Intercorp Financial Services

Public Excerpt of Cybersecurity and Information Security Policy

I. Introduction

As a holding company of financial, insurance and wealth management institutions in Peru and abroad, Intercorp Financial Services Inc. ("IFS" or the "Company") acknowledges the importance of safeguarding the information of its subsidiaries' employees, clients and third parties. IFS is fully committed to compliance by its subsidiaries with international standards and applicable local laws and regulations that ensure the best practices in cybersecurity and information security.

IFS and its subsidiaries have implemented a cyber resilience strategy designed to protect, identify, and respond to cybersecurity threats, as well as actions for the recovery of technology and operational processes to ensure business continuity in the event of a cybersecurity breach. This strategy includes the implementation of tools, procedures, and teams of cybersecurity experts operating under a management framework based on industry standards such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), ISO 27001, and PCI DSS. It also considers new industry trends, current regulations, and definitions established by IFS' subsidiaries.

This document summarizes IFS' guidelines in connection with its subsidiaries' cybersecurity and information security policies and systems. The provisions set forth below are applicable to all of IFS' management, subsidiaries and business units as well as any third-party handling information provided by IFS or any of its subsidiaries and/or their representatives.

II. Objectives of the Cybersecurity and Information Security Policy

1. **Confidentiality:** Information shall only be accessible to authorized individuals, entities or processes. This includes implementing measures to safeguard personal and proprietary information.

2. **Availability:** Ensuring timely and reliable access to, and use of, information.

3. **Integrity:** Ensuring authenticity and non-repudiation of information and preventing any unauthorized modification or destruction.

III. Banking Sector – Interbank

While the Cybersecurity Division of Interbank leads cybersecurity risk management, the function extends across the organization, involving other teams in business, technology, risk, and auditing divisions. Both the strategy and the cybersecurity risk management framework consider business strategy, cybersecurity-related regulations, risk appetite, and the global cybersecurity context. The cybersecurity risk management framework is designed to establish capabilities and responsibilities at different control layers, including:

- Teams, tools, and procedures for the identification, assessment, control, and mitigation of cybersecurity risks;
- A governance model that sets the cybersecurity management framework, and provides direction and information to top management for decision-making; and

- An independent audit model that supervises the cybersecurity management model definition and execution.

The Cybersecurity Division is responsible for defining methodologies, procedures, and tools for managing cybersecurity risks and for defining policies approved by Interbank's board of directors. Both Interbank's board of directors and the executive team seek to ensure adequate resource allocation (people, technology, and processes) for this purpose. They also promote the development of a culture around strong cybersecurity habits throughout the organization.

IV. Insurance Sector – Interseguro

Interseguro has a framework for comprehensive risk management, including cybersecurity risks. The framework establishes procedures for the identification, assessment, mitigation, and communication of cybersecurity risks. While the Information Security and Cybersecurity unit is responsible for providing methodological support for cybersecurity risk management and defining control policies and procedures, the function extends across business and support units, which are accountable for the risks.

Additionally, an audit layer has been established to independently assess the performance of the defined management framework. Interseguro's strategy focuses on the implementation of measures to prevent, detect, respond to and recover from cybersecurity threats in a global environment where the materialization of cybersecurity risks continues to increase. These measures have primarily centered around improving identity and access management controls, both in preventive aspects and monitoring activities. Additionally, the governance framework has been strengthened through the updating of information security policies and associated procedures, along with the reinforcement of vulnerability identification processes through red team exercises.

V. Wealth Management Sector – Inteligo Group

The subsidiaries of Inteligo Group: Inteligo Bank, Inteligo SAB, Inteligo Perú Holdings, and Interfondos, have a framework for comprehensive risk management, including cybersecurity risks. The framework establishes procedures for the identification, assessment, mitigation, and communication of cybersecurity risks. While the Information Security unit is responsible for providing methodological support for cybersecurity risk management and defining control policies and procedures, the function extends across business and support units, which are accountable for the risks. Additionally, an audit layer has been established to independently assess the performance of the defined management framework.

As a part of their cybersecurity strategy, the subsidiaries of Inteligo Group have strengthened its identification, protection, detection and action cybersecurity plans, which reduced the occurrence of attacks and mitigated the risk of cyber threats. This strategy is based on the cybersecurity framework of the National Institute of Standards and Technology (NIST), and other standards such as ISO 27000 and 27032. The cybersecurity strategy includes improvements to security on different fronts, including mobile devices, workstations, in the cloud and on premises. Inteligo uses updated technology such as behavior analysis and artificial intelligence, which allow its human resources to reduce time spent on threat detection and analysis.

VI. Commitments

1. Periodic Reviews

The board of directors of each of the subsidiaries of the Company is responsible for approving the policies and guidelines for implementing the cybersecurity and information security policy and ensuring its continuous improvement. Each subsidiary of the Company shall perform regular assessments to ensure the adequacy, sufficiency and effectiveness of the controls and systems.

2. Integrity and Data Protection

The subsidiaries of the Company shall undertake the obligation to maintain security standards that include, but are not limited to, human resource security, physical and logical access controls, operational security, communication security, and incident management.

3. Monitoring and Responding to Information Security Threats

The subsidiaries of the Company shall implement procedures for incident management, establishing methodologies for incident classification, maintenance of information security operations, identification of potential threats and vulnerabilities, implementing internal incident reporting mechanisms, identifying improvement measures following incidents, and preserving evidence to facilitate forensic investigations.

4. Individual Responsibilities

All personnel are responsible for safeguarding information, complying with internal policies and procedures, completing training and promptly reporting suspected incidents or potential vulnerabilities that could affect information security and cybersecurity. Clear individual responsibilities shall be established for employees, contractors, temporary staff, providers and third parties in general.

5. Third Parties

The subsidiaries of the Company shall ensure that contractual arrangements with third parties comply, as applicable, with regulatory requirements in connection with cybersecurity and information security, defining provider's responsibilities and ensuring the implementation of complementary measures when deemed necessary.