INFORMATION SECURITY POLICY

POLICY PURPOSE:

The Company aims to provide Services in accordance with the applicable Legal and Regulatory framework and other contractual obligations, in a manner that protects information from intentional or unintentional theft, destruction, or use in violation of Laws and Regulations. The purpose of information security is to ensure the business continuity of the Company and to minimize the risks that threaten information, avoiding security incidents and reducing the impact these incidents may have. It was developed in accordance with the requirements of the ISO/IEC 27001:2022 standard

SCOPE OF APPLICATION:

The Security Policy is applied by all Company personnel involved in the execution of Services, as well as the equipment used and the facilities utilized by the Company in the context of executing the Services, including any additional terms of the relevant contracts

DISTRIBUTION TABLE:

DEPARTMENT or POSITION	NAME	DATE	SIGNATURE

CHANGES COMPARED TO PREVIOUS VERSION:

SUMMARY OF MODIFICATION	PAGE	PARAGRAPH	SIGNATURE

CREATED BY: DEFINE SOLUTIONS SA

APPROVED BY: MANAGEMENT

POLICY ANALYSIS

The goal of this policy is to protect the informational assets of the Company and its clients from all internal, external, intentional, or unintentional threats. The specific objectives of the Company regarding Information Security are:

- Information is protected from any unauthorized access
- Revenue streams and profitability of the company are protected
- Supply of goods and services to customers is ensured
- Confidentiality of Information is maintained
- Integrity of Information is maintained
- Availability of Information is maintained
- Compliance with legal and regulatory requirements is ensured

- Business Continuity Plans are developed, maintained, and tested
- Information Security training is provided to all personnel
- All actual or suspected security incidents are reported to the Information Security Management Officer (CISO) and fully investigated

To achieve the above objectives, specific Security Policies and Procedures have been developed and implemented, describing the Management's directions, the Implementation Method of the Policy or Procedure, and all related responsibilities of the personnel. Personnel and external partners (when required) are obliged to implement the Security Policies that fall within the scope of their activities

Management is committed to providing all necessary resources and means for the implementation of this and other Security Policies

For the documentation of the implementation of the Information Security Management System, the company completes the "Statement of Applicability" with the responsibility of the CISO

According to the company's service security framework, the strategic objectives of "PHAEA RESORTS." are defined as:

- Providing competitive services
- Effective leadership and governance to create a strong and sustainable corporate identity
- Achieving financial performance that ensures the continuous provision of quality services
- Harmonious balance between economic growth, positive social impact, and environmental protection
- Providing accurate and documented reports that ensure the correct strategic directions
- Building trust and consistency relationships with its customers

STAKEHOLDERS AND REQUIREMENTS

STAKEHOLDERS	**REQUIREMENTS**
CUSTOMERS	Ensuring the protection of their sensitive personal data in accordance with the requirements of Regulation EU 2016/679 (GDPR)

STAKEHOLDERS	REQUIREMENTS
SUPERVISORY AUTHORITIES	Compliance with legislation
BANKS	No leakage of information related to application login details
INSURANCE BODIES/PUBLIC INTEREST BODIES	Updated legal documents
DATA PROTECTION AUTHORITY (DPA)	Compliance with legislation
EMPLOYEES	No leakage of contracts with financial or personal details
SHAREHOLDERS/OWNERS	No leakage of financial data
PARTNERS/SUPPLIERS	No leakage of cooperation contracts or know-how

INFORMATION SECURITY MANAGEMENT SYSTEM SCOPE

The scope of the company's ISMS is: "Top Management and IT Support for Hotel Services" It concerns the following locations:

- Phaea Blue Hotel, Elounda, Lasithi
- Phaea Cretan Malia Hotel, Malia, Heraklion
- Village Heights Hotel, Hersonissos, Heraklion
- Koutouloufari Village Holiday Club, Koutouloufari, Heraklion
- Heraklion Offices, Heraklion, Crete
- Athens Offices, Athens

EXCLUSIONS FROM THE ISMS SCOPE

The paragraphs excluded from the specifications of Annex A of the ISO 27001:2022 standard and the reasons for their non-application are recorded in the Statement of Applicability

CHIEF INFORMATION SECURITY OFFICER (CISO)

Responsible for the regular review of the information security policy and for training employees on security issues is Mr. Matthaios Kopidakis

INFORMATION SECURITY POLICY

Information Security is a top priority for PHAEA to:

- Ensure the availability, integrity, and confidentiality of data generated, received, and distributed
- Ensure the company's compliance with relevant legal and regulatory requirements
- Protect the interests of the company and its partners, who rely on it for the secure use and distribution of their confidential data
- Maximize the reliability of business information resources

To achieve these goals, PHAEA has implemented an Information Security Management System in accordance with the ISO/IEC 27001:2022 standard

The implementation of the system aims to:

- Protect stored files, computing resources, and information distributed through business services from any threat, whether internal or external, intentional or unintentional
- Systematically assess and evaluate the risks associated with information, ensuring timely and proper risk management
- Ensure secure data storage, virus prevention, handling internal and external threats, enforcing access control to systems, and managing information security incidents and unforeseen events
- Continuously inform management and personnel on Information Security and Data Protection issues

The Information Security Officer is responsible for overseeing and monitoring the system's operation and informing all relevant personnel about the Information Security Policy

All personnel involved in activities and processes related to Information Security are responsible for complying with the system's Policies and Procedures

