ABOUT CABEI'S ETHICS

TITLE I

CODE OF ETHICS

CHAPTER I
GENERAL ASPECTS

Article 7-01. Purpose. The purpose of this Code is to establish the institutional principles, ethical values and standards of behavior that must be observed in the Central American Bank for Economic Integration, hereinafter called the Bank, which should encourage and guide the behavior of the Bank's staff.

Article 7-02. Scope of application. The institutional principles, ethical values and standards of behavior will be applied and generally observed at all hierarchical levels of the Bank, including members of the Young Professionals Program and any type of fellowship, interns or others. Likewise, these principles, values and standards of behavior will be required, as appropriate, for their compliance in the hiring of external consulting services, suppliers, contractors and others.

Article 7-03. Effectiveness of regulations in the framework of ethics. Compliance with the provisions of this Code will be taken into consideration for maintaining the staff's relationship with the Bank. In those cases in which the Bank is affected in its interests, assets or contractual obligations, as a result of the action or omission of a member of its staff that leads to non-compliance with the institutional principles, values and standards of behavior established in this Code, the sanctions that are contemplated in the norms and procedures complementary to this Code shall be applied in accordance with the provisions of Title II of this Book.

Article 7-04. Definitions.

Harassment: Any unsolicited verbal or physical conduct that interferes with the work environment or that has the purpose or effect of creating an intimidating, hostile or offensive work environment.

Workplace harassment: Those abusive, conscious and premeditated behaviors by a superior or whoever takes their place, which, carried out in a systematic and repetitive manner, violate the dignity or psychological or physical integrity to the detriment of a subordinate.

Sexual harassment: Those behaviors that involve any type of unwanted sexual proposal, request for sexual favors or other verbal or physical manifestation of a sexual, explicit or subtle nature.

Conflict of interest: Any situation in which a member of the Bank's staff has a personal interest (direct or indirect) in any Bank operation or activity that unduly influences their judgment, their decisions or actions at the Bank or its clients. . In other words, a person's private interests interfere or can be understood to interfere with their decision-making and with the fulfillment of their official functions. Direct personal interest is understood if it benefits the own staff member and indirect if conflict of interest situations benefit some of the relatives of the staff member (fourth degree of consanguinity and second degree of affinity) or someone with whom the employee has a close relationship with.

Dignity: Self-respect on how people behave.

Discrimination: Giving inferiority treatment to a person or group for reasons of race, nationality, gender, religion, age or any other personal condition.

Integrity: Straight, fair, faultless conduct.

Members of CABEI: Members of the Bank are the founding members or countries, the non-founding regional members or countries and the non-regional members or countries, as established in the Constitutive Agreement.

Staff members: Pursuant to the provisions of article 16 of the General Regulation of Human Resources Administration, which includes temporary staff for a work contract (contractors).

Hierarchical levels: All levels contemplated in the Bank's organization, including Board of Directors, Executive Presidency and Comptroller's Office.

CHAPTER II

INSTITUTIONAL PRINCIPLES, VALUES AND STANDARDS OF BEHAVIOR WITHIN THE FRAMEWORK OF ETHICS

Article 7-05. Institutional principles. The institutional principles that the Bank uses as a basis to appropriately meet its objectives and that should be considered as a guide in all the Bank's institutional actions are described below:

a) The fulfillment of its purpose and its institutional framework:

The Bank will act diligently in each of its operations, faithfully complying with its purpose, the Constitutive Agreement and its rules, regulations, resolutions and agreements that regulate the Bank.

The Bank will act diligently in order to protect the interest and equitable treatment of all the members of the Institution in the terms established in the Constitutive Agreement and in the corresponding regulations in such a way that it objectively and impartially meets its economic integration and economic and social development programs.

b) Customer service:

The Bank will serve its clients promptly, with dedication, transparency and professionalism, facilitating the management of operations and providing them with the information that allows them access to the Bank's services, in an environment of teamwork culture, as well as protection of your confidentiality and privacy.

c) Compliance with sources:

The Bank shall honor its commitments to the sources of funds, complying with the terms and conditions accepted in the loan contracts. Furthermore, the Bank must ensure that these commitments are consistent with the Bank's equity integrity, that they strengthen its participation in the international capital markets, as well as its institutional prestige.

The Bank shall observe compliance with the agreements and regulations that are in force in its relations with international and multilateral credit organizations and other institutions, maintaining and cultivating an image of an exceptional institution in the international arena.

d) Valuation of the Bank's human resources:

The Bank will foster an organizational climate conducive to its stability and the integral fulfillment of its staff members. Likewise, it must promote the synergy of work between the different areas, respect for human dignity and favor the growth and individual well-being of its members, effectively preventing any form of harassment or discrimination of any nature, including, but not limited to those of a labor and sexual nature by members of the staff or higher management bodies.

e) Culture of teamwork and cooperation:

The Bank, as an institution that works for the integration and development of its member countries, will promote a work environment that fosters the generation of a teamwork, respect and cooperation culture among its staff members.

f) Grounds for actions:

The Bank's actions will be carried out based exclusively on technical criteria and based on the highest standards of multilateral development banking, as well as the sound practices of the banking industry; the latter pursuant to the provisions of the Constitutive Agreement.

The Bank will not accept conditions of a political nature or that contravene the Bank's purpose from clients or sources of funds.

