1. PURPOSE AND SCOPE

The purpose of this policy is to establish a corporate framework within the scope of Information Security and Cybersecurity, which governs the categorization and proper handling of information within Grupo UNACEM with a systematic and structured approach that seeks to protect the integrity, confidentiality and availability of Information Assets.

This policy applies to Grupo UNACEM, which is comprised of UNACEM CORP S.A.A.A. (hereinafter, the "Company"), its Subsidiaries (hereinafter, "Business Unit"), and its directors, managers and other employees (hereinafter, "employees").

This document governs all information generated, processed, stored or transmitted by Grupo UNACEM, as well as the infrastructure used for such purposes, regardless of its format (electronic or physical). This includes data in transit or at rest within the business units.

The effectiveness and constant execution of this policy is crucial to minimize the risk of information loss, reputational damage, and to guarantee the competitiveness and operational efficiency of Grupo UNACEM. The classification approach allows assigning appropriate levels of protection and stipulating specific controls for different types of information, based on its value, legal requirements and sensitivity. Appropriate management of the treatment of information supports informed decision-making, ensures transparency and strengthens the trust of our stakeholders.

2. POLICY.

Grupo UNACEM establishes guidelines to protect and properly manage data according to their level of sensitivity: public, internal and confidential / critical. It defines responsibilities in the classification, security controls, audits and measures for secure storage, access, transfer and disposal of information. In addition, it includes incident response protocols and an ongoing training program to raise employee awareness of information security.

3. GUIDELINES

The following are the guidelines to be implemented by the Business Units, in accordance with the roles and responsibilities described in Chapter 4.

3.1. Information Classification

Grupo UNACEM defines the following structure to systematically classify information, ensuring that it is managed in a way that preserves confidentiality, integrity and availability in accordance with corporate policies and applicable regulations.

Table N° 01: Information Classification

Classification	Description	Examples
Public	This category includes information that is accessible by any person without representing a risk for Grupo UNACEM. Its disclosure is intentional and may be part of the Group's normal operations or legal requirements. The protection of public information focuses on guaranteeing its integrity and availability.	Annual reports, significant events, press releases, corporate website content, institutional brochures.
Internal	Internal information is restricted to use within Group UNACEM and its unauthorized disclosure could have a negative impact. Information Security and Cybersecurity policies are designed to protect this information from unauthorized access. Internal information is non-public information.	Operating procedures, internal policies, agendas, project tracking reports, databases, accounting documentation, internal financial and non-financial reports and any other information that is not defined as public.
Confidential / Critical	Confidential / critical information is that Internal, whose unauthorized disclosure or improper handling could cause significant damage to Grupo UNACEM or interested parties. It includes personal, financial and customer data, and any other type of information that the Group has and that requires safeguarding with appropriate levels of security. Access is controlled and measures are taken to protect its integrity, confidentiality and availability.	Personal data of customers or employees, business strategies, critical operational assets, sensitive financial data.

3.2 Information Management and Protection

a) We promote that each employee knows and complies with his or her responsibilities in the correct classification of information according to the established criteria.

b) We develop detailed guidelines that indicate how to classify, declassify and eliminate information (Public, Internal, Confidential / Critical) according to retention and relevance deadlines.

c) We implement adequate security controls, such as labeling, data encryption, validation, authentication and access authorization, as well as constant monitoring, to protect the information according to the assigned classification level.

d) We conduct periodic audits and evaluations to verify compliance and update classification criteria according to their relevance and effectiveness.

e) We establish secure storage protocols according to the classification level, using controlled physical environments and encrypted data.

f) We implement an access control system based on the least privileged requirements, limiting access to authorized personnel only.

g) We define and apply secure methods for information transfer, including encryption and secure communications networks.

h) We provide validated methods for the secure destruction of Public, Internal and Confidential information.

i) We implement an incident response process to mitigate impacts and prevent recurrences, with timely notification.

j) We implement an ongoing training program to train employees in classification and secure information handling, using up-to-date educational materials.

k) We conduct periodic evaluations to measure the understanding and application of Information Security and Cybersecurity policies in the organization.

