Security Policy of Information

Table of contents

Level:	Corporate	Created by:	Victor Pena
Owner:	IT Manager	Approve by:	German Serna
Affected plants:	Grupo Cosmos XXI and Societies	Date:	07/05/2021

Versions	Date	Modif.
1	20/01/2020	Created
2	07/05/2021	Modificated

Security Policy of Information

1. OBJET

Establish the objectives of the information security policy for Grupo Cosmos XXI and its societies.

2. OBJECTIVE

The Board of Directors approved at its meeting on 26 January 2021, following a favourable report by the Audit and Compliance Committee and on a proposal from the Information Security Committee(hereinafter also the**"ISC"),**this Information Security Policy (hereinafter, also the "Policy"),which sets out the principles and guidelines with which Grupo Cosmos XXI (hereinafter also the "**Group**" or **"Company")** will protect your information, in accordance with applicable regulations and its ethical values, defined in the Code of Conduct and Responsible Practices (hereinafter, the "**Code of Conduct**") as well as with the provisions of the Regulations of the Information SecurityCommittee (hereinafter, the "Regulation")and other applicable regulations.
Grupo Cosmos XXI will ensure the protection of information, regardless of how it communicates, shares, screens or stores (hereinafter, the**"Information").** This protection affects both existing information within the Group and information shared with third parties.
In this sense, Information Security means the safeguarding and protection of (i) the Information owned by Grupo Cosmos XXI, regardless of whether it is in its own systems or third parties; and (ii) information owned by third parties, which is in The Cosmos Grupo Cosmos XXI systems.
For the purposes of this Policy, Information Systems means all technologies or technological means, own or third parties that manage, store or transmit Information (including cloud technologies or the like).

3. REACH

This Policy shall apply to the Company and its Group of companies and shall bind all its staff, regardless of the position and role it performs.
For this purpose, Group means companies in which Grupo Cosmos XXI S.L is involved in the shareholding or management of them both vertically and horizontally.
The application of the Policy may be extended, in whole or in part, to any other natural and/or legal person linked to the Group for a relationship other than that of employment where this is possible because of the nature of the relationship and is suitable for the fulfilment of the purpose of that relationship.
In accordance with the Policy, Grupo Cosmos XXI may develop procedures and instructions to implement and comply with the obligations assumed, as well as to adapt it to the various local laws applicable to the Group.
In addition, the application of this Policy is complementary to other internal mandatory rules, such as the Compliance Policy on the Protection of Personal Data and Privacy, and those that regulate issues related to the Company's information.

4. GENERAL PRINCIPLES

The achievement of the objectives described in paragraph 3 is articulated by the following general principles:

- Classification of Information. The Information will be classified according to its value, importance and criticality to the business, so that the protection measures are adapted to the classification level of each information asset. Similarly, the classification of Information assets will be carried out taking into account the legal, operational requirements and good practices and standards in this regard.

-Use of Information Systems. The use of the Systems shall be limited for lawful and exclusively professional purposes for the performance of work-related tasks. Consequently, these means and systems are not intended for personal use and may not be used for any unlawful purpose.

-Function segregation. Risk concentrations arising from the absence of segregation of functions and the one-person reliance on business-critical functions should be avoided.

In this regard, formal procedures should be established to control the assignment of privileges to Information Systems, so that users have access only to the resources and information necessary for the performance of their functions.

-Retention of Information. Periods of retention of Information by category shall be established, where necessary or appropriate, taking into account operational or regulatory compliance needs, as well as the corresponding procedures for the destruction of information.

-Access to Information by Third Parties. The procedures for monitoring the making available and access by third parties to Information relating to Grupo Cosmos XXI or any other third parties related to the Group will be developed.

-Information Security in Systems. Development and production environments will be maintained in Standalone Systems. Similarly, the development and maintenance of Information Systems should include the necessary controls and records to ensure the correct implementation of security specifications.

-Continuity. A continuity management process will be established to ensure the retrieval of Critical Information for the Group in the event of a disaster, reducing unavailability time to acceptable levels.

-Compliance. The Group's Information and Communications Systems must be permanently appropriate to the requirements of the legislation in force in all jurisdictions in which it operates, as well as to the internal development regulations that apply.

Responsibility for the protection of Information and the Systems that treat, store or transmit it extends to all organizational and functional levels of Grupo Cosmos XXI, each to the extent applicable, as follows:

5. EMPLOYEE RESPONSIBILITIES

- All employees of the Group must know, assume and comply with the Policy, as well as the internal regulations of security and use of the Systems in force, being obliged to maintain the professional secrecy and confidentiality of the Information handled in their working environment and must communicate, as a matter of urgency and according to established procedures, the possible incidents or security problems that are detected.
- Employees who contract third-party services involving their use or access to the Information should understand the risks arising from the outsourcing process and ensure effective management of the information.
- Employees' use of Digital Systems or Services, including expressly email and instant messaging services, will be limited for lawful and exclusively professional purposes for performing job-related tasks. Consequently, these means and systems are not intended for personal use and may not be used for any unlawful purpose.

