INFORMATION SECURITY REGULATION

Table of contents

1 Introduction 3

1.1 Purpose 3

1.2 Scope 3

1.3 References 3

2 Definition of Information Security 3

3 Security Organization 4

3.1 Responsibilities 4

3.1.1 PLANASA Board 4

3.1.2 Information Security Committee 4

3.1.3 Information Security Director/Officer 5

3.1.4 Personal Data Protection Responsible 5

3.1.5 Process Owner 6

3.1.6 Users 6

3.2 Third Party Relationships 6

3.3 Audit of Information Security 8

4 Asset Classification and Management 8

4.1 Responsibilities for assets 8

4.2 Information Classification 9

5 Human Resources Security 10

6 Physical and Environmental Security 12

7 Communications and Operations Management 12

7.1 Operating procedures and responsibilities 13

7.2 Third-party service management 13

7.3 System Planning and Acceptance 13

7.4 Malicious Software 13

7.5 Internet Navigation and Electronic Messaging 13

7.6 Information Back-up 14

7.7 Network Security 14

7.8 Storage Media Management 14

7.9 Information Exchange 15

7.10 Traceability 15

8 Access Control 17

8.1 Access Management Procedures 17
8.2 User Access Management 17
8.3 Network Access Control 18
8.4 Privileged Access Rights 19
8.5 Access Control to Applications and Data 19
8.6 Mobile Computing and Tele-working 19
9 Systems Acquisition, Development and Maintenance 20
10 Incident Management 21
11 Business Continuity Management 21
12 Compliance 22
12.1 Compliance with External Requirements 22
12.2 Compliance with Internal Regulations 22

INFORMATION SECURITY REGULATION

1 Introduction

1.1 Purpose

This document has been prepared with the aim of establishing guidelines and general principles for initiating, implementing, maintaining and improving information security in PLANASA Group and, to this end, it includes the security measures applicable to corporate information and information systems.

These guidelines are intended to establish a common starting point in the framework of which, to the extent that it is applicable, procedures are progressively developed considering the specific needs in terms of information security.

Specific needs of the Organization may result from factors such as its organizational structure, business processes, information systems and, even, its geographic location.

These guidelines are based on international norms and standards of best practices for the management of information security.

This Regulation meets the principles in information security defined by the PLANASA Group Headquarters in Spain.

1.2 Scope

This document applies to all entities belonging to PLANASA Group.

The implementation of these guidelines will be made in a respectful manner with any other legal or internal requirements that could also be applicable to regulate aspects coincident with them.

These guidelines shall be known and respected by all employees and third parties who have access to PLANASA Group's information.

1.3 References

- PLANASA Group Information Security Policy
- ISO/IEC 27002:2005 Code of practice for the management of information security.
- COBIT® (Control Objectives for Information and Related Technology) by ISACA
- ITIL (Information Technology Infrastructure Library)
- Organic Law 15/1999 of Personal Data Protection.
- Royal Decree 1720/2007, which approves the regulation for implementing the Organic Law 15/1999.
- RGPD (Reglamento General de Protección de Datos). Reglamento (UE) 2016/679

2 Definition of Information Security

Information is a valuable and critical asset for PLANASA Group, without which the Organization could not develop its activity.

The information security is defined as the protection of the confidentiality, availability and integrity of information against a wide range of threats in order to ensure business continuity, minimize risks and maximize return on investment and opportunities.

For this reason, it is recognized the importance of security measures to ensure that the information will not be affected by internal and external threats, such as human errors, malicious actions (fraud, embezzlement, sabotage, privacy violations, etc.), technical errors, or force majeure events, such as natural disasters.

The signatories of this Regulation have the responsibility to develop, review and validate the security policies.

The adoption of these directives by PLANASA Group will minimize the potential risks to which the Organization is exposed in the development of its business activities.

3 Security Organization

3.1 Responsibilities

All responsibilities in information security will be clearly defined. People who have been assigned responsibilities may delegate some of its tasks but are still responsible for them to be executed properly.

Below are described the main responsibilities in terms of information security in PLANASA Group.

3.1.1 PLANASA Board

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:

- 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.

