

General Information Security Policy V 1

INFORMATION

THE ENGLISH VERSION

Document ID:		IT Management Santora B.V
Version:	1.0	The Board of Directors
Process owner:	Compliance Department/IS	
Document Classification:	Internal	
Effective Date:		
Applicable:	Company-Wide	

TABLE OF CONTENTS

Contents

Section 1: General provisions	1
Section 2: Information Security	2
Chapter 1: Company's Context and Information Security Management System (ISMS).....	2
Chapter 2: The Company's ISMS Scope	2
Chapter 3: The scope of ISO 27001 certification.....	3
Chapter 4: Information Security Objectives.....	3
Chapter 5: Network Security	4
Chapter 6: Security Awareness	4
Chapter 7: Training and Responsibilities	4
Chapter 8: Document Review	5

CONTENT

Section 1: General provisions

The aim of this Policy is to define the purpose, direction, principles, and basic rules for information security management of Radon B.V. (hereafter the Company). This 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.

This policy and other supporting and related documentation of the Information Security Management System

have been designed in accordance with the specification contained in ISO 27001:2013.

Section 2: Information Security

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 is not limited to:

- Governance, organization structure, roles, and accountabilities
- Standards, Guidelines, Policies, and procedures
- Information systems, information flows, and decision-making processes
- Relationship with, and perceptions and values of, internal stakeholders

1.3 It is 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 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:

- Shareholders
- Employees
- Clients
- Government agencies
- Suppliers
- 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.

2.3 The ISMS scope doesn't include the premises of the Company's betting shops and the employees working there. The scope certification is the 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 applications, "Spring" and "FC Bank" programs, 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 information security of the Company are the following:

- Ensure compliance with current laws, regulations, and
- Ensure the confidentiality, integrity, and availability of the Company's information assets
- Ensure the disclosure and mitigation of information security risks
- Ensure the continuous improvement of the information security management system
- Establish controls for protecting the Company's information and information systems against any forms of harm and loss.
- Ensure that the Company is capable of continuing its activities even if major security incidents
- Ensure the protection of personal data (privacy).
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by the Company
- Comply with methods from ISO/IEC 27001/
- 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 this policy.

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

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

4.6 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:

- Support ISMS activities and the ISMS framework
- Periodically review the security
- Conduct information security effectiveness measurement at least once a year

4.7 This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

Chapter 5: Network Security

5.1 The network services of the company are protected by methods of firewalls, passwords, VPNs and proper encryption. To ensure proper protection when it comes to the network of the company, access control measures are taken place to minimize the amount of contact and overall minimize chances of incidents occurring in the network.

Chapter 6: Security Awareness

6.1 All employees of the company are given the training needed to ensure they are acknowledged and aware of how to be more aware of detecting suspicious files and how to protect the company's systems by using the anti-malware systems set up by the IT team. The purpose of these measurements is to protect the Company and its employees from computer viruses, spyware and any other type of malware.

6.2 The company has also taken adequate measures to limit the use of company information on personal devices. The company allows the use of having company information on personal devices such as mobile phones on a case-by-case basis and approval from the responsible key person should be obtained. Employees of the company are able to access the company's email account, contacts and calendar on their personal mobile phones once they obtain approval from the key person responsible.

Chapter 7: Training and Responsibilities

7.1 When first joining the company, the employee will be presented with an employment contract containing all the necessary details and measures that will be taken by both the company and what is to be expected by the employee. The employee will then be on a training period and be trained by the person responsible for the respective departments. Once this training period has finished, a review of the access rights needed for the

employee should be done and specific access controls based on the review will be given. If an existing employee chooses to switch departments, another review will be carried out, and the access rights of the employee will be changed accordingly.

Chapter 8: Document Review

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