INFORMATION SECURITY POLICY

1. Purpose and Scope

ZUNIBAL fully acknowledges the implications of information security associated with its operations and its commitment to stakeholders. The primary purpose of this policy is to ensure the proper safeguarding of information assets and the continuity of the services provided by maintaining the capability to prevent, detect, respond to, and recover from potential security incidents. To this end, the organization adopts the necessary security measures to maintain an acceptable level of risk. It also recognizes the importance of monitoring service performance, analyzing identified vulnerabilities, and establishing effective responses to incidents.

It is ZUNIBAL's responsibility to ensure that security is integrated into all stages of the information systems life cycle from design to decommissioning including acquisition decisions and operational activities. Security requirements related to each phase are identified and considered during project planning and development.

This document applies to all ZUNIBAL personnel as well as all stakeholders.

2. Scope of Application

According to the Information Security Policy, security measures must be applied to all systems, services, and resources related to Information and Communication Technologies (ICT) used by ZUNIBAL to support its organizational processes and that affect the various associated information elements.

The entity's ICT resources are intended to support operations and essential management activities necessary for its functioning. These resources include central and departmental systems, workstations, computers, printers, output devices and peripherals, internal and external networks, communication services, and storage systems owned by ZUNIBAL.

This policy applies not only to internal staff but also to all persons, entities, institutions, units, and services both internal and external that use ICT resources and have access to the entity's information assets. This includes those who connect directly or indirectly to such resources, whether remotely or through external devices, and particularly covers services offered over the Internet. In this context, such individuals shall be considered users, in accordance with the terms established in this policy.

3. Information Security Principles

This policy, together with its corresponding regulations, is based on fundamental protection principles aimed at ensuring that the organization can achieve its goals through proper management of information systems. These core principles, which must be considered in all information security–related decisions, are described below:

3.1 Comprehensive Security Approach

Security is treated as a holistic process involving all human, material, organizational, and technological elements related to the system. Therefore, it is essential to ensure that all actors involved in the process are aware of the Information Security Policy and perform their responsibilities accordingly. Coordination among all participants applies to all initiatives and actions undertaken by ZUNIBAL.

3.2 Risk Management

Risk analysis and management play a key role in information security. It is essential to keep risk levels within acceptable limits through the ongoing implementation of appropriate and updated security measures. This ensures proportionality between the nature of the data and processing activities, the risks to which they are exposed, and the corresponding security measures.

3.3 Incident Prevention and Recovery

System security must encompass prevention, detection, and recovery to prevent threats from materializing or significantly impacting the data managed by information systems or the services provided. This is achieved through preventive measures including deterrence and exposure reduction detection measures complemented by effective responses to address security incidents, and recovery measures that restore services and information. The system ensures data preservation and service availability throughout the information life cycle.

3.4 Multiple Layers of Defense

The system must have a protection strategy based on multiple layers of security so that, if one layer fails due to an unavoidable incident, there is sufficient time for an appropriate response, reducing the likelihood of system compromise and minimizing the final impact. These defense layers include organizational, physical, and logical measures.

3.5 Periodic Review and Continuous Improvement

ZUNIBAL regularly reviews and updates implemented security measures to ensure they remain effective in light of the continuous evolution of risks and protection systems.

4. Leadership and Commitment

ZUNIBAL's Management demonstrates its leadership and commitment to the fundamental principles of information security through the implementation of the Information Security Management System (ISMS), assuming the following responsibilities:

- Establish and align the Information Security Policy and Information Security Regulations with the strategic direction of the organization.
- Ensure the availability of necessary resources for the effective operation of the ISMS.
- Communicate the importance of effective system management and compliance with established requirements at all organizational levels.
- Provide direction and support to those contributing to ISMS operation, fostering an information security culture.
- Collaborate with other relevant management areas to strengthen leadership within their areas of responsibility, ensuring the integration of information security across all processes.
- Ensure that the ISMS achieves its intended results in terms of information protection and service continuity.
- Promote continuous improvement in information security by supporting initiatives that enhance efficiency and effectiveness in security management.

5. Management Policy

ZUNIBAL's Management recognizes the need to ensure compliance with defined levels of confidentiality, integrity, and availability for its information assets. This is essential for carrying out the company's activities, achieving strategic objectives, and demonstrating its capacity for efficient service management.

To achieve these goals, the Information Security Management System (ISMS) has been developed and implemented, providing a robust framework for the secure management of the company's assets. Furthermore, this system serves as a guarantee of trust and satisfaction for all stakeholders by integrating a secure methodology for service delivery.

