the protection of personal data (privacy).
- 4.1.8 ensure the availability and reliability of the network infrastructure and the services supplied and operated by the Company
- 4.1.9 comply with methods from ISO/IEC 27001/ 2022.
- 4.1.10 ensure that external service providers comply with the Company's information security needs and requirements.

4.2 The Company's business continuity plan and risk management framework provide the context for identifying, assessing, evaluating, and controlling information-related risks through the establishment and maintenance of an ISMS. Risks will be evaluated through assessing threats and identifying vulnerabilities to critical information assets. The risk assessment, Statement of Applicability, and risk treatment plan identify how information-related risks are controlled. The security Manager is responsible for reducing the risk to an acceptable level. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

4.3 In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems, and information security incident reporting are fundamental to the Policy.

4.4 All employees of the Company and certain external parties identified in the ISMS are expected to comply with the Policy and with the ISMS. All staff will receive appropriate training on information security.

4.4.1 The ISMS is subject to continuous, systematic review and improvement.

4.5 The Company has established an information security committee, chaired by the CEO, and including the Information Security Manager and other executives. The main functions of the Information Security Committee are:

- 4.5.1 Support ISMS activities and the ISMS framework;
- 4.5.2 Periodically review the security policies;
- 4.5.3 Conduct information security effectiveness measurement at least once a year.

Chapter 5: Connected companies

5.1 There are three companies that are connected to Company:

- 5.1.1 Ucraft, (Connected to the management);
- 5.1.2 PascalGaming (Connected to the management);

5.2 The connected companies should follow information security policies, procedures, and guides.

5.3 The connected companies are required to inform Information Security Department about their employees' job terminations to have the employee's accesses revoked. They should create a task on the Information Security Department (ISP) through Jira. In the *Description of the task* the manager should submit the following information:

- 5.3.1 The employee's name/surname,
- 5.3.2 The employee's position,
- 5.3.3 Employee's last working day,
- 5.3.4 Employee's corporate mail address.

5.4 In the case of suspected information security incidents or events, employees must contact their company's Information Security Manager. The connected company's Information Security Manager should inform the Company's Information Security Manager about the incident within 48 hours via one of the following means:

Email: jsms@softconstruct.com

Jira: ISP

PandayoPlus: Information Security Channel

Chapter 6: Policy Review

6.1 The Policy will be reviewed one year from the effective date, unless the document owner submits any process changes prior to that date.