3.1.2 Information Security Committee

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.

The Information Security Committee will be composed by representatives from the following areas:

- Information Systems
- Human Resources
- Financials
- Compliance

3.1.3 Information Security Director/Officer

The role of the Information Security Officer will be assigned to the Head of IT.

Responsibilities of the Director of Information Security include the following:

- Define and implement controls in compliance with the Organization’s information security policies.
- Coordinate efforts to assess the adequacy of implemented controls, and to recommend additional measures based on the assessments.
- Propose refinements to assessment methodologies and processes (e.g., risk assessment) subject to management approval.
- Evaluate information security incident management data from across the organization, reporting these data to appropriate management, and recommending appropriate action based on the data.
- Identify significant threat and vulnerability changes, both internal and external, and recommending appropriate action.
- Provide consulting services for information security throughout the Organization.
- Monitor the level of information security through the established indicators and the performance of audits,

Information security officer could delegate part of his responsibilities in other individuals under his supervision.

3.1.4 Personal Data Protection Responsible

In the context of information security, the Personal Data Protection Responsible will define the obligations and legal requirements regarding data protection in order to comply with current legislation.

Additionally, the Personal Data Protection Responsible will be a member of the HR department.

3.1.5 Process Owner

A Process Owner is the role responsible for ensuring that a business process is fit for purpose.

The Process Owner's responsibilities include sponsorship, design, and continual improvement of the process and its metrics.

Responsibilities of a Process Owner, regarding information security, include the following:

- Assign an appropriate classification to information.
- Assign day-to-day administrative and operational responsibilities within the process.
- Determine the appropriate criteria for granting access to information and information systems (role definition) and approve system access requests.
- Ensure that users participating in the business process implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of information.
- Understand and approve how information is stored, processed and transmitted by the Organization.
- Define risk tolerance and accept or reject risk related to security threats that impact the confidentiality, integrity and availability of information.
- Define the business audit log strategy (identify the events to be audited, define the responsibilities and frequency for audit log reviews, determine retention periods for audit logs, trails, and audit reports, etc.).
- Understand how information is governed by Organization's policies and regulations, third-party contracts and legal requirements.
- Validate and approve any change that could have a significant impact in the business process.

3.1.6 Users

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.

3.2 Third Party Relationships

PLANASA Group will ensure, through the implementation of controls and the establishment of contractual clauses, that information security is maintained in those cases where there is access, communication or data processing by third parties.

To do this, risks related to information and information systems must be identified in business processes involving third parties, in order to implement appropriate controls before granting access.

In those cases where it is necessary to connect to third party sites, it will be required to perform a risk assessment process in advance, in order to identify the requirements for specific controls.

Requirements for confidentiality and non-disclosure agreements will also be included in third-party contracts, including the required actions when the agreement is terminated, such as the return or destruction of information.

Those responsible for hiring third parties shall ensure that agreements contain the information security requirements based on the type of company and the service provided, especially when the service involves access, processing, communication or management of information and information systems owned by PLANASA Group.

3.3 Audit of Information Security

An independent review of the information security management will be performed on a regular basis or when significant changes occur in the implementation of security. This review or audit may be internal or external, on condition that it is performed by a separate area independent than the area to be audited.

4 Asset Classification and Management

4.1 Responsibilities for assets

PLANASA Group will ensure the designation of responsibilities for the main assets of the Organization in order to ensure and maintain adequate protection over them.

Assets, for the purposes of this document, may be of different types, but they all, in one way or another, have value to the Organization and are involved in its business processes:

- Information assets: databases, files, contracts and agreements, operating procedures, archived information, etc.
- Software assets: applications, operating systems, etc.
- Physical assets: computer equipment, communication devices, auxiliary equipment, removable media, etc.
- Supplies: electricity, air conditioning, communication lines, etc.

All assets of the Organization will be clearly identified and inventoried and will be assigned to an owner. The owner will be responsible for ensuring that assets are properly classified in the inventory, reviewing this classification when changes occur, and ensuring that security controls identified by the Organization are met.

PLANASA Group will ensure that, in addition to identifying all important assets, their criticality is assessed, process in which the different business areas should participate.

