



INTERCORP FINANCIAL SERVICES INC.

---

## **CORPORATE COMPLIANCE POLICIES**

## **Table of Contents**

1. Introduction.....	1
2. Purpose.....	1
3. Legal framework.....	1
4. Scope .....	2
5. Responsibilities.....	2
4.1. Of the Board of Directors of IFS and Group Companies .....	2
4.2. Of the General Managers of IFS and Group Companies .....	2
4.3. Of the Corporate Compliance Officer (CCO)/Chief Compliance Officer (CCO) .....	3
4.4. Compliance Officer of the group subsidiary or subsidiaries: .....	3
4.5. Of the employees .....	3
6. General Guidelines .....	3
7. Policies.....	4
7.1. Money Laundering and Financing of Terrorism Risk Management .....	4
7.2. Foreign Account Tax Compliance Act – FATCA .....	9
7.3. Improper Use of Privileged Information .....	18
7.4. Anti-corruption.....	30
8. Monitoring.....	32
9. Internal and External Audit .....	33
10. Sanctions for non-compliances .....	33
11. Reports on non-compliances.....	33
12. Inquiries.....	33

## **Corporate Compliance Policies – IFS**

### **1. Introduction**

IFS has a firm commitment to promote and ensure the Compliance culture together with its subsidiaries, with the purpose of reaching the highest integrity and ethical conduct standards in its organizations.

### **2. Purpose**

These Corporate Compliance Policies have the purpose of establishing the general guidelines for the development of an entrepreneurial conduct according to the values and principles established by IFS.

Thus, based on the international Compliance standards, this document has been prepared, which includes the following:

- Money Laundering and Financing of Terrorism Risk Management.
- Foreign Account Tax Compliance Act – FATCA.
- Improper use of privileged information
- Anti-corruption Program

These policies are part of a Compliance Program, which has been prepared to:

- a. Disseminate the existing internal mechanisms to prevent, detect and report inappropriate activities with the purpose of making timely and efficient decisions.
- b. Guarantee the development of training and programs designed to educate the employees in the policies, procedures and standards adopted by our Corporation.
- c. Ensure that the timely and adequate corrective measures are taken to prevent the recurrence of inappropriate conducts.
- d. Implement mechanisms of evaluation of the effectiveness of the essential elements of the policy.

### **3. Legal framework**

This Manual has been prepared based on the applicable rules in force, established by bodies such as the Banking, Insurance and AFP Superintendence (*Superintendencia de Banca, Seguros y AFP - SBS*), Market and Securities Superintendence (*Superintendencia de Mercado y Valores - SMV*), the Financial Intelligence Unit (FIU), and the Internal Revenue Service. In addition, it is based on the rules of the countries where the companies of the group and subsidiaries are established, such as Panama and Bahamas, and any other country where any company is established.

#### **4. Scope**

These policies are applicable to the following companies of the group and subsidiaries, which are part of Intercorp Financial Services Inc. – IFS:

- Banco Internacional de Perú S.A.A. (“Interbank”) and its subsidiaries.
- Interseguro Compañía de Seguros de Vida S.A. (“Interseguro”) and its subsidiaries.
- Inteligo Group Corp. (“Inteligo”) and its subsidiaries.

The rule comprised in the policy contains minimum standards of mandatory compliance, therefore, when a local rule differs from the requirements established in these Corporate Compliance Policies, the strictest one shall be applied. In addition, if there is any conflict between the local rule and this policy, the group company and/or subsidiary of IFS impacted must consult with its compliance department and with the compliance department of the parent company, if applicable, to resolve the conflict.

If the Corporate Compliance Policies cannot be applied in a certain country, because they contravene a rule, custom, case law, legal principle or local doctrine, the group company and/or subsidiary of IFS must guarantee that it will refrain from beginning or continuing commercial relationships, and any type of transaction. If commercial relationships already exist in that country, the group company and/or subsidiary of IFS must establish an action plan to terminate them.

#### **5. Responsibilities**

##### **4.1. Of the Board of Directors of IFS and Group Companies**

- Approve and ensure the compliance of this policy.
- Ensure that the corporate compliance policies are aligned with the strategy of IFS or group company.
- Appoint a Corporate Compliance Officer (CCO)/Chief Compliance Officer (CCO), who will be ratified by the corresponding group companies (according to the rule applicable to each country).
- Ensure the Independence of the performance of the duty of Compliance Officer.

##### **4.2. Of the General Managers of IFS and Group Companies**

- Ensure that the guidelines contained in this document are established, implemented and maintained.
- Allocate the appropriate resources and organization for the adequate management and compliance of these policies.
- Appoint a responsible officer(s) in charge of compliance risk management.
- Promote the dissemination of the compliance culture inside IFS companies.

- 4.3. Of the Corporate Compliance Officer (CCO)/Chief Compliance Officer (CCO)
- Ensure the execution, compliance and continuous improvement of this corporate compliance policies.
  - Promote the compliance of the guidelines established in these corporate policies, by all employees.
  - Periodically inform the Board of Directors and the General Management about the operation of these policies.
  - Provide advice and guidance to the compliance officers of the group companies and their employees on the corporate policies and answer the inquiries that may be made regarding them.
  - Periodically review and update these policies.
  - Any other duty that could be relevant for the purpose of reducing the risk of eventual non-compliances of the contents of the corporate compliance policies, even understand and ensure the 'compliance with United States Securities Law and Regulations.'
- 4.4. Compliance Officer of the group subsidiary or subsidiaries:
- Define the scope of the compliance program in coordination with the CCO based on the corporate policies.
  - Coordinate with the CCO the establishment of a compliance system for the subsidiaries of IFS.
  - Take the necessary actions to surveil the compliance of the prevention system.
- 4.5. Of the employees
- Comply with the guidelines of these policies.
  - Adequately manage the risks they could be exposed to as part of their responsibilities
  - Report any non-compliance of this document to Compliance or through the channels established for this purpose.

## **6. General Guidelines**

Each group company and/or subsidiary must individually assess the main compliance risks to which they are exposed due to the nature of their industry. In that sense, this document defines the minimum scope that the compliance program must have:

- No activities of corruption of/to public and private officers, money laundering and financing of terrorism and the improper use of privileged information will be tolerated.
- All the policies included in this document must be implemented, reported and monitored.
- It must be guaranteed and looked after the compliance of the policies included in this document in all the jurisdictions where commercial activities are developed.

## **7. Policies**

### **7.1. Money Laundering and Financing of Terrorism Risk Management**

The objective is to manage the risks in order to prevent money laundering, financing of terrorism or other financial crimes by the subsidiaries of IFS, its customers, employees, suppliers and/or counterparties.

