INFORMATION SECURITY POLICY

Table of contents

INFORMATION SECURITY POLICY

1 Preface

The Information Security Policy is an elementary component of the Company Policy in PLANASA Group. It is an indispensable building block in the Group's management system and, as such, it is an important guideline for the implementation and continuous improvement of the Group's business processes in international competition.

This PLANASA Group information Security Policy aligns policy and best practices in its area of responsibility to the information security policy and best practices defined by the PLANASA Group Headquarters in Valtierra (Spain).

These business processes rely increasingly upon information and information systems. The security of information and information systems is more than the protection of the technical infrastructure but includes the management and control of our information flow. This requires all employees to be aware of the importance of information security as part of the business processes, the implementation of infrastructures, as well as the development and deployment of information systems.

This Policy serves as a basis for the development of the corresponding regulations for information security. Therefore, these are regulations for all employees to ensure a definite and clear understanding of the responsibilities related to information security and to guide them in the secure handling of the Group's information.

By means of this Information Security Policy, the PLANASA Board obligates management and staff to employ the regulations defined and actively support the continuous development of information security.

The PLANASA Board approves the regulations based upon this Information Security Policy. All instructions made in connection with the information security management are, therefore, binding for all departments and employees.

2 Goal

The Information Security Policy described in this document defines the basic goals, strategies and responsibilities for ensuring information security in the PLANASA Group.

This policy is intended to establish a common starting point and a framework to develop progressively the necessary procedures considering the specific needs in terms of information security.

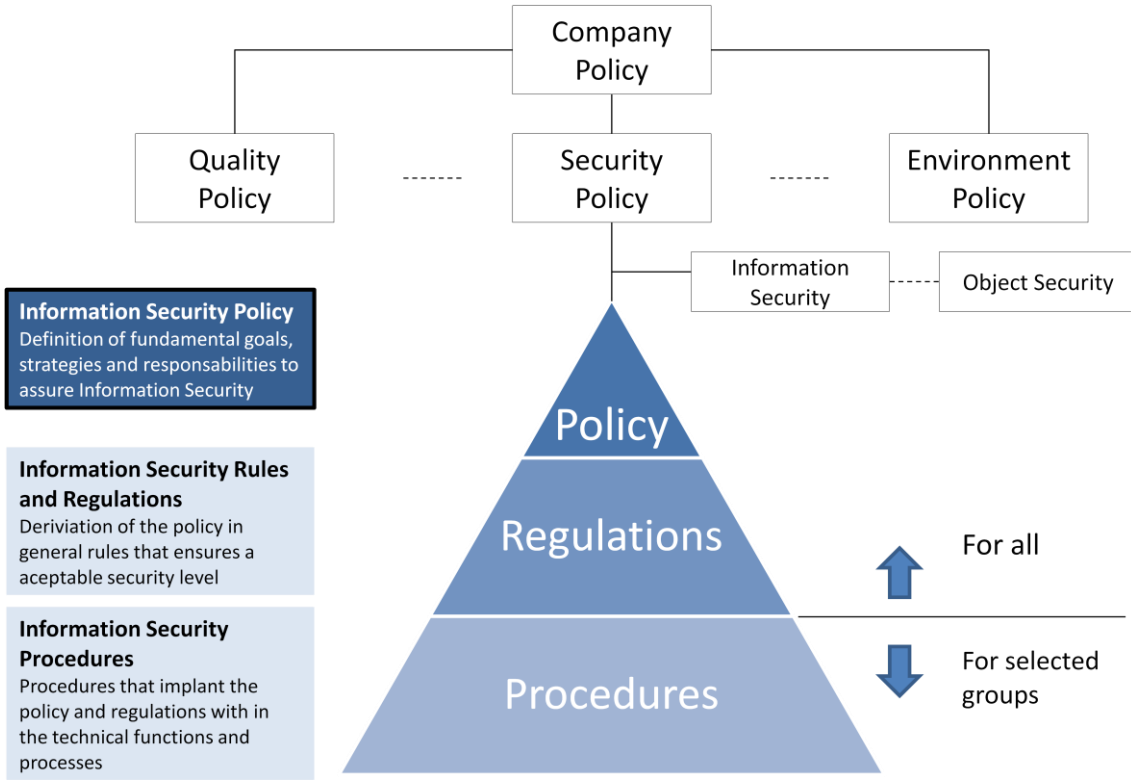
The specific needs of the Company may arise from factors such as organizational structure, business processes, information systems and, even, geographic location.

Information Security policy is based on standards and regulations and pursues to implement them in all PLANASA Group companies.