PLANASA Group’s asset inventory will include all the information needed for disaster recovery, including type of asset, format, location, backup information, licenses, and its value from the point of view of business.

PLANASA Group will guarantee that rules are defined for an acceptable use of information and information systems, which will be documented and implemented.

Permitted uses shall be known by all users (employees, external partners and third parties) with access to PLANASA Group’s information. Some of the rules to be observed by users are the following:

- When a computer, mobile device or peripheral is assigned and delivered to a user, the responsibility rests with the user, and it cannot be exchanged with other users. The user responsible for a given equipment, will not allow anyone to use their equipment without supervision, except from the technical personnel who performs maintenance and support tasks.
- Any change in the initial configuration of the equipment may compromise the security of data, damage communications accesses and disrupt its proper functioning, so it is

forbidden to modify the initial configuration of the equipment. Also, computers and mobile devices should be regularly connected to the Organization's network, so they can be updated correctly.

- When computers, mobile devices or peripherals are provided on loan, a return date will be established that should be met. Equipment must be delivered back with all its components.
- Any theft or loss of a computer, mobile device, data storage unit, or paper documentation should be immediately reported.

4.2 Information Classification

PLANASA Group will hold an information classification document that allows, according to the information type, to establish the appropriate controls for the use and treatment of information. All information of the Organization will be labeled and protected according to this classification.

The following levels will be considered for information classification:

- Public
  - This type of information can be communicated without restrictions and is intended for general public use.
  - This data will not cause harm to any individual, group, or to the Organization if made public.
  - Requires basic protection from unauthorized tampering. This type of information can be freely disseminated to anyone.
- Internal-use-only
  - Information that does not need to be labeled as "Confidential" will be categorized as "Internal-Use-Only."
  - This information can be disclosed to any employee or third-party that maintains a relationship with the Organization, previously adhered to a not disclosure agreement.
  - Requires protection from unauthorized access or tampering.
- Confidential
  - This data will likely cause significant harm to an individual, group, or to the Organization if disclosed.
  - Requires the highest level of protection from any unauthorized access, disclosure or tampering, whether in hard copy or digital format.
  - Process Owners must closely manage the access and storage of confidential information.
  - Access to such information may only be granted to authorized individuals on a need to know basis.

Additional classification sublevels could be defined if deemed necessary, on condition that, at least, the previous three ones are considered.

All staff shall be familiar with the classification made and their associated security procedures.

If PLANASA Group's assets are deposited into third parties' facilities, they shall be treated with the security measures established by PLANASA Group.

If PLANASA Group personnel have access to third-parties information, it will be handled with the same security measures than the Organization's own confidential information.

Regarding personal data protection, PLANASA Group will be guided by what is stated in the local regulations and laws.

5 Human Resources Security

PLANASA Group will ensure that appropriate Human Resources controls exists to reduce the risk of theft, fraud or misuse of information by employees, contractors and third-party users.

For those users with a relevant role related to information security, the following aspects will be considered:

- Recruitment:
    - Pre-employment screening: Appropriate background verification checks will be performed (it includes, where appropriate, components such as identity verification, character references, CV verification, etc.).
- During the employment relationship
    - Terms and conditions of employment: a statement of rights and responsibilities will be signed by the user, including rights and responsibilities with respect to information security.
    - Information security awareness, education and training: Information security training and regular updates of organizational policies and procedures will be provided to the user.
    - Disciplinary process: There should be a formal disciplinary process for those who have committed a security breach.
- Termination:
    - Return of assets: All Organization's information and physical assets will be returned upon termination of the employment relationship or contract.
    - Removal of access rights: Access rights to information and information systems should be removed upon termination of the employment or contractual relationship.
    - Knowledge transfer: Appropriate mechanisms will be established to ensure that knowledge gained during the employment relationship will remain in the Organization after termination.

PLANASA Group will ensure that staff and third parties are aware of their responsibilities for information security. To that end, it will be necessary to develop norms that detail the responsibilities, duties and obligations of users in matters of information security.

These norms will regulate, at least:

- Permitted uses of information systems.
- The use of identifiers and passwords.
- Obligation of confidentiality.
- Compliance with legislation (regulations on personal data protection, intellectual property, etc.).