The rules applicable to the prevention of Money Laundering and Financing of Terrorism are:

- SBS Resolution N° 2660 – 2015
- Law 27693, law that creates the FIU
- Supreme Decree - Regulations of the law that creates the FIU
- CONASEV Resolution N° 0033-2011

#### **7.1.1. Responsibilities**

Of the Board of Directors of each group company

- Appoint a ML/FT compliance officer.
- Approve and ensure the compliance of this policy.
- Periodically establish and review the operation of the MLFT Risk Management System.
- Promote the dissemination of the compliance culture inside the organization.
- Take into account the ML/FT risks when establishing the strategic objectives.
- Ensure the Independence of the exercise of the role of Compliance Officer.

Of the Chief Compliance Officer (CCO)

- Develop, supervise and manage the MLFT prevention program at corporate level, disseminate it among the group companies and/or subsidiaries and periodically control its compliance. Said program must take into account the local regulations, including those of bank secrecy of each country.
- Coordinate the deployment of the annual work plan of the corporate MLFT prevention program.
- Ensure the strengthening of the compliance culture at IFS group level.
- Be the spokesperson between the Board of Directors of IFS and its subsidiaries, informing about important issues that may occur, according to the policies and guidelines established. For that purpose, a report that will have a minimum annual periodicity shall be issued.

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

- Be the spokesperson between the group companies and/or subsidiaries and the SBS, the SMV or other local regulators or equivalent ones, if applicable.
- Approve all the internal communications related to MLFT Risk management disseminated to the employees.
- Be the spokesperson in the sharing of information, establishing the adequate safeguards on the confidentiality and use of the information shared, when it is necessary to share customer information between the subsidiaries for MLFT Risk Management purposes.
- Consider and respect the laws of each country related to information sharing in the case of companies that are located in different countries. The procedures and policies developed by each company must be aligned with the Corporate Policies related to the sharing of customer information and be coordinated with the CCO.

Of the Corporate MLFT Compliance Officer and/or Compliance Officer

- Coordinate with the CCO the implementation and management of the MLFT Risk Management system for the company or companies he/she is in charge of.
- Promote the definition of strategies for MLFT Risk Management.
- Implement policies and procedures to ensure adequate MLFT risk management.
- Ensure that the company complies with the MLFT rules of the jurisdiction where it operates.
- Evaluate and verify the application of the policies and procedures of the MLFT prevention system, that includes: knowledge of the customer, knowledge of the market, knowledge of the correspondent bank, knowledge of suppliers, knowledge of counterparties and brokers, as applicable; as well as the necessary procedures to ensure the level of integrity of the directors, managers and employees.
- Communicate the CCO any incident or situation of risk that affects or could affect the operation of the procedures or controls established by the MLFT Risk Management of the company and/or of the IFS group.
- Answer to the requests of information made by the regulatory bodies and competent authorities.
- Provide the information requested by the CCO.
- Prepare and submit MLFT risk management reports to the board of directors and the CCO.
- Coordinate with the Human Management and Development department the adequate development of the Training Program of the employees of the company, on MLFT Risk Management.

Of the General Manager

- Manage the implementation of the MLFT prevention system jointly with the board of directors.
- Provide the necessary resources for the management of the Compliance Officer.
- Ensure that the development of programs and plans that guide the activities and the use of resources is carried out as established in this document.
- Direct the corrective measures that may be necessary for the compliance of this policy.
- Promote the dissemination of the compliance culture in the company.

#### Of the corporate coordinator

- Directly coordinate with the Corporate Compliance Officer the issues related to the implementation and execution of the Money Laundering and Financing of Terrorism Prevention Program in their company.
- Inform about the compliance of the Money Laundering and Financing of Terrorism Risk Management Program to all the lines of business of their company.
- Communicate the Corporate Compliance Officer any incident that affects the operation of the procedures or controls of the Money Laundering and Financing of Terrorism Prevention Program.
- Execute the processes and procedures contained in the MLFT Prevention Manual.

#### **7.1.2. Main Corporate Policies**

##### Risk approach

- The group companies and/or subsidiaries must have a MLFT Compliance Officer, who will communicate in a reasonable term the CCO the incidences or non-compliances with the corporate policies.
- Based on the MLFT prevention policies of IFS and the local rules, each group company and/or subsidiary must have a manual for MLFT Risk Management, approved by its board of directors, with risk management guidelines, policies, processes, procedures and methodologies that allow to identify, assess, control, mitigate, monitor and report their MLFT risks.
- The ML/FT Compliance Officer must ensure to have an operations monitoring system, adequate and proportional to the ML/FT risks and the size of the company. For the operations qualified as suspicious, the appropriate measures will be taken and the reports will be sent to the corresponding governmental authorities intended that purpose and within the terms established.



- Annually, each company will send the CCO an executive report on the compliance of the local policies and procedures. Said reports must be sent, as a maximum, within the first seven business days of each year. Likewise, if any high-impact incidence and/or non-compliances of this policy is identified, the report will be sent within fifteen days from the occurrence of the event.
- If the CCO finds any inconsistency or something unusual in any report, he/she must refer it to the Board of Directors of IFS, within the quarter from having discovered it.
- If there are relevant discrepancies or non-compliances, the CCO must refer them to the Board of Directors of IFS.

#### Of employees

- The companies and their subsidiaries must have an employment policy for their employees, managers and directors.
- All the employees of the companies and their subsidiaries are obliged to comply with the provisions of the Code of Conduct that, among others, highlights the principles, values, policies and controls that must be considered for MLFT Risk Management.
- In order to achieve high ethical standards among the employees of the companies, the principles, values and policies established in the Code of Conduct will be considered.
- The companies and their subsidiaries maintain a strong commitment to develop and maintain in their employees the necessary knowledge and abilities for the adequate operation of MLFT risk management.
- The companies and their subsidiaries will develop training programs to train their employees in the rules in force on MLFT Risk Management, the policies, rules and procedures established by the companies, as well as communicate all their directors, managers and employees in general the relevant changes in the rules.

#### Due diligence process in the knowledge of the customer

The group companies must comply with the following basic principles: i) identification, ii) verification and iii) monitoring

##### i. Identification

- Identify the customers at the beginning of the commercial relationship, as established in the legal rules in force.
- Establish the purpose of the commercial relationship.
- For the ML/FT prevention system, the final beneficiary is the individual on whose behalf a transaction is carried out and/or the one that has or exercises the final effective control over a customer in favor of whom an operation is carried out. It also

includes the persons who exercise the final effective control over a legal entity. The companies and their subsidiaries must identify the final beneficiary with whom a commercial relationship is established and verify if they are:

- a. A shareholder of the entity
- b. The one who has control over the customer and its equity
- c. The one who carries out transactions on behalf of another person or of the commercial relationship established.

ii. Verification

- The group companies and their subsidiaries must implement the application of procedures of verification of the information provided by customers.
- It is prohibited for the group companies and their subsidiaries to open or maintain accounts, products and/or services of any kind, as anonymous or with fictitious, inaccurate names, or exclusively with codes.
- The group companies and their subsidiaries, according to the characteristics of their customers, the products and services they offer, the operations carried out by them, the degree of risk and the level of update and verification of their information, may establish specific restrictions at commercial, operating and/or transactional level, whether at the beginning or during the commercial relationship.
- The group companies and their subsidiaries will establish policies on the knowledge of the customer, knowledge of the employee, knowledge of the market, knowledge of the correspondent bank, knowledge of suppliers and knowledge of counterparties and brokers defined under a risk approach.

iii. Monitoring of operations

- Since the monitoring of operations is one of the main mechanisms for the detection of unusual operations carried out by customers, all subsidiaries must have a monitoring system, whether automated or electronic according to the volume of transactions of each company.
- In order to prevent the disclosure of information that endangers the correct operation of the MLFT Risk Management System, the criteria and parameters established for the generation of alerts in the monitoring systems must not be published or disclosed. These parameters will be contained in internal procedures of exclusive use by the personnel appointed by the ML/FT Compliance Officer for this work.