To reinforce its commitment—and given that information security aims to ensure operational continuity and mitigate risk by preventing and, if necessary, minimizing the impact of security incidents—ZUNIBAL establishes the following strategic information security objectives, aligned with the company's context and strategic direction:

- Promote an organizational culture in which information security is a core pillar embedded in all organizational management practices and processes.
- Protect the confidentiality, availability, and integrity of organizational data to support the business strategy and comply with applicable legal and contractual requirements.
- Conduct risk analysis and management focused on information security.
- Use security resources optimally to support business objectives.
- Efficiently and effectively leverage existing security knowledge and infrastructure.
- Safeguard ZUNIBAL's information resources and technology against internal and external threats, whether intentional or accidental.

- Establish monitoring and reporting processes to ensure compliance with information security objectives and appropriate incident response.
- Ensure the resilience of the organization and its information systems against climate change or natural disasters.

6. Security Organization

To meet these objectives throughout all phases of the information life cycle and to assign responsibilities appropriately, ZUNIBAL establishes a structure that promotes consistent application of the information security policy. This structure effectively adapts to frequent technological and organizational changes in the business environment.
Accordingly, ZUNIBAL establishes the following committee and roles related to the supervision and management of information security:

- Information Security Committee
- Security Officer
- Information Systems Officer
- ISMS Officer

7. Personal Data

ZUNIBAL processes personal data and maintains a Record of Processing Activities documenting these processes and identifying the responsible parties. Each of its information systems complies with the security levels required by applicable regulations, taking into account the nature and purpose of the personal data involved.

The security measures implemented under this Information Security Policy, as well as the risk assessments conducted to fulfill the obligations of the General Data Protection Regulation (GDPR), are effectively coordinated with the Security Officer and the Information Security Committee. This ensures that personal data protection is fully integrated into the ISMS framework and that applicable privacy regulations are met.

8. User Obligations

All members of ZUNIBAL are responsible for knowing and strictly complying with the Information Security Policy and the related Security Regulations derived from it. Management ensures that these policies reach all interested parties by providing the necessary means for their dissemination and understanding.

It is vital that all employees fully recognize the importance of preserving information system security. Each individual plays an essential role in maintaining and improving security within ZUNIBAL.

Consequently, a continuous awareness program is established for all members of the organization, with special emphasis on newly joined personnel. Individuals responsible for the use, administration, or operation of information and communication technology (ICT) systems receive specific training in secure system management, as required for their duties. This training is mandatory before assuming any responsibility, whether in their initial position or in case of a role change within the organization.

9. User Responsibilities in Case of Non-Compliance

The Information Security Committee is authorized to assess whether organizational personnel are failing to comply with the obligations established in this policy, as well as in related regulations and additional instructions.

If any non-compliance is identified, both preventive and corrective measures are implemented with the primary goal of preserving and protecting the organization's information systems and networks. These measures are applied without prejudice to possible disciplinary consequences.

Once a breach of the Information Security Policy is confirmed, the Committee follows established procedures to initiate the appropriate disciplinary actions. The procedures and sanctions applied comply with current legislation governing the disciplinary regime for organizational personnel.

10. Relations with Third Parties

When ZUNIBAL provides services to other entities or handles information originating from them, the responsible party for such relationships must inform them of the Information Security Policy, as well as any applicable rules and instructions to be shared. Communication and coordination channels are also established between the respective Information Security Officers to ensure effective collaboration on security matters. Procedures are implemented for responding to possible security incidents, allowing for a rapid and efficient reaction in case of events that may jeopardize information security.

When ZUNIBAL uses third-party services or shares information with them, contractual agreements are established requiring these third parties to comply with the security obligations and measures specified in the contracts. These third parties may implement their own operational procedures to ensure compliance with such obligations. Specific

procedures may also be established to prevent, detect, report, and resolve security incidents in collaboration with the third parties. The objective is to ensure that third-party personnel are adequately informed and trained in security matters, at least to the same level required by this policy.

In particular, third parties must comply with security measures based on auditable standards and may be subject to certified third-party audits verifying their compliance with these policies.

If a third party cannot comply with any aspect of this security policy, a report must be submitted by its Security Officer identifying the associated risks and mitigation measures. This report must be approved by ZUNIBAL before continuing the relationship or service in question.

Policy review 00 approved by the Board of Directors on November 14, 2025