For specific profiles with greater responsibilities related to information security, their functions and duties will be adequately documented and formally communicated to people who are assigned to these roles.

PLANASA Group will ensure segregation of duties in critical processes, putting in place the appropriate measures to prevent that a single person could have full capacity to perform all tasks in this kind of processes.

Likewise, the Human Resources Management should establish mechanisms to:

- Communicate appropriately the information security rules and regulations to all affected personnel.
- Ask employees to sign confidentiality clauses when it is advisable and feasible.
- Remind employees regularly their responsibilities regarding information security.
- Educate employees on issues related to the protection of sensitive corporate information through training and awareness.
- Maintain limited access to files or locations where sensitive information is located.
- Avoid providing confidential information about the Organization during recruitment and selection processes.
- Take appropriate measures to prevent or limit the loss of information when an employee leaves the Organization, depending on the level of access to sensitive information they had (e.g. perform exit interviews and revoke access rights).
- Identify people who work with sensitive information, whether they are employees, consultants or other external partners, and to monitor, as a preventive measure, their access to information, with the level of detail and frequency that was determined appropriate according to the nature of the information.

Regarding personal data protection, the Human Resources Management should be guided by what is stated in the local regulations and laws.

6 Physical and Environmental Security

PLANASA Group will ensure that appropriate mechanisms are established to prevent unauthorized physical access and potential damage to facilities or equipment of the Company.

For each area (Data Centers, offices, etc.), the level of security required will be defined, and the appropriate controls will be implemented in order to meet, at least, the following aspects:

- Appropriate authorization for personnel who must be given access to restricted areas.
- The definition of security perimeters (such as physical barriers, card access controls, manned reception desk, etc.) to control access to facilities.
- The design and implementation of physical protection mechanisms against damage such as fire, floods, earthquakes, and other forms of natural or human-induced disasters.
- The control of loading and unloading zones and, if possible, to isolate these areas from information treatment resources to prevent unauthorized access.
- The use of appropriate intrusion detection systems, such as motion and perimeter alarms, audio and video surveillance.
- The existence of appropriate access controls to ensure that only authorized personnel are allowed access.
    - Recording of date/time of entry and exit of visitors, and/or video recording of activities in the entry/exit area, as appropriate.
    - All employees, contractors and visitors will wear their identification card, always, in a visible location.
- Areas with information processing resources will be specially protected.
    - Access rights to these facilities will be reviewed, updated and revoked when necessary.
    - It will be possible to obtain an audit trail of all accesses made to such facilities.

Regarding equipment security, the following controls will be considered:

- Equipment will be located and protected to reduce the risks of environmental threats, as well as the opportunities for unauthorized access.
- Equipment should be protected from power failures, telecommunications failures, and other disruptions caused by failures in supporting utilities.
- Power and communications transmission lines supporting information systems will be protected against interception or damage.
- Equipment will be properly maintained to ensure its availability and integrity.
- Appropriate security measures should be applied to off-site equipment,
- Equipment, information or software should not be taken off-premises without prior authorization and subject to appropriate restrictions
- Security controls will be applied for equipment in transit and in off-site premises, appropriate to the setting and the sensitivity of the information on or accessible by the device.
- All equipment containing storage media, and independent storage media devices, should be checked to ensure that sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

7 Communications and Operations Management

7.1 Operating procedures and responsibilities

Both operating procedures and good practices of PLANASA Group will be properly documented, updated and available to all users that require them to develop their functions. To this end, PLANASA Group will ensure that this documentation is reviewed periodically and is aligned with the latest versions of the guidelines in which it is based.

When applicable, segregation of duties and responsibilities will be implemented to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

7.2 Third-party service management

PLANASA Group will ensure that information security controls, service definitions and service level specifications are included in third-party service delivery agreements.

The Department responsible for a third-party service will ensure an effective communication of the PLANASA Group’s information security policies, regulations and procedures to third-party personnel, and will perform a continuous monitoring and review of third-party services to ensure that they meet the established requirements.

