General Overview of the Use of Confidential Information

Scope	This policy applies to all Employees, as well as to their family members or other people living at the same residence, Directors, Providers, Suppliers and Third Parties that generate, acquire, use, transfer, keep and manage inside or privileged information.
Objective	To guarantee the correct use of the bank's internal information.
Documents Related to External Norms	**Central Bank of the Bahamas** ▪ Guidelines for Corporate Governance of Bank and Trust companies with a License for carrying our business in and from the Bahamas. **Superintendency of Banks of Panama** ▪ Rule Nº 6-2011 – issued by the Superintendency of Banks of Panama **International Standards Organisation** ▪ ISO 27002 Information Security
Corporate Documents Intercorp Financial Services	▪ Corporate Governance Manual ▪ Policies and Procedures regarding the Undue Use of Privileged (Insider) Information ▪ Code of Ethics and Conduct
Other Related Policies and Processes	**Processes** ▪ CT.3.2.02 How to Classify Information Assets ▪ CT.3.2.01 Information Systems Users Administration **Policies**: ▪ Code of Ethics and Conduct ▪ Business Continuity ▪ Information Systems Security ▪ Using the Internet and E-mail ▪ Know your Employee ▪ Managing Vendors, Suppliers, Providers (Providers) and Third Parties ▪ Information Assets Management
Related Exhibits	▪ Classifying Information Assets ▪ Non-Disclosure Agreement for Providers ▪ Employee Non-Disclosure Agreement

Definitions

- **Non-Disclosure Agreement:** Legal agreement, between at least two parties or entities for sharing confidential material or knowledge for certain purposes, but restricting the public use thereof.
- **People with Access to Privileged (Insider) Information:** List of those Employees, Directors or others that, because of their functions, do have access to privileged (insider) information.
- **Restriction Period:** Period of time during which personnel with access to privileged (insider) information should abstain from trading in the Bank's economic securities in order to avoid any possible conflict of interest.
- **Economic Securities of the Bank:** Any kind of securities that it may issue from time to time, e.g. warrants for buying common stock, debt titles, preferred shares, convertible obligations and options, traded on some securities exchange or not or other derivative financial instruments, common stock of another entity where such entity initiates the Bank's strategic discussions and operations about a combination or consolidation, merger, acquisition or similar operation.

Policy Administration

It is the responsibility of the general manager

- Review and approve any modification of this policy.
- Guarantee, in accordance with the provisions of the Board of Directors, the resources and the appropriate organization for the adequate management of compliance with this policy.

Control mechanisms for using inside information.

The Legal Manager, as authorised delegate of the General Manager, is responsible for the following:

- Making a List of people with access to privileged (insider) information as well as such updates thereof as may apply.
- Channelling the queries related to managing inside information made by the information users and provide that information to the Corporate Compliance Officer.
- Informing the Compliance Officer of the following:
  - ✓ The list of people with access to privileged (insider) information as well as such updates thereof as may apply.
  - ✓ Evidence that the Employees with access to privileged (insider) information have signed off on the Information Assets Management Policy as sign that they understand it.
  - ✓ Risks of failure to comply with the guidelines established herein.
  - ✓ Recommendations that, in his or her judgment, would be necessary to adopt in case of any undue use of insider information.

The Human Development and Management Manager is responsible for:

- Ensuring that the internal user signs a non-disclosure agreement when joining the Bank.

Each and every Employee is responsible for:

Control mechanisms for using inside information, Continued

- Notifying the General Manager about rumours or other non-official statements from the Bank, related to confidential information that includes: confidential analyses, financial information, data, business plans, as well as information received from Customers or third parties of which it is expected that it will remain confidential.

- Seek guidance from the Legal Manager in a situation that could be perceived as irregular or inappropriate.

The General Manager is responsible for:

- Announcing all of the Bank's important information through such internal or external channels as may deemed to be correct at the time. This includes, but is not limited to, information to financial news agencies and the press.

Each and every person with access to privileged information is responsible for:

- Complying with the restriction period assigned for privileged (insider) information to which he or she may have access in the course of their work. For Financial Statements, their restriction period starts at the day after the period-end closing until their publication, complying with the terms established thereto by current regulations in force.

Use of confidential information

- Abstaining from buying, selling or executing any operation related to the Bank's economic securities during the restriction period, whether in their own name, through an intermediary or by any third party to whom confidential or privileged (insider) information may have been disclosed. .

- Avoiding talking about the privileged (insider) information related to the Bank in public places.

- Follow the guidelines of this Policy, once becoming aware of insider information. Any doubt if the information known really is privileged information should be taken up with the Legal Manager as the General Manager's authorised delegate.

All Employees are responsible for:

- Treating the Privileged (Insider) Information as confidential and abstaining from talking about it with any other person who does not have the need to know such information for legitimate business purposes.

- Assuring the Bank's best interest by upholding the confidentiality of its business and operations, as well as the confidentiality of its Customers' information.

Use of confidential information, *Continued*	▪ Channelling the sending of any information to the Directors through the Vice-President / General Manager. In such cases as may so warrant it to be direct, then a prior review thereof should be requested from the Vice-President / General Manager and the latter should be copied when sending the E-mail or any other means of communication. ▪ Notifying the Legal Manager whenever they become aware that some insider information is being leaked to persons that should not know it.

Executors and General Responsibilities

Employees	▪ Reporting unofficial statements to the General manager, which are related to the confidential information of which they are aware, while seeking guidance about any situation that could be perceived as irregular or inappropriate.
General Manager	▪ Ensuring compliance with this Policy and be responsible for communicating any and all of the Bank's important information.
Legal Manager	▪ Keep the list of people with access to privileged (insider) information up-to-date and act as liaison for exchanging information with the Corporate Compliance Manager.
Human Development and Management	▪ Ensuring that the internal user signs a non-disclosure agreement when joining the Bank.
People with Access to Privileged (Insider) Information	▪ Assure good use of the privileged (insider) information that they have access to because of their work and abstain from using it for direct or indirect personal benefit or that of third parties.