- The ML/FT Compliance Officer has the obligation of reporting suspicious operations to the local regulator, based on their policies and good judgment, which must be kept as confidential according to the local laws on bank secrecy.

#### Record-keeping of operations

- The companies and their subsidiaries are obliged to identify the operations of their customers and keep a record of those operations.
- MLFT Risk Management comprises all customers without exception, consequently, the companies and their subsidiaries shall not maintain customers excluded from the Record-keeping of Operations or from the controls established by the regulation in force.
- The companies and their subsidiaries will establish policies and procedures to keep a record of the operations carried out by customers, as established by the legal rules in each country where they develop their activities, and inform the corresponding authorities, if applicable.
- The companies and their subsidiaries will establish policies and procedures to ensure the compliance of the Law and the internal policies referred to record-keeping and reports required.

#### Special Lists that contribute to the Prevention of ML/FT

- The companies and their subsidiaries shall not provide services to individuals or companies included in the following lists:
  - a. OFAC (Office of Foreign Assets Control).
  - b. Lists of Terrorists of the European Union.
  - c. Lists related to the Financing of Weapons of Mass Destruction Proliferation: Lists issued by the United Nations Security Council. It includes, at least, the consolidated List of the United Nations Security Council Resolution 1718, on the Democratic People's Republic of Korea (North Korea) and the consolidated List of the United Nations Security Council Resolution 1737, on Iran.
  - d. Lists of the United Nations Security Council Resolutions.
  - e. Other lists defined by the local regulation in each country where the company develops its activities and negative lists that are managed by each company.

#### 7.2. Foreign Account Tax Compliance Act – FATCA

The corporate FATCA policy has been developed for the Group Companies that classify as a Foreign Financial Institution (FFI) and are part of the Expanded Affiliated Group (EAG). A glossary of terms can be found at the end of this document.

The rule applicable to FATCA is the Law of Audit of Foreign Accounts and the policies listed below have the purpose of providing the corporate action guidelines for the compliance of FATCA:

- All the companies of the EAG of Intercorp Perú Ltd. that classify as an FFI according to FATCA must comply with said rule according to the corporate guidelines established.
- Intercorp Ltda. will be the Lead FFI and it will be responsible for identifying the FFIs that comprise the EAG and registering them with the IRS.
- In order to comply with the rule, the CCO shall be the FATCA Corporate Compliance Officer appointed by the Lead FFI.
- The FATCA Corporate Compliance Officer shall be responsible for defining the FATCA Compliance Program, consolidating and disseminating it among the other FFI and periodically controlling it.
- The General Management of each FFI of the group must appoint a Point of Contact-POC (responsible for FATCA) who will be in charge of the implementation of the requirements of the rule according to the FATCA Compliance Program, who will functionally report to the FATCA Corporate Compliance Officer.
- The procedures and policies developed by each FFI for the compliance of the rule must be aligned with FATCA Corporate Policies and be approved by the FATCA Corporate Compliance Officer.
- The individual policies related to FATCA may be stricter, but, in no case, less strict than the corporate policies related to FATCA.
- The FATCA Corporate Compliance Officer will review annually the compliance with FATCA in the entire EAG.
- The FATCA Corporate Compliance Officer will carry out the certifications required by FATCA.
- The FATCA Corporate Compliance Officer must approve all the communications (internal and external of the Group) related to FATCA.
- The FATCA Corporate Compliance Officer must identify and evaluate the changes in FATCA Corporate Policies if: (i) modifications are made to FATCA, (ii) an IGA is signed in a country where an FFI is incorporated; or, (iii) modifications are made in the local regulations of the country of incorporation of an FFI that affect the compliance with FATCA.
- The Point Of Contact-POC (responsible for FATCA) of each FFI must identify and communicate the FATCA Corporate Compliance Officer if any change in the local regulations of the country of incorporation of the FFI affects the compliance with FATCA.
- No employee of the companies of Intercorp Perú Ltd who qualifies as an FFI may cooperate with the customers of those companies to evade the provisions of FATCA.
- The employees who have direct contact with customers must inform the Point Of Contact-POC (responsible for FATCA) in each FFI, if they identify indicia or have knowledge that one of its customers is a U.S. Person.

**7.2.1. Related to onboarding or registration of new customers**

- From the effective date of the rule, all the FFIs must evaluate and classify their new customers according to the requirements of FATCA.
- The procedure of onboarding or registration of new customers must be applied to new customers (individuals and legal entities), from the effective date of the rule.
- Each FFI may decide if it will evaluate and classify all its new customers or only those that obtain products impacted by FATCA.
- The information provided by the customer according to the procedures described in the rule must be assessed, with the purpose of verifying whether there is indicia of being a U.S. Person or not.
- FATCA classification of new customers must be registered in a mandatory field in the customer database that the FFI defines.
- If a new customer is classified as a U.S. Person, they must provide W9 form and sign a waiver.
- New customers classified as an FFI must provide their GIIN code.
- The FFI will not accept new customers classified as recalcitrant or NPFFIs if the FFI is incorporated in a country where the withholding requirements of FATCA are not compatible with the local laws.
- Each FFI may define its own new customer evaluation and classification strategy provided that it is aligned with FATCA Corporate Policies and the FACTA rule.
- The Point Of Contact-POC (responsible for FATCA) of each FFI must periodically review and validate (based on a sample) the classification given to new customers.

**7.2.2. Related to existing customers**

- The FFIs must implement annual verification procedures that allow to identify if the financial accounts of new customers who were not evaluated or classified, because they were below the minimum thresholds, exceeded US\$ 1,000,000. If so, they must be evaluated and classified according to FATCA.
- The existing customers will be evaluated according to the information available electronically and/or in physical files (as required by FATCA) obtained through onboarding, AML and KYC processes.
- Each FFI must have the necessary documents that support the conduction of the evaluation and classification procedures established by the rule. Those documents must be kept for a period of no less than 10 years.
- FATCA classification of the existing customers must mandatorily appear in a field of the database defined by the FFI.
- It is required to have a database that allows for the management and tracking of the information requested and delivered by the existing customers identified with indicia of being a U.S. Person.
- The existing customers classified as a U.S. Person must provide W9 form and sign a waiver.