7.3 System Planning and Acceptance

PLANASA Group will ensure the monitoring of the use of information and information systems in order to identify and schedule future capacity requirements, considering current use, projected trends, and anticipated changes in business requirements.

Likewise, acceptance criteria for new information systems, upgrades, and new versions will be appropriately established, and suitable tests will be carried out during development and prior to acceptance.

7.4 Malicious Software

The malicious code such as viruses, worms, trojans, spyware, etc. are programs that can be created to carry out purposes as: collect sensitive information, take the control of a computer, damage or disable a computer, modify or delete data, etc.

PLANASA Group will ensure the implementation of controls for the detection, prevention and recovery from malicious software, as well as the establishment of procedures for staff awareness.

7.5 Internet Navigation and Electronic Messaging

PLANASA Group users may receive access to the Internet as well as electronic messaging. Electronic messaging includes email, instant messaging (IM), audio-video conferencing and any other one-to-one, one-to-many, or many-to-many personal communications.

PLANASA Group will ensure that information involved in internet navigation and electronic messaging will be appropriately protected.

Internet navigation and electronic messaging security measures and procedures will include, at least, the following aspects:

- Protection of messages from unauthorized access, modification or diversion.
- Correct addressing and routing.
- Reliability and availability of internet and messaging services.
- Limitations in the use of less-secure messaging systems (e.g. free/commercial email and IM).
- Stronger levels of authentication and message content protection when using public networks.
- Web-filtering tools to avoid access to objectionable content (pornography, gambling, hacking, cracking, etc.).
- Restrictions on the type of files exchanged to reduce the risk of virus infections and unreasonable use of systems (e.g. executable files, audio and video, etc.).
- Mass mailing, spam and identity fraud detection techniques.

7.6 Information Back-up

PLANASA Group will ensure that back-up copies of information and software are made, and tested at appropriate intervals, in accordance with an agreed-upon back-up policy. The aim will be to maintain the integrity and availability of information and information systems.

Back-up rules and procedures will include, at least, the following aspects:

- Formal definition of the level of backup required for each system (scope of data to be imaged, frequency of imaging, duration of retention, etc.) based on legal, contractual and business requirements.
- Complete documentation of restoration procedures for each system.
- Storage of the back-ups in a remote location in order to ensure recovery in case of disaster.
- Regular testing of back-up media and restoration procedures.

In this sense, it will be ensured, in all cases, compliance with the specifications of the local data protection act.

7.7 Network Security

PLANASA Group will ensure that the Organization’s networks are appropriately managed and controlled, in order to protect them from threats, and to maintain security for the systems and applications using the network, including information in transit.

Security features, service levels and management requirements for all network services will be identified in reasonable detail, and included in network services agreements, whether those services are provided in-house or outsourced

7.8 Storage Media Management

PLANASA Group will establish procedures for media management, to prevent unauthorized disclosure, modification, removal or destruction of information assets, or interruptions to business activities

In cases of removal or disposal of data storage media, it will be performed in a secure way to avoid information leakage to third parties.

Documentation for organizational data systems will be appropriately protected against unauthorized access, as it may contain sensitive information (descriptions of applications, processes, data structures, etc.).

To ensure confidentiality, PLANASA Group will ensure the implementation of encryption mechanisms to devices containing sensitive information in storage locations and during transport.

7.9 Information Exchange

PLANASA Group will ensure that appropriate control measures are developed and implemented to protect the exchange of information both within and outside the Organization, covering the use of all types of communications facilities and data storage media.

These control measures must meet the specific requirements of the local personal data protection act.

In case of exchange of information or software between the Organization and external parties, agreements will be established including, at least, the following aspects:

- Procedures to ensure appropriate identification and labeling, appropriate notifications to sender and recipient, traceability and non-repudiation.
- Minimum technical requirements for packaging and transmission.
- Specification of responsibilities and liabilities in the event of an information security incident.
- Any other type of security measures that are considered necessary according to the information type.

If information in send in physical storage media, appropriate security measures will be established to prevent unauthorized access, misuse or corruption while in transit. These controls will include:

- The reliability of carriers or courier services, which must be approved by the corresponding area.
- The identification of messengers who collect the devices.
- The use of containers designed to protect the contents from physical damage that may occur during transport.