5.1 Responsibilities in relation to suppliers and other third parties

- In addition to paragraph 5.1, contracts with third parties involving the use or access of third parties to the Information, including those for the provision of outsourcing services or contracts, shall include specific security requirements relating to the technology and activities of those performing such services.

• In this regard, they shall include provisions ensuring that suppliers, subcontracted personal or any third-party company that uses or accesses, potentially or in real, the Information (through the Systems or any other means, as set out in paragraph 1), must know and comply with the Policy as far as apply to them, being obliged to maintain the professional secrecy and confidentiality of the Information handled in their relationship with the Group.

5.2 Department of Information Security

The Information Security Department will exercise its control function independently and it is its responsibility to implement this Policy and monitor its compliance, as well as that of all requirements arising from applicable laws, rules and good information security practices. Therefore, it is responsible for:

- Implement an Information Security Strategy that ensures compliance with the basic principles of this Policy, and in particular that addresses the following aspects:
    - adequate access to the Information, based on the principle of minimum privilege and the approval of the owner of the Information asset;
    - adequate segregation of roles and roles in Information Systems; or a correct configuration, management and operation of the infrastructure, services and/or software used in the various *business* processes both inside and outside the Group's premises, from a security point of view;
    - successful implementation of security requirements throughout the life cycle of information systems that support the Company's processes.
    - adequate protection of the Systems and Information they face from physical or environmental threats, in view of their criticality, that allows to identify, evaluate, prevent and respond to any risk that may compromise their security.
- Establish and review appropriate controls to ensure compliance with this Policy and its development regulations, including the organizational and technological mechanisms necessary to facilitate continuous monitoring of access and use activities of the Systems, services or Information managed by the Group.
- Prevent, detect and respond to any Information Security incidents and act in accordance with the "Information Security Procedure: Grupo Cosmos XXI Incident Response Plan".
- Promote the normative development of this Policy, through the procedures or instructions necessary to define a global framework for information security action in all its areas. You must also review, update and communicate any changes arising from variations in this Policy.
- Conduct training and awareness-raising activities on Information Security processes.
- Establish a continuous improvement approach.
- Ensuring compliance with existing legislation in the field of competences con assigned to it by this Policy.

5.3 Information Security Comittee

Grupo Cosmos XXI has an Information Security Committee composed of members of the Directorate that, in compliance with the Regulations, aims to ensure that good practices on security management are applied effectively and consistently throughout the Group.
Among other functions, he assumes responsibility for overseeing information security strategy, including spending plans, investment and security resources, and coordinating the security needs of management, business, and geographies.

It shall also report through the Department of Information Security, at least annually, to the Executive Chairman and the relevant Grupo Cosmos XXI Governing Bodies on the state of security, the evolution of threats and risk appetite, the allocation of security resources and significant incidents.

6. IMPLEMENTATION & FUTURE PROJECTS

Grupo Cosmos XXI is committed to allocating specific resources to ensure the effective implementation of the Policy.
Grupo Cosmos XXI is committed to considering information security requirements for future projects with the pretension of the guaranteed the security and compliance with information systems.

7. CONTROL AND AUDIT

Grupo Cosmos XXI expressly reserves the right to take, proportionately, the monitoring and control measures necessary to verify the correct use of the Systems it makes available to its employees, including the content of communications and devices, respecting, in any case, the current legislation and guaranteed the dignity of the employee. The communication and acceptance of this Policy will be validated previously notification to the worker.

The Group will undergo regular reviews and controls, as well as internal and external audits to assess the overall compliance with this Policy.

The assessment of a possible breach of this Policy shall be determined in the relevant procedure, in accordance with the provisions in force, without prejudice to legal responsibilities, including of a sanctioning nature in the field of employment, which, where appropriate, may be enforceable to the non-compliance.

8. POLICY COMMUNICATION

This Policy will be available on the Intranet of Grupo Cosmos XXI (Sharepoint Online) for all employees and will be available to all Company stakeholders on the corporate website (www.gcosmos.com). The Policy will also be the subject of appropriate communication, training and awareness-raising actions for its timely understanding and implementation.

9. POLICY UPDATE

The Policy will be revised and updated where appropriate, in order to adapt it to changes that may arise in the business model or in the context where the Group operates, guaranteeing at all times its effective implementation.

Legal Rep. Committee of Direction

ISC (Legal Rep. Information Security Committee)

Signature

Signature