- The existing customers classified as FFI must provide their GIIN code.
- The FFI must not carry out any type of operation with existing customers classified as recalcitrant or NPFIs if the FFI is incorporated in a country where the withholding requirements of FATCA are not compatible with the local laws. If possible, any relationship with customers classified as recalcitrant and NPFIs must be terminated.

7.2.3. Related to the change of circumstance

- FATCA classification of (new and existing) customers could be affected if a change of circumstance occurs. Changes of circumstance are the modifications in the basic information of customer (related to the seven types of indicia), that make FATCA classification given no longer valid.
- The FFIs must implement procedures to detect changes in the basic information of their customers that imply a change of circumstance.
- After a change of circumstance, if a customer does not submit the documents that justify their new status in a period of 90 days, said customer will be considered as recalcitrant.
- The FFIs must review, on a monthly basis, the changes of circumstance of customers and they will have 60 days to collect the information and update FATCA classification of customer.

7.2.4. Related to withholding

- The withholding required by FATCA shall be applicable only if the local laws of the place where the FFI is incorporated allow it.
- The withholding is applicable to customers classified as recalcitrant or NPFIs.
- The payments subject to withholding are:
  - Any payment of interest, dividends, rents, salaries, wages, premiums, annuities, compensations, remunerations, fees and other fixed, determinable, annual or periodic profits or income, if said payment comes from sources inside the USA.
  - Any gross income from the sale or other disposition of any property that could generate interest or dividends from sources inside the USA.
- Each FFI is responsible for the identification, calculation and application of withholding according to the terms established by the rule.

7.2.5. Related to reporting

- Reporting is applicable to customers classified as:
  - U.S. Person.
  - Recalcitrant.
  - NPFIs.
  - NFFE with substantial U.S. owners.
- The products subject to reporting are passive products related to: deposit accounts, escrow accounts and debt or equity instruments maintained in the

FFI, life insurance contracts with cash value or annuities, among others. Each FFI is responsible for identifying the products subject to reporting.

- Each FFI is responsible for meeting the reporting requirements in the terms established by the rule for each type of customer.
- It is not allowed to disclose the identity of customers classified as recalcitrant in the reports required by FATCA, unless the local laws of the country where the FFI is incorporated allow it.
- The reports made under FATCA must have the approval of the FATCA Corporate Compliance Officer before they are sent to any external entity of the Group.

7.2.6. Related to the creation of new products or modification of existing products

- Each time new products are created or the existing products are modified, they must be evaluated by the Point Of Contact-POC (responsible for FATCA) of each FFI with the purpose of identifying whether it is impacted by FATCA or not, which shall be communicated to the FATCA Compliance Officer. Each FFI is responsible for establishing this control in the procedures of creation / modification of related products.
- A product will be impacted by FATCA if:
  - It is subject to reporting.
  - It is subject to reporting and generates payments subject to withholding.

7.2.7. Related to counterparties

- Counterparties are all third parties through which transactions impacted by FATCA and/or transactions related to products impacted by FATCA are completed (v.g. brokers, dealers, banks, brokerage firms, escrow agents, among others). In general, the transactions impacted by FATCA are all those that can involve payments subject to withholding.
- The FFIs may only make investments in the United States (directly or indirectly) through counterparties that:
  - Comply with FATCA (which are FFIs).
  - Are incorporated in the USA.
  - Are incorporated in a country that has signed an IGA.

7.2.8. Related to third parties that perform duties of FATCA

- One of more duties of FATCA can be outsourced with the approval of the FATCA Corporate Compliance Officer.
- If any of the duties of FATCA or process impacted by FATCA is outsourced, the supplier of the service must comply with the provisions of FATCA rule in compliance with FATCA Corporate Policies. The specific activities must be established in the contract.

7.2.9. Related to the acquisition, sale, liquidation or closure of new companies or own funds.

- If Intercorp Perú Ltd. acquires (directly or indirectly) a company in which it has a 50% interest or more (even if it does not have voting right or managerial rights), it must be communicated to the FATCA Corporate Compliance Officer.
- If Intercorp Perú Ltd. or one of the FFIs that comprise its EAG establish an own fund, it must be communicated to FATCA Corporate Compliance Officer. All funds, according to FATCA, are FFIs regardless of whether they have legal entity status or not.
- The FATCA Corporate Compliance Officer must determine if the companies acquired classify as an FFI.
- All new own funds and new companies that qualify as FFI must be registered with the IRS by the Lead FFI as members of the EAG.
- If any of the FFIs registered with the IRS is sold, liquidated or deregistered, it must be communicated to the FATCA Corporate Compliance Officer. The lead FFI must update the registration with the IRS indicating the deregistration.

7.2.10. Glossary

▪ **Active NFFE (Active Non-Financial Foreign Entity)**

A NFFE engaged in non-financial activities and where less than 50 % of its income of the last calendar year is passive income, and less than 50 % of its weighted average of assets generate passive income.

▪ **AML (Anti Money Laundering)**

Anti-Money Laundering.

▪ **Annuity**

Series of periodic payments (e.g. products of life annuities)

▪ **Cash Value**

Any amount that:

- Is payable under a life insurance contract to any person upon its redemption, delivery, cancellation; or,
- Any person entitled to said amount during the insurance contract.

▪ **Existing customers**

Customers maintained by the FFI before July 1, 2014.

▪ **New customer**

Customers acquired by the FFI from July 1, 2014.



- **EAG (Expanded Affiliated Group)**

It is an affiliated group, comprised by all the companies that classify as FFI in which a same owner holds more than 50% interest (beneficial interest) of each of them (even if they do not have voting right or managerial rights).

- **Excepted NFFE (Excepted Non-Financial Foreign Entity)**

Non-financial foreign entity exempted from withholding.

- **FATCA (Foreign Account Tax Compliance Act)**

Rule issued by the IRS to prevent tax evasion. It includes new compliance rules related to accounts or investments outside the USA by its citizens and residents.

- **FDAP (Fixed, determinable, annual or periodic)**

It means any payment which is fixed, determinable, annual or periodic. For instance, the payments of dividends, interest, coupons, etc.

- **FFI (Foreign Financial Institution)**

- Any financial institution incorporated outside the USA and its territories, that meets any of the following circumstances:
  - a. It accepts deposits in the normal course of a banking business or a similar one;
  - b. It maintains financial assets on behalf of third parties, as a material portion of its business (50% of income from interest, dividends and financial returns);
  - c. It is involved in the business of investment, reinvestment or trading of financial assets;
  - d. It is a life insurance company that offers any product with cash value or annuity;
  - e. It is a Holding or Treasury Center that is part of an EAG.
- Any financial institution incorporated outside the USA and its territories, which is a resident in a country that has, effective, a Model 1 IGA or a Model 2 IGA.