INFORMATION SECURITY POLICY

3 Context

The following overview shows how should be the integration of the Information Security Policy within the different Company Policies (To be model):



The information security regulations supplement the existing and relevant regulations (e.g. conditions of employment, Local Data Protection Act).

4 Scope

The Information Security Policy and all associated regulations applies to all the companies belonging to the PLANASA Group

5 Information Security in PLANASA Group

The success of the company is greatly influenced by the experience and “know how” of its employees. Uncontrolled data loss and manipulation of data, knowledge and information (subsequently referred to as “information”) can greatly threaten success.

Information and infrastructure that are put in place for the purpose of data processing and communication are valuable corporate assets that need protection. Therefore, all employees have

INFORMATION SECURITY POLICY

a personal obligation to protect information and communication resources against all forms of loss, forgery and abuse, and to handle the provided tools with the necessary care.

Compliance with the Information Security Policy is an important measure to ensure and benefit the Group's position in the market. The continuous implementation of the Information Security Policy in the business processes enhances a positive image in the market and ensures confidence in our products and services.

Understanding the potential of using modern information technologies is essential in order to increase competitiveness. This implies the need to implement measures to protect the confidentiality, integrity and availability of information during the planning, development and procurement of infrastructure and information systems, as well as during day-to-day operations.

The following principles are to be adhered to:

- **Confidentiality:** Information which is not specifically intended for public release is only to be made available for authorized individuals.
- **Integrity:** A fault free processing of information is to be assured, as well as the protection from unauthorized alteration.
- **Availability:** Information assets should be provided within an agreed time frame.
- **Accountability:** The access to information that is worth protecting and performing transactions must be non-deniable.

The following security measures are to be deployed to assure the above principles:

- **Authentication:** Unique identification upon access to information is to be assured.
- **Authorization:** The access to information is only to be granted to authorized individuals and is to be limited to the necessary scope, which is needed for working.
- **Auditing:** The access to information that is worth protecting is to be logged and controlled**.**

It is necessary to frequently review the information security requirements with regard to the changing requirements of the business. Methods and tools are to be used frequently for analysis and audits to recognize new risks and security requirements.

6 Responsibilities

Information security is greatly influenced by the responsible behavior of management and employees, as well as information systems operators.

The basis for the deployment of information security procedures and the compliance with information security principles lies in an adequate awareness about security of all internal and external employees. Therefore, corresponding information and training measures for users must be undertaken, to Planasa the IT security risks associated with the lack of knowledge or inappropriate usage.

PLANASA Board actively supports information security within all Group companies, by promoting actions with the aim of improving information security. In addition, the PLANASA Board is committed to:

INFORMATION SECURITY POLICY

- Provide a clear direction and visible support for information security initiatives.
- Encourage the implementation of information security measures.
- Provide the necessary resources to ensure the appropriate level of information security.
- Approve the designation of specific roles and responsibilities for information security across the Organization.
- Promote plans and programs relating to information security awareness.
- Ensure compliance with existing regulations in its area of responsibility.
- Appoint the Information Systems Department to lead the implementation of this Policy in the PLANASA Group.

PLANASA Group will have an **Information Security Committee**, led by the Information Systems Department, whose main objectives are:

- Develop and maintain the Information Security Regulation of PLANASA Group.
- Propose, promote and coordinate all projects, at Group level, regarding information security.
- Ensure compliance with policies and guidelines for information security in the definition of Security Management Plans and Disaster Recovery Plans for information systems.
- Lead and coordinate the development and implementation of the necessary operative procedures in matters of information security.
- Lead and coordinate the knowledge management in PLANASA Group, working together with corporate functions and experts in areas related to information security.
- Coordinate actions to improve security with the Responsible for compliance with local data protection act.
- This committee will be composed by the following members:
    - Head of IT (Chairman)
    - CFO
    - Members of IT department as required
    - CHRO
    - Head of Compliance

Any **internal or external person** (PLANASA Group staff or external staff) that makes use of information and information systems is required to use them with the care required and is subject to the Information Security Policy of PLANASA Group. Their main responsibilities are:

- Only use information systems to perform authorized tasks in compliance with laws and regulations.
- Protect information throughout its lifecycle from creation or receipt through processing, communication, transportation, storage, disclosure to third parties and its eventual destruction.
- Protect all forms of information, computerized or not, consistently with information security regulations.
- Protect information from unauthorized access, improper dissemination or loss.
- Be aware of legal and regulatory requirements existing in the Organization.
- Any breach of information security regulations must be properly reported when detected.

Approval

INFORMATION SECURITY POLICY

Prepared by:	Approved by:	Date of approval:
Global Head of IT	**Planasa Group Management Board**	**February, 2020**