If the information sent is sensitive, PLANASA Group will consider additional controls such as the use of closed containers, hand delivery, pack opening detection, data encryption, etc.

PLANASA Group will ensure the establishment and implementation of procedures to protect information associated with the interconnection of business information systems.

7.10 Traceability

PLANASA Group will evaluate what audit logs that record user and system activities, exceptions, and information security events should be produced, reviewed and kept for an agreed-upon time period, to assist in future investigations and access control monitoring.

Audit record keeping may have implications from the point of view of the protection of personal data and privacy of individuals. Therefore, prior to maintain audit logs, it will be considered the applicable law.

All information related to audit records will be appropriately protected against tampering and unauthorized access.

System administrators and system operators’ activities, as well as faults, will be appropriately logged, analyzed, and actions taken, as part of the general audit trail process.

The clocks of all relevant information processing systems should be appropriately synchronized with an agreed-upon time source, with the aim of protecting the accuracy of log information.

PLANASA Group will consider the audit trail requirements to meet the local personal data protection act.

8 Access Control

8.1 Access Management Procedures

PLANASA Group will ensure that access control procedures are established, documented and periodically reviewed, based on business needs and external requirements. Access management procedures and associated controls will consider the following aspects:

- Security requirements for information and information systems supporting business processes (according to the type of information, anticipated threats and vulnerabilities, confidentiality, integrity and availability requirements, etc.)
- Guidelines for determining access rights, such as the principle of least privilege (users have access only to information necessary for the performance of its functions) or information classification (confidential, internal use, etc.).
- Segregation of duties during access provisioning (e.g. access request, access authorization and access administration)
- Authorization flow to grant access (authorization must be approved by the direct responsible of the user, the head of the department, the role owner, etc.).
- Controls established for a timely removal of access rights.
- Relevant legislative and regulatory requirements (e.g. local personal data protection act).
- Consistency among such procedures across systems and networks.

8.2 User Access Management

PLANASA Group will ensure the definition of formal user registration and de-registration procedures for granting and revoking access to all information systems and services. The use and management of access privileges will be controlled and restrictive.

PLANASA Group will ensure the establishment of controls to review user’s access rights. These controls will include:

- Periodic review of user’s lists (e.g. every six months), specially for privileged roles (“super users”).
- More frequent review of privileged access rights (“super users”).
- Review of users after any status change (promotion, demotion, transfer, termination, etc.).

Identification and authentication mechanisms will be established to access to all systems through username and password.

All system users will have a unique identifier ("user-ID") for their personal use only. Shared user-IDs will be employed only in exceptional circumstances, where there is a clear justification, and under the authorization of the role owner. In these cases, additional controls must be activated to ensure the accountability of actions taken with these user-IDs.

Formal password management procedures will be established to guarantee confidentiality and robustness of passwords. These procedures will include secure methods for creating and distributing temporary and initial-use passwords.

Passwords will be changed periodically and will have to meet minimum security parameters that shall be familiar to users. In this sense, the password management system should:

- Ensure the quality of passwords, not allowing the creation of passwords that do not meet a minimum length of 8 characters (including letters, numbers and symbols).

- Enforce password change by the user, at least, after 90 days.
- Keep a history of 3 used passwords so that users can not repeat them.
- Store encrypted passwords.

Access to PLANASA Group's information systems will be protected by secure log-on procedures. A secure log-on procedure should:

- Not display help messages prior to successful log-on that could aid an unauthorized user.
- Not display of passwords as entered (e.g., hide with symbols such as asterisks).
- Not transmit passwords in clear text through the network.
- Limit the number of unsuccessful log-on attempts in total or for a given time period.

PLANASA Group will consider the possibility of lock out interactive sessions after a defined period of inactivity, attending to the criticality of the information accessed or the risks associated to the location of equipment. Resumption of the interactive session should require re-authentication.

For high-risk applications or remote communications, PLANASA Group will consider the possibility of establishing restrictions on connection times such as restricting overall connection duration or connection time period (e.g., normal office hours); restricting connection locations (e.g., to IP address ranges), or requiring user re-authentication at timed intervals.