- **Financial Account**

It refers to deposit accounts, escrow accounts and debt or equity instruments maintained in a financial institution, life insurance contracts with cash value or annuities, among others.

- **GIIN (Global Intermediary Identification Number)**

It is the identification number assigned to a PFFI or a Registered-Deemed Compliant FFI, as well as to the entities classified as Model 1 FFI, with the purpose that the registered entities can be identified through the code assigned. All GIIN assigned will appear in the list published by the IRS.

- **Hold Mail**

Service provided by certain banking entities, where the correspondence of a customer is received and kept by the banking entity.

- **IGA (Intergovernmental Agreement)**

An agreement between the US government or the IRS and a foreign government to implement or facilitate the implementation of FATCA.
- **IRS (Internal Revenue Service)**

US governmental agency responsible for tax collection and compliance with tax laws in the USA.
- **KYC (Know your customer)**

Knowledge of the customer.
- **Model 1 IGA**

Model of agreement between the IRS and a foreign government, in which the FFI shall report to the domestic regulatory authorities.
- **Model 2 IGA**

Model of agreement between the IRS and a foreign government, in which the FFI shall report to the IRS.
- **Non-U.S. Person**

Individual who does not have US nationality or citizenship.
- **NFFE (Non-Financial Foreign Entity)**

Non-financial entity incorporated outside the USA and its territories.
- **NFFE with substantial U.S. owners**

The shareholders, who own more than 10% interest and which are also US citizens or residents, of a NFFE classified as Passive.
- **NPFFI (Non-Participating FFI)**

Financial institution incorporated outside the USA and its territories, which does not comply with FATCA.
- **Passive NFFE**

A NFFE that is not Active or Excepted.
- **PFFI (Participating FFI)**

Financial institution incorporated outside the USA and its territories, which complies with FATCA.

▪ **Recalcitrant**

It refers to customers of the FFI in any of the following cases:

- Individuals with U.S. indicia, who did not provide sufficient evidence that proves their U.S. Person or Non-U.S. Person status;
- The holder of the account does not provide a valid W-9 form or provides an incorrect combination between TIN and name;
- According to the laws of the country of incorporation of the FFI, if the customer is classified as a U.S. Person, they do not provide a valid Waiver that allows for the reporting of their accounts.

It is a Passive NFEF that did not provide the necessary documents to certify that it does not have Substantial U.S. owners.

▪ **Registered Deemed Compliant FFI (RDC FFI)**

It is an FFI that meets the procedure requirements described in paragraph (f)(1)(ii) of the rule, or described in any of paragraphs (f)(1)(i)(A) to (F) of the rule, or it is treated as a Registered Deemed Compliant FFI under a Model 2 IGA. A Registered Deemed Compliant FFI also includes any FFI, or branch of an FFI, which is a Model 1 that meets the registration requirements of a Model 1 IGA.

The requirements mentioned are the following:

- To register with the IRS according to the procedures established by the IRS and commit to the terms of the registered deemed compliant status;
- To have its responsible officer who will certify, every three years, to the IRS, whether individually or collectively, for an expanded affiliated group of the FFI, that all the requirements for the category have been met as of December 31, 2013;
- Keep in its records the confirmation of the IRS of the registration of the FFI as a deemed-compliant FFI and GIIN or any other information that the IRS specifies;
- Agree to notify the IRS if there is a change of circumstances that would make the FFI ineligible for a deemed-compliant status. For that purpose, it must correct it within the six months following the modification of the information.

▪ **Substantial U.S. Owner**

It means the shareholders of an entity, who hold more than 10% interest and who are also US citizens or residents.

▪ **TIN (Taxpayer Identification Number)**

Taxpayer identification number.

▪ **U.S. Account**

It means any financial account maintained by an FFI, owned by one or more U.S. persons or U.S. foreign entities.

▪ **U.S. Indicia**

Indicia in the basic information of customers that could indicate that a customer is a U.S. Person:

- US Citizenship/Nationality.
- Place of birth in the USA.
- Address (of any kind) in the USA.
- Telephone number (considering the country code) in the USA.
- Permanent instructions of transfer to the USA as country of the destination account.
- US address of the persons with powers granted over an account.
- Address of any US bank that works as Hold Mail for the customer.

▪ **U.S. Person**

The individual who has US nationality, citizenship or residence.

▪ **W-9**

Form issued by the IRS which is used by the U.S. Person for their TIN.

▪ **Waiver**

Document certified by the IRS that must be signed by the individuals identified as U.S. Person, to authorize the PFFI to report said individual with the IRS.

7.3. Improper Use of Privileged Information

The laws that govern the securities market of several countries and which are applicable to the companies that maintain securities listed in a stock exchange have the purpose of guaranteeing that all investors in a company have equal and timely access to “Material Information” (as defined in the glossary attached hereto) related to said company when deciding to buy, keep or sell their securities.

The rules applicable to this policy are:

- The Regulations against Market Abuse
- Rules on the improper use of privileged information and market manipulation

The objective of this Policy and Procedures on the Improper Use of Privileged Information (the “Policy”) of Intercorp Financial Services Inc. (“IFS” that, collectively with its subsidiaries Banco Internacional de Perú S.A.A. (“Interbank”), Interseguro Compañía de Seguros de Vida S.A. (“Interseguro”) and Inteligo Group Corp. (“Inteligo”) and any subsidiary of those subsidiaries, shall be called herein as the “Organization” or the “Subsidiaries”, excluding IFS) consists in establishing the restrictions and procedures applicable to the purchase and/or sale of securities of the Organization (“Securities of the Organization”) by the persons with access to Material Information or Privileged Information (as defined in the glossary attached hereto) related to the Organization. The Policy has been developed to support the

Organization and its employees in order to prevent any risk of violating the applicable rules in force of the securities market.

### **Scope of the policy**

#### **7.3.1. Persons included in this Policy**

- All the directors, officers and employees in general of the Organization with access to Privileged Information, as well as their relatives or other persons who live in the same domicile;
- Any other person or entity, including a trust, legal entity, partnership or other association, that carries out an operation with securities of the Organization, which securities are actually owned by any of the persons indicated in the first bullet above; and,
- Any external person or entity that has access to Privileged Information.

The persons and entities described above are called the “Included Persons”

The Corporate Compliance Officer/Chief Compliance Officer (CCO) shall keep a central register with the updated list of all the Included Persons, who have been identified and designated as such by the corresponding Compliance Officers of the Organization. Each Compliance Officer of the Subsidiary Companies shall identify and designate the Included Persons in their corresponding companies and subsidiaries and shall provide this list to the Corporate Compliance Officer/Chief Compliance Officer (CCO). Each Compliance Officer of the Subsidiary Companies shall identify and designate the Included Persons in their corresponding companies and subsidiaries and shall provide this list to the Corporate Compliance Officer/Chief Compliance Officer (CCO) of IFS.