Management is committed to achieving the company's goals, complying with Information Security principles, and continuously improving the Information Security Management System by providing the necessary resources

COMMUNICATION PLAN

Objective: To ensure that company employees have access to all the information they need and know the extent of the information they can communicate within and outside the company

WITH WHOM AND BY WHOM	COMMUNICATION METHOD	WHEN	TYPE OF INFORMATION
MANAGEMENT - EMPLOYEES	Mail, Physical document	Anytime and at every system update	Information Security Objectives, Company Policies, Company Procedures
CISO - MANAGEMENT	Mail, Physical document	Anytime and at every system update	Information Security Issues
CISO - EMPLOYEES	Mail, Physical document	Anytime and at every system update	Security Policies
AUTHORITIES (POLICE, FIRE DEPARTMENT, CYBER CRIME UNIT) - MANAGEMENT	Phone, Mail, Physical document	Anytime	Information Security Incidents
CERTIFICATION BODIES - CISO, ACCOUNTING (FINANCIAL MATTERS ONLY)	Phone, Mail, Courier	Anytime	Contracts, Payment Proofs, Company Policies, Company Procedures
SUPPLIERS - ACCOUNTING	Phone, Mail, Physical document, Courier	Anytime	Cooperation Contracts
SPECIAL STAKEHOLDERS (e.g., Information security forums) - CISO - IT MANAGER	Phone, Mail, Physical document	Anytime	Information Security Incidents, Information Security Issues 1

RESPONSIBILITIES

Management Responsibilities

The main responsibilities of Management regarding Information Security management in the Company are:

- Formulating the Company's policy on Information Security
- Approving and reviewing Information Security Policies, Procedures, and Work Instructions
- Approving Risk Management Plans and Emergency Management Plans (Business Continuity)
- Ensuring the resources required for the effective implementation of the Information Security Management System
- Creating the necessary conditions in the company to promote understanding and awareness among personnel of their roles and responsibilities related to Information Security
- Ensuring the continuous improvement of the Information Security Management System
- Making decisions on imposing sanctions in cases of disciplinary offenses related to Information Security

Information Security Management Officer Responsibilities

The Chief Information Security Officer (CISO), appointed by Management, is the representative of Management on Information Security issues and, in addition to other duties, has the following responsibilities:

- Collaborating with Management to develop Security Policies, procedures, and standard methods, in accordance with the Company's General Security Policy
- Ensuring the implementation, maintenance, and monitoring of Security Policies to ensure compliance with legal and regulatory requirements, current legislation, and standard requirements
- Informing Management about the performance and improvement of Security Policies
- Updating the company's information asset list and classifying their importance, in collaboration with relevant business executives
- Coordinating the Information Security Management Team to identify and assess risks threatening the Company's information assets, in collaboration with relevant business executives
- Collaborating with Management and the Information Security Management Team to determine the necessary controls to address risks
- Monitoring and reporting to Management on any security incident and activating the corresponding plan and strategy to address and prevent its recurrence
- Monitoring the effectiveness of controls applied to address risks and reporting to Management

- Organizing and conducting Internal Audits to check the effectiveness of the System
- Communicating with external Bodies regarding Information Security Management
- Ensuring personnel training on Information Security Management and the importance of participation in the System's implementation
- Preparing and coordinating the ISMS review by Management

The CISO reports directly to Management on all matters related to Information Security and is authorized to act on its behalf on these issues

Information Security Management Team Responsibilities

The members of the Information Security Management Team are:

- Antonaki Danae
- Kopidakis Matthaios
- Manousos Bouloukakis
- Dasenakis Valantis
- Katsanevakis Aris

The main responsibilities of the Information Security Management Team are:

- Examining the Company's activities that fall within the ISMS scope and identifying the involved information assets and the risks threatening them
- Assessing and evaluating the identified risks
- Examining, proposing, and recording control measures to address risks
- Periodically reviewing the effectiveness of risk management plans
- Identifying emergency situations and coordinating actions for the preparation and approval of emergency plans
- Reviewing the effectiveness of emergency plans

Department Heads Responsibilities

The main responsibilities of the Company's Department Heads regarding Information Security management in the company are:

- Participating in identifying, assessing, and planning the management of risks related to the information assets managed by their Unit
- Supervising the compliance with Security Policies by their department's staff
- Actively participating in reviewing related security incidents to investigate their causes and design necessary corrective actions
- Identifying significant changes and trends that may affect Information Security practices in their area of responsibility and collaborating with the CISO and Management to adapt to new conditions

Personnel Responsibilities

The main responsibilities of personnel involved in the Information Security Management System regarding Information Security management in the Company are:

- Implementing Security Policies, related procedures, and work instructions that fall within the scope of their work
- Immediately reporting to the CISO any security incident they become aware of

POLICY ENFORCEMENT

Any employee who violates this Security Policy may be subject to disciplinary sanctions at the discretion of the Company's Management

RELATED PROCEDURES/POLICIES:

CODE	TITLE
ALL POLICIES AND PROCEDURES OF THE SYSTEM	

RELATED FILES:

DOCUMENT CODE	DOCUMENT TITLE	FORMAT	RESPONSIBLE FOR STORAGE	RETENTION TIME
EPA.01.01	STATEMENT OF APPLICABILITY	PRINTED/ELECTRONIC	CISO	INDEFINITE

VERSION: 1

DATE: 15/07/2024