All users of PLANASA Group's information systems (both employees and external personnel) should know:

- Their responsibilities for the custody, use and creation of passwords, with emphasis on the personal nature of passwords and the prohibition to share them.
- The actions to be taken when leaving their computer unattended, such as locking the session.
- The obligation to maintain a clean desk and clear screen policy, ensuring that any sensitive information is stored locked, documents are collected immediately from printers, and a diligent custody of the information accessed during their job's functions is maintained.

8.3 Network Access Control

Regarding the use of the network services, PLANASA Group will ensure that controls are established to assure that users only have access to the services for which they are specifically authorized. Likewise, to the extent possible, users' connection capabilities will be restricted to what is necessary to perform their functions.

In case of remote connections (external connections), risks will be assessed to determine the appropriate authentication method, considering the following aspects:

- Analysis of the option of identifying the computers on the network to authenticate connections from specific locations or equipment.
- Control and limitation of access (both physical and logical) to configuration ports and remote diagnostics. In those cases which are not strictly necessary for business activities, they will be disabled.
- Assessment of the appropriateness of segregating certain specific services or systems on the network, applying to each logical domain appropriate security measures in response to the risk.

- Assessment of the need for routing mechanisms to ensure that network connections between machines and information flows do not violate access policy.

8.4 Privileged Access Rights

PLANASA Group will ensure the implementation of controls to restrict operating system and database access to authorized users, by requiring authentication of authorized users in accordance with the defined access control policy. The use of special systems privileges will be recorded and monitored.

PLANASA Group will ensure that use of system utilities that can override system and application access controls is restricted, and appropriately monitored whenever used (e.g., by special event logging processes).

8.5 Access Control to Applications and Data

PLANASA Group systems will allow logical access controls consistent with the access control rules defined, so that users have restricted access according to these rules.

It will be assessed the need for isolating sensitive systems, i.e. to provide a computing environment especially dedicated to those systems that contain critical or sensitive information.

8.6 Mobile Computing and Tele-working

PLANASA Group will ensure the definition of guidelines and procedures that include controls to be established when working with mobile computing devices (laptops, tablets, etc.) that contain information of the Company. The following aspects will be considered:

- Physical protection of equipment (with emphasis of theft).
- Appropriate user authentication and access controls.
- Cryptographic methods for any stored sensitive data.
- Data backups for stored sensitive data.
- Anti-virus and other protective software.
- Security for network connections.
- Rules for the use of portable devices in public places.

In those cases where tele-work is permitted, PLANASA Group will ensure the definition of guidelines that contemplate, at least:

- Authorizations required for tele-work.
- Physical and environmental security measures of the environment in which tele-work will be performed.
- Proposed working environment: equipment to be used for the development of tele-work, support and maintenance of it.
- Security requirements of communications considering the criticality of the resources that will be accessed remotely.
- Use of domestic networks and requirements or restrictions as to wireless network configuration.
- Anti-virus protection and firewall requirements.
- Data backup processes and security measures for those backup copies.
- Security audit and review.

- Revocation of authorizations, access rights and return of equipment upon completion of tele-working activities.

9 Systems Acquisition, Development and Maintenance

Requests from PLANASA Group's business units for new information systems, or enhancements to existing information systems, will include the specification of the security requirements. The business unit that performs the request shall consider the criticality of the information processed by the system and the business process supported.

When acquiring or developing a system, to the extent that the criticality of the system requires it, the following aspects related to application process controls will be considered:

- Input data validations.
- Internal processing validations.
- Requirements of authenticity and integrity of inter-process messages.
- Output data validations.

Where deemed appropriate, according to the requirements of system security, cryptographic mechanisms will be implemented, always ensuring that the necessary controls are identified in terms of:

- Rules for the use of cryptography.
- Cryptographic key management.

PLANASA Group will ensure the implementation of appropriate controls during the acquisition, development and maintenance of systems to ensure the security of system files, such as:

- Separate environments for development, pre-production (if any), and production, to the degree practicable, to reduce risks of unauthorized access or disruptive changes to production systems
- Controls for installing software on production systems.
- Protection of test data, especially if it contains sensitive information or information subject to the legislation on personal data protection.
- Access control to software source code.