#### **7.3.2. Responsibilities of each company**

Board of Directors:

- Approve and supervise the compliance of the policies on the improper use of privileged information.
- Approve or perform the necessary actions that allow to prevent the abuse of privileged information.
- Approve the sanctions proposed by the CCO for non-compliances related to the policies on the improper use of privileged information.

General Management

- Guarantee, according to the provisions of the Board of Directors, the resources and the appropriate organization for the adequate management of compliance of the policies on the improper use of privileged information.

Main Office of Corporate Compliance or Chief Compliance Officer (CCO)

- Supervise and ensure the compliance of this policy.
- Refer the cases of potential non-compliances to the General Management and the Board of Directors, as applicable.

#### Compliance Officer

- Review and identify any risk of non-compliance of the policies to timely communicate it to the CCO.
- Recommend the CCO the measures that, in their judgment, should be taken in case of an eventual abusive or unfair use of privileged information.
- Share the policies of privileged information with all the employees of the company.
- Conduct a quarterly review of the compliance of the policy.
- Validate that the included persons have signed the certificate in which they declare that they have read and understood the terms of the policy.
- Inform the results to the OCC.

#### Employees

- Comply with the compliance policy of their company, as well as seek guidance with the compliance officer and/or direct boss under any situation that could be perceived as irregular or inappropriate.

#### **7.3.3. Operations contemplated in this Policy**

- All type of securities that could be issued by the Organization periodically including, without limitation, common shares, common shares purchase options, debentures, preferred shares, convertible obligations and options traded or not in a stock exchange or other financial derivatives (collectively, the “Securities of the Organization”); and,
- The common shares of another entity in which said entity begins discussions and strategic operations with the Organization regarding a combination or consolidation, merger, acquisition or similar operation.

#### **7.3.4. Individual responsibility**

##### **Information of the Company**

All the Included Persons may have access, incidentally or in the normal development of their work with the Organization, to information on the financial results or the financial position or other plans of the Organization, which are not in the public domain yet. Said person has the obligation of not using this privileged position for their own direct or indirect benefit, or for

the benefit of third parties. Thus, said person is responsible for understanding this Policy and following its guidelines.

### **Certificate**

A copy of this Policy shall be provided to all the directors, officers and employees and to external persons or entities of the Organization, identified and designated as Included Persons. The receiver must sign a certificate that they have read and understand the terms of the Policy. A form of certificate is attached hereto. The original of the Certificate signed must be sent to the CCO of IFS, by the Compliance Officer of the corresponding company.

### **Prohibitions related to the improper use of privileged information**

The improper use of Privileged Information implies the trading of securities using confidential internal information. According to the rules applicable to the Organization related to the improper use of Privileged Information, a person trades based on Privileged Information regarding a security or an entity if the person who carries out the purchase or sale had knowledge of the Privileged Information at the time when the person carried out the purchase or sale.

### **Prohibition of Trading of Securities based on Privileged Information**

- No Included Person must buy or sell the Securities of the Organization, or otherwise advise or help a third party in the trading of Securities of the Organization, if they have knowledge of Privileged Information.
- Likewise, if an employee obtains Privileged Information about another public entity, in the performance of their duties in the Organization, they are prohibited by this Policy to trade the securities of said entity.
- The information that has been disclosed to the public through the adequate channels but which has not been yet absorbed by the investors and the financial community, must continue being considered as Privileged Information and as an illegitimate base to trade securities.

### **Confidentiality of Privileged Information**

- All Included Persons must act with maximum precaution to keep the confidentiality of said information. Any person with access to Privileged Information that “discloses” it to another person shall be as responsible as the person who receives the Privileged Information for the improper use given to it by them.
- In order to reduce the possibility that the Privileged Information be inadvertently disclosed:

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

- The Included Persons must refrain from talking about information related to the Organization in public places where someone could listen to these conversations.
- The Included Persons must treat the Material Information and/or Privileged Information as confidential and they must not talk about it with any other person who does not “have the need to know” the information for legitimate business purposes.
- The employees who become aware of a disclosure of Privileged Information, whether inadvertently or otherwise, must immediately inform the CCO of IFS about said disclosure.

In order to prevent the disclosure of Privileged Information about a customer, borrower, investment, acquisition goal or seller to persons other than those who work in an issue particularly confidential, the Compliance Officer of the company where these persons work may build what is known as an “ethical barrier” around an operation or issue.

An ethical barrier is a mechanism designed to stop the flow of information from one department or person to another with the purpose of keeping the confidentiality or avoiding conflicts of interests. Depending on the specific situation, the creation of an ethical barrier can include procedures such as the identification of selected members of the personnel who will have access to the issue, establishing a separate physical environment for the project with restricted access, using independent servers for computer files and/or regularly deleting all the electronic information related to the issue, as necessary. The procedures of ethical barrier established for a specific issue must be communicated in writing to the affected persons. The employees who consider that it is necessary to establish an ethical barrier in a certain situation, must consult with the Compliance Officer of the company where they work.

The request of creation of an ethical barrier must be informed to the CCO of IFS by the Compliance Officer of the company that receives the request.

**Additional restriction applied to the persons of the company with access to privileged information**

In order to minimize the risk of a non-compliance with this Policy and all the purchases, sales and other operations with Securities of the Organization carried out by the Included Persons or Persons of the Company with Access to Privileged Information must be previously authorized.

**Previous Approval Procedure**

Before beginning any operation with Securities of the Organization, the Persons of the Company with Access to Privileged Information must provide



the CCO of IFS with a Request for Approval, which model is attached hereto. The Requests for Approval must be delivered by email. If an operation is approved, but the trading is not carried out within two (2) business days computed from the date of approval, a new Request for Approval must be submitted. The Compliance Officer of each of the Subsidiaries must channel the corresponding requests for previous approval to the CCO of IFS. All the approvals shall be granted by the CCO of IFS.

### **Restriction Periods**

As of the closing of each quarter and within the terms established in the applicable regulation, the Organization will announce the market the financial information about its performance. The Organization has established what it calls the “restriction period” for the Included Persons who may have access to this information in the performance of their duties. Even if the Organization is not in a restriction period, no Included Person may buy or sell Securities of the Organization if they have Privileged Information.

The restrictions periods shall apply from the beginning of the first day following the last month of each tax quarter (namely, it begins on January 1, April 1, July 1 and October 1 of every year) until and including, two full trading business days following the public disclosure of the quarterly or annual financial results of IFS or its Subsidiaries, as applicable.

In addition to these restriction periods regularly scheduled, the Organization may impose restrictions on all or on a relevant group of persons with access to Privileged Information or additional restriction periods during which Privileged Information exists.

No Person of the Company with Access to Privileged Information may buy, sell or enter into any other operation regarding the Securities of the Organization during any restriction period.

Restriction periods do not apply to:

- The purchase or sale of Securities of the Organization in a “blind” trust, mutual fund, “hedging” account or similar agreement, provided that there is no possibility of discussing or giving instructions regarding the investment of the funds managed in those investment vehicles.
- Other cases included in this Policy.