4. RESPONSIBLE FOR THE POLICY AND ITS REVIEW

The Corporate Director of Risk and Compliance is responsible for this Policy and ensures compliance with it.

The Corporate CISO, appointed by the person responsible for this Policy, is in charge of ensuring its implementation, leading the information security and cybersecurity strategy, supervising compliance with the established objectives and coordinating the definition and alignment of budgets and resources at corporate and local level.

The General Managers of the Business Units shall ensure compliance with this Policy, its guidelines and the information security and cybersecurity strategy. To this end, they shall designate and supervise the Local CISO responsible for its implementation, as well as ensure the availability of the necessary resources to achieve the objectives established in their Business Unit.

The Corporate CISO shall review and update this Policy when any significant change occurs in Grupo UNACEM's environment or at least every two years, submitting any changes to the corresponding levels of approval.

Local CISOs are responsible for the direct operation of information security and cybersecurity, and shall adapt, implement, maintain operations and deploy technology solutions in accordance with this policy in their respective Business Units, and escalate any necessary exceptions to the Corporate CISO & CDO in a timely manner.

Everyone in Grupo UNACEM has an independent responsibility to comply with the rules and guidelines set forth herein, as well as to seek guidance in case of any doubt or need to analyze whether an activity may violate the rules described in this policy.

5. REFERENCE DOCUMENTS

Code	Document
-	Code of Ethics and Conduct
-	ISO/IEC 27001
-	NIST Cybersecurity Framework version 2.0
-	Corporate Data Protection Guidelines

List the individuals who participated in the review and consensus of a process document.

Document Name	Corporate Policy on Information Classification and Management			Version
Prepared by	Luis Budge Corporate Cybersecurity Manager	Date of Elaboration	05/16/2025	1.0
Prepared by	Guillermo Cortijo Corporate Information Security and Cybersecurity Supervisor	Date of Elaboration	05/16/2025	1.0
Reviewed by	Fernando Dyer Corporate Director of Risk and Compliance	Revision Date	05/26/2025	1.0
Reviewed by	Pedro Lerner Corporate CEO	Revision Date	05/26/2025	1.0
Reviewed by	Risk and Compliance Committee	Revision Date	06/25/2025	1.0
Approved by	Board of Directors	Approval Date	06/25/2025	1.0

6. ANNEX - DEFINITIONS

- **Information Assets:** Any data, information or resources related to information that have value for the Group and therefore require protection.
- **Confidentiality:** The property of information to be accessible only to those authorized to access it.
- **Integrity:** Guarantee of the accuracy and completeness of the information and the methods of its processing.
- **Availability:** Characteristic of the information for being accessible and usable by an authorized user when required.
- **Business Continuity:** Ability to continue delivery of products or services at acceptable pre-established levels after a disruptive incident.
- **Risk Management:** Coordinated activities to direct and control an organization with respect to risk.
- **Information Users:** Any employee or individual handling data on behalf of the Group, responsible for adhering to policies and procedures for classifying and handling information.

- Corporate CISO (Chief Information Security Officer): The leadership figure in charge of information security strategy and overseeing its implementation at the corporate level.

- Local CISO (Chief Information Security Officer): Responsible for implementing and maintaining the corporately defined information security strategy in their respective business unit.

- Classification Levels: Categories assigned to information to determine the protection and management needs based on its sensitivity and value for Grupo UNACEM.

- Security Controls: Protective measures implemented to safeguard information and prevent unauthorized access, alteration or loss.

- Cryptography: Use of mathematical techniques to encrypt and decrypt data in order to protect the confidentiality and integrity of transmitted or stored information.

- Lowest Clearance: Security principles whereby users are granted the lowest level of clearance necessary to perform their tasks.

- Business Impact Analysis (BIA): Process aimed at identifying the operational and financial impacts resulting from the interruption of business activities and processes.