PLANASA Group will ensure that the implementation of changes in information systems is documented and controlled using formal change control procedures. To this end, it will be mandatory the establishment of mechanisms to ensure that:

- Formal procedures for change management exist, including specification, authorization, testing, user acceptance and managed implementation.
- Software package modifications are restricted as much as possible, limiting it to situations where there is a justified need.
- Outsourced software development is appropriately supervised and monitored by the Organization.
- Systems are reviewed and tested after implementation to ensure that there have been no adverse effects.
- Opportunities for information leakage are appropriately minimized or prevented.

In addition, PLANASA Group will ensure the establishment of procedures to maintain up to date information about published technical vulnerabilities, and to apply the appropriate countermeasures to address the risks posed by such vulnerabilities.

10 Incident Management

PLANASA Group will ensure the establishment of mechanisms for a timely communication and resolution of information security incidents, events and discovered weaknesses.

All PLANASA Group's information systems users (employees, contractors and third-party users) must report any observed or suspected information security incident through appropriate channels as quickly as possible.

Incident management responsibilities and procedures will be clearly established to ensure a quick, effective and orderly response to information security incidents.

PLANASA Group will ensure the establishment of mechanisms to quantify and monitor the type, volume and estimated cost of information security incidents.

Once the incident is completely solved, a closing procedure should be defined in order to gather all the lessons learned and launch improvement actions if needed.

In those cases where it is necessary to take a legal action against a person or Organization as a result of an information security event or incident, it will be necessary to consider the applicable legislation for the collection, processing and presentation of evidences before the competent authority.

11 Business Continuity Management

PLANASA Group will ensure the development and maintenance of business continuity plans and procedures covering critical processes of the Organization. These procedures will include information security requirements needed to maintain or restore operations and ensure availability of information at the required level and in the required time, following interruptions to or failures of business processes.

Business continuity procedures will provide the actions to take in case of failure of critical organizational processes. The assessment of business continuity should begin with the identification of events that can cause interruptions to business processes, together with the probability of occurrence, the impact of such interruptions and their consequences for information security.

Plans and actions to ensure business continuity will be based on business process analysis in order to identify which of them are critical and define a Restore Time Objective per process (RTO, how fast business processes have to be recovered in case of major disaster) and a Recovery Point Objective (RPO, the loss of information that the Organization can assume depending on the business impact)

PLANASA Group will ensure that, for information systems managed both internally and externally, Disaster Recovery Plans will be developed supporting business continuity plans and procedures.

If business continuity relies on vendors, PLANASA Group will include proper Service Level Agreements in order to ensure the RTO and RPO.

Business continuity plans and procedures will be tested and updated regularly to ensure that they are up to date and effective.

12 Compliance

12.1 Compliance with External Requirements

PLANASA Group will be responsible for defining, documenting and maintain updated all legal, regulatory and/or contractual requirements that are relevant to information systems, as well as the actions taken by the Organization to meet them.

To do this, specific controls and responsibilities will be established to fulfill the existing requirements.

Some relevant aspects to consider regarding compliance are:

- Compliance with the legislation on the use of material protected by intellectual property rights and the use of licensed software.
- Protection of important records of the Organization from loss, destruction or falsification.
- Compliance with local personal data protection act.
- In case of use of encryption mechanisms, it will be ensured that they meet all requirements established by current applicable legislation.

12.2 Compliance with Internal Regulations

PLANASA Group will ensure that information and information systems comply with current regulations regarding information security.

PLANASA Group will ensure that information security policies and regulations are effectively communicated to all persons affiliated with the Organization, including relevant external parties that handle data on the Organization's behalf.

Heads of the different business units shall ensure that information security procedures are carried out correctly in their area of responsibility, ensuring compliance with the rules and procedures regarding information security.

PLANASA Group's information systems will be reviewed periodically to verify compliance with the security measures and controls. Information system audits will be planned and executed minimizing the risk of disruption of business processes.

Access to audit tools will be protected to prevent any misuse or compromise.

Approval

INFORMATION SECURITY REGULATION

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