Any Person of the Company with Access to Privileged Information who has questions about the restriction periods must contact the Compliance Officer of the company in which they work or to which they provide services or the CCO of IFS.

### **Additional Restrictions on the Trading by the Persons of the Company with Access to Privileged Information**

The Persons of the Company with Access to Privileged Information are also prohibited to participate in the following operations with the Securities of the Organization:

- Short-term trading; all the Securities of the Organization must be maintained during a minimum term of six months;
- Purchases, or sales, at margin;
- Short sales (namely, the sale of shares that are not their own at the time of the sale); and,
- Purchase or sale of purchase or sale options.

### **Restrictions on the trading by persons with potential access to privileged information**

No Person with Potential Access to Privileged Information may buy or sell Securities of the Organization if they have knowledge of any Privileged Information.

Every employee, regardless of their position in the Organization, for the single fact of having knowledge of Privileged Information, shall be subject to this Policy and to strict legal rules that regulate the improper use thereof. Any person who has doubts on whether they have knowledge of Privileged Information about the Organization or not, must contact the Compliance Officer of the company in which they work or to which they provide services or the CCO of IFS.

### **Glossary of Privileged Information**

- **Material Information**

“Material Information” shall mean any act, decision, agreement, event, trading in course or information referred to the Organization, the Securities or its businesses that:

- Have the capacity to significantly influence in the investment or vote decision of a reasonable shareholder;
- Once publicly disclosed, it would be expected to significantly alter the information available in the market about the Organization; or,
- Have the capacity to significantly influence in the liquidity and/or the price of the Securities of the Organization.

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

- Material Information includes, among others, information about results, including any information about the financial results and the significant changes in the financial results and/or the financial position (annual, semi-annual, quarterly, monthly) and the financial projections.
- The information can be important, regardless of whether it is positive or negative for the Organization.
- Other types of information that can be considered as Material Information are:
  - Mergers, divestitures, acquisitions, acquisition offers, joint ventures, or significant changes in the assets;
  - Changes in the management or changes in control;
  - Changes in predicted profits or losses;
  - Transfers of shares or plans for the purchase or redemption of important shares;
  - Payment of dividends or changes in the dividend policy;
  - Valuation reports;
  - New significant products, services or market;
  - Significant developments related to customers or suppliers (e.g. the acquisition or loss of an important contract);
  - Changes in the auditors, or notice of the auditors that the Organization can no longer rely on the audit report;
  - Auditors' report including a qualified opinion;
  - Financial Statements of the Organization;
  - Events related to the Securities of the Organization (e.g. defaults, redemptions, payment in installments, reacquisition plans, changes in the dividends, changes in the rights of the holders, offers of additional securities);
  - Significant profits or losses in important operations of the business;
  - Significant termination or dismissal of employees;
  - Significant litigation against the Organization or any significant development related to said litigation;
  - Bankruptcy or judicial receivership;
  - Important financing operations including significant increases or reductions of the indebtedness amount; and,
  - Any other information that could have a significant impact on the market value of the Securities of the Organization.

▪ **Privileged Information**

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

“Privileged Information” shall mean the Material Information, directly or indirectly, referred to the Organization which has not been disclosed to be made available of investors in general. The information continues to be “private” until it has been disclosed to the public through the adequate channels and the investors have had sufficient time to absorb and evaluate the information – usually two (2) business days, unless the laws applicable to the company that is part of the Organization establish a different term.

All material information related to the Organization shall be disclosed only through the regular disclosure channels so that all the interested persons in the Organization and their securities have, in the extent possible, fair and timely access to said information. A person that has knowledge about Material Information may not try to “win the market” trading securities simultaneously with the official disclosure of that information or short after said disclosure.

In general, it can be considered that the information has been absorbed and evaluated by public markets two (2) days after the information has been publicly disclosed. If an announcement is made after the closing of the operations, for instance, a Friday, the trading will not be permitted until the next Wednesday, at least.

All the Material Information of the Organization shall be announced through the procedures established to guarantee the adequate distribution to the agencies of financial news and the press, as well as to specialized publications and other interested persons.

Until this procedure has been followed, the information has not been “disclosed to the public”. The fact that the information can appear in a specialized publication or in an announcement made by the customer, supplier, manufacture partner or joint venture, competitor or governmental agency is not enough. The improper use of Privileged Information does not become licit for the fact that material information is transmitted through rumors or other non-official declarations in the press or in the market. When employees become aware of rumors or other non-official declarations about the Organization, the CCO of IFS must be immediately notified in order to determine if measures must be taken for an adequate and broad public disclosure of any information that may be important.

In addition to the information related to the Organization that has not been publicly disclosed, it must be assumed that the private information includes confidential analyses, financial information, data and business plans, as well as information received from a customer or third party

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

with the expectation that it will be kept as confidential and that it will be used only for business purposes.

In addition, it must be taken into account that, according to Peruvian rules, the information intended to be disclosed to the general public is not considered publicly disclosed when it has been disclosed by the Organization only in a general shareholders' meeting, in a board of directors' meeting or in similar meetings or if it has been disclosed by the Organization in a committee, group of investors, analysts or other participants.

- **Employee**

"Employee" shall have the definition assigned in the Code of Ethics and Business Conduct Standards.

*INTERNAL USE INFORMATION: The partial and total reproduction of the document without authorization is prohibited*

**Certificate of having read and understood the policy of improper use of privileged information**

**CERTIFICATE**

The undersigned hereby certifies Intercorp Financial Services Inc. that he/she has read and understands the Policy and Procedures on the Improper Use of Privileged Information of Intercorp Financial Services Inc. effective as of [\_\_\_\_\_], 2018, which copy shall be kept by the undersigned.

I also declare that as of the date of execution of this certificate I am the holder of [\_\_\_\_\_] shares of [\_\_\_\_\_]

**By:** \_\_\_\_\_

**Name (Print):**

**Date:** \_\_\_\_\_

**Form of request for approval**

**Please send to:**

[Insert pertinent names and contact information]

**Date of submission:** \_\_\_\_\_, 20\_\_\_\_

**Request for Approval to Participate in Operations with the Securities of the Organization**

**Name:** \_\_\_\_\_ **Telephone number** \_\_\_\_\_

I request the approval to carry out the following operations related to the Securities of the Organization:

**Type of Operation:**

Purchase \_\_\_\_\_ Sale \_\_\_\_\_ Exercise of Option \_\_\_\_\_

Other \_\_\_\_\_ (Explain:) \_\_\_\_\_

**Securities of the Organization that will be Traded:**

Number of shares or amount:  
\_\_\_\_\_

**Holder** (Indicate if it is not applicable):

Name of beneficiary if they are not you: \_\_\_\_\_

Relationship of the beneficiary with you: \_\_\_\_\_

**Certification:** I hereby certify that, when making the request, I comply with the applicable provisions of the *Policy and Procedures on the Improper Use of Privileged Information of Intercorp Financial Services Inc.* I understand that the approval, if granted, shall be valid for a maximum term of two (2) business days (including the date of approval) or until any applicable restriction period begins, whichever occurs first.

Date: \_\_\_\_\_, 20\_\_\_\_ Signed: \_\_\_\_\_

-----  
Only for the use of [insert the title of the adequate officer of the company]

Date and time of reception: \_\_\_\_\_ By: \_\_\_\_\_

Approved: \_\_\_\_\_ Rejected: \_\_\_\_\_

By: \_\_\_\_\_ Date: \_\_\_\_\_

#### 7.4. Anti-corruption

The companies of IFS group have a zero-tolerance policy towards corruption and, in that sense, they will reject any business transaction that implies any form of bribery. Thus, no benefits are offered or given to improperly influence in the decisions or actions or third parties.

All employees and directors have the duty and commitment to comply with those policies.

##### **7.4.1. Scope of the Policy**

Anti-corruption policies comprise the different stakeholders (suppliers, customers, employees) of the companies that are part of IFS Group, considering the following:

- Law N° 30424
- Ministerial Resolution N° 0061-2018
- ISO 37001: Anti-bribery Management System
- For the companies that operate in Peruvian territory:
  - Peruvian Law, Legislative Decree 1352: Legislative Decree that expands the administrative responsibility of legal entities
  - Peruvian Law, Legislative Decree 1385: Legislative Decree that sanctions corruption in the private scope
- Foreign Corrupt Practices Act of 1977 (FCPA) of USA
- Bribery Act 2010 of UK
- International good practices

##### **7.4.2. Policies**

- Employees must not offer or promise anything of value to a third party with the intention of obtaining or retaining any business or improper, illegal or unethical advantage. Some examples of benefits that could be used to influence are:
  - Gifts, meals
  - Invitations to events or meetings
  - Employment offers
  - Business opportunities
  - Personal favors
- Exceptionally, officers can give gifts, travels and/or entertainment presents to officers of national or foreign governments, with a written authorization of the general manager or of a director of the company.
- The companies and their subsidiaries must have a channel for complaints that must be managed by the department designated by the senior management. This department must manage the complaints, keeping the confidentiality of the sender.



- Employees shall not make any payment to officers of national or foreign governments, including governmental employees of lower rank, to accelerate, expedite, thank or reward the performance of a routine governmental action. Some examples of actions that are not acceptable are shown below:
  - A payment to improperly avoid a penalty or taxes.
  - A payment to corruptly influence in the decision of an officer to issue a permit or a license
  - A payment to improperly ensure a favorable decision on zoning
  - A payment to improperly influence in the award of a contract with the State
  - A payment to a lawmaker to support a preferential legislation
  - A payment to a government inspector to not to take into account the safety regulations or rules.
- The employees on behalf of any of the companies of IFS Group shall not make any kind of contribution to any candidate to political positions or to a political party in any country, unless the Guidelines on Political Donations of the Company are followed or unless the contribution is previously approved in writing by the senior management.
- Likewise, facilitating payments which purpose is to expedite steps or facilitate the provision of a service are prohibited, even if they do not have the purpose of obtaining an improper benefit.
- The use of funds, assets or personnel of any of the companies of IFS Group for any illegal, improper or unethical purpose is strictly prohibited.
- Employees must not use third parties or entities (such as distributors, agents, advisors, relatives or family companies) to offer or give benefits through them which we are not permitted to offer or give.
- Sponsorships: The purpose of the activity of sponsorships is the granting of economic aid to the sponsored persons for the development of their sports, charity, cultural, scientific or similar activities in exchange for their commitment to cooperate in the advertising activity of the companies and their subsidiaries. In any case, the activity of sponsorship must be directed to strengthen the brand and the business of the companies and their subsidiaries. The department responsible for the management of sponsorships and donations shall implement procedures and controls to avoid that, under their name, activities that violate this policy be carried out.
- Donations and Contributions to Foundations and other non-governmental entities: the companies and their subsidiaries must establish timely procedures in order to prevent that the donations and contributions can be used as excuse to carry out practices that violate this policy, code of ethics and conduct.

In general, under the Anti-corruption Policies, a governmental officer may be:

- An employee or officer of a government (including departmental or regional, provincial, municipal and local governments, independent and semi-independent bodies, councils and agencies);
- An employee or officer of companies owned or controlled by a government or state;
- An employee or officer of political parties or an officer of a political party;
- An employee or officer of international public organizations (usually, organizations comprised by member States, such as the UN);
- An employee or officer of State-owned utility companies; or a candidate to a public or political position.
- In addition, any person who acts on behalf of the abovementioned persons or entities must be treated as a foreign governmental officer under this Policy.

Improper payments, gifts or objects of value are not always evident. They can include:

- Excessive entertainment or entertainment not related to a legitimate business purpose
- Gifts, invitations or luxurious, expensive or excessive presents
- Travels not related to a legitimate business purpose
- Personal loans
- Improper commissions or payments
- Unexplained commissions or fees
- Political donations or contributions with commitments
- Fees contingent or conditioned to the “success” of a work or management
- Cash payments to expedite the services
- A promise to pay or payment request for a service that exceeds the normal, usual or market commission or fee charged for that service is a sign of alert that said payment could violate the Policy. If you become aware of an agreement that indicates that excessive commissions or fees have been paid or will be paid, you must inform the Compliance Officer immediately.

## **8. Monitoring**

The group companies must periodically carry out processes of monitoring of the controls implemented to assess the compliance with the corporate policies.

This monitoring must be carried out at least with the periodicity established by the relevant rules in the place where the activity is developed.

## **9. Internal and External Audit**

The group companies must conduct internal and external audits with the purpose of measuring the effectiveness of the program and improve the operations of the organization. They must be conducted as established by the internal regulation and/or rules of the company.

## **10. Sanctions for non-compliances**

The violations to these policies are serious events, which have consequences inside the organization and in some legal cases. The employees who fail to comply with them shall be subject to the corresponding disciplinary measures, even including termination, as established in the code of conduct and internal work regulations. In the case of non-compliances with the applicable laws, they could cause civil or criminal actions by the competent authorities.

## **11. Reports on non-compliances**

Any person who violates any policy or who has knowledge of a violation by another person, must immediately inform it to the Compliance Officer of the company in which they work and they must also immediately inform the CCO with the purpose of immediately implementing the corresponding corrective measures.

Each company which is part of IFS group must develop an instruction manual that defines the policies, responsibilities and sanctions that will be applied in case of non-compliance with any of the rules. In any way they must have a channel of complaints, which must be managed by the department designated by the senior management. This department must manage the complaints, keeping the confidentiality of the sender.

## **12. Inquiries**

The inquiries regarding any of the provisions or procedures of this document must be sent by email to the OCC/CCO, compliance box or to the email of the compliance officer assigned to each group company.