Article 7-06. Ethical values. Each member of the Bank's staff will behave, in all their relationships and activities, in accordance with the ethical values set forth below:

a) Fairness:

Each member of the Bank's staff shall observe a legal, ethical and fair behavior in all of its activities and operations under their responsibility, based in the veracity, honesty, rightfulness and excellence and shall behave with prudence in all of its behaviors, inside as well as outside of the Bank.

b) Transparency:

Each member of the Bank's staff will carry out its activities and communications with clarity, without doubt or ambiguity and without hiding or omitting any type of information. Likewise, they will behave with Independence, avoiding under all circumstances, from incurring in associated risks on situations that cause conflicts of interest, for themselves as well as for other members of the staff.

c) Loyalty and Confidentiality:

Each member of the Bank's staff shall behave and observe, under all circumstances, a behavior of commitment and loyalty or faithfulness towards the Institution, as well as towards its colleagues, fostering a positive institutional image in all of his/her behaviors, avoiding comments or actions that can cause damage to the Bank. Personal activities must be characterized by due discretion and confidentiality in the handling information and other matters of an institutional nature.

Article 7-07. Behavior Standards. Each member of the Bank's staff should behave, in his/her professional or personal grounds, in agreement to the following guidelines with the ethical framework:

a) Prevention of a conflict of interests:

Always, when a member of the Bank's staff has any direct or indirect interest in a certain active or passive operation or a topic that is submitted to the Bank's consideration, he/she shall publicly inform of such fact to the corresponding instances of analysis and approval and shall abstain from any process, knowledge or decision on this particular case.

To the purpose of this article, financial interest is understood as any right to receive interests, dividends, capital appreciation, fees or other payments or monetary benefits.

The latter in conformity to the policies in force about the matter.

b) Adequate use of privileges and immunities:

Staff members must make appropriate use of the immunities, exemptions and privileges that the Constitutive Agreement and other international instruments confer on the Bank since they are conferred in the interest of the latter and not for personal advantage.

c) Non-tolerance of harassment:

The Bank's staff members must provide, at all times, a work environment where harmony, dignity, decorum and respect prevail, so harassment will not occur under any circumstances in the Bank's work environment.

In view of the above, it is the responsibility of the Bank's staff members to take the necessary measures in order to prevent situations that may generate any type of harassment. The higher authorities will implement the necessary measures to prevent harassment situations, including the following:

i. Disseminate that disrespectful behavior and bullying will not be tolerated.

ii. Ensure that people raising concerns receive support and are not retaliated against.

iii. When necessary, bring complaints and concerns to the attention of the Ethics Office.

d) Refraining from retaliating:

The Bank's staff members must abstain directly or indirectly from exercising threats or actions that may be considered or interpreted as retaliation to the detriment of who has filed a complaint or who cooperates in the investigation thereof.

In this sense, the Bank's staff members should avoid promoting or carrying out situations aimed at exercising actions, measures or implying with acts or words the intention of causing damages as a retaliatory measure against the person, whether he or she is a member of the Bank. staff, customer or supplier, who reports or cooperate in good faith in the investigations of any complaint.

No authority in the Bank, regardless of rank, may exercise any action or measure against the person who has filed a complaint, nor may it promote acts or measures that may be interpreted as retaliation for filing a complaint against third parties.

e) Non-tolerance of prohibited practices:

The Bank's staff members must avoid, at all times, any act of fraud, corruption, as well as other prohibited practices, whose actions may harm the image and reputation of the Bank, in addition to affecting the trust of staff members, shareholders, suppliers, customers and, in general, the development of its operations, pursuant to the provisions of the policy regulating the matter.

f) Compliance with financial obligations:

The Bank's staff members must attend promptly and in due form to the financial obligations contracted, both internally and externally to the Bank, including the payment of loans and credit cards, among others, in order to avoid that, due to personal financial difficulties, actions that may affect the Institution are generated.

ANNEX IV

Integrity Provisions contained in Annex IV of the Framework Contract.

A. Counterparts and their Related Parties:

All natural or legal persons that provide CABEI with goods and/or services, whether as suppliers, contractors, consultants, (hereinafter all of the above will be listed in this document as "the supplier"), as well as any other similar condition, hereinafter referred to as Counterparts and their Related Parties, must abstain from carrying out any act or action that is framed or may be classified as a Prohibited Practice as established in the following section (B) of this Annex.

B. Prohibited Practices:

In view of the above, CABEI has established a Reporting Channel as the mechanism to report irregularities, as well as the commission of any Prohibited Practice, in the use of CABEI funds or the funds administered by CABEI.

For the purposes of this contract, the following are prohibited practices:

CABEI's staff involved in the procurement of goods and/or contracting of services, as well as natural persons and representatives, officers and employees of legal entities that participate as suppliers of said goods and services, must observe the highest ethical levels throughout the acquisition process or during the contractual execution phase. In this sense and without this list being exhaustive, the following shall be considered prohibited practices:

a) Bribery: Consists of the offer, supply, acceptance or direct or indirect request of anything of value in order to improperly influence the action or decision of the competent person of making decisions in the process of acquiring goods and services that CABEI is performing.

b) Fraudulent Practice: Any act or omission, including a misrepresentation of the facts, which misleads or seeks to mislead another person in order to obtain an improper benefit, financial or other.

c) Collusion: Consists of actions between bidders aimed at obtaining prices in any of the acquisition methods used by CABEI at artificial, non-competitive levels, capable of depriving other participants of the benefits of free and open competition.

d) Coercive Practice: It consists of threatening another person or the members of his/her family, to cause in his person, honor, or property a wrongdoing that constitutes a crime, in order to influence decisions during any of the acquisition or contracting processes or during the execution of the corresponding contract, whether the objective has been achieved or not.

The Bank will reject any award proposal if it is determined that the selected supplier has promoted or executed these practices and will be excluded from CABEI's procurement processes. Likewise, the Bank reserves the right to unilaterally terminate the contract without the need for any judicial or extrajudicial declaration in case it will be determined that the selected supplier has promoted or executed these practices.

C. Declarations and Obligations of Suppliers:

The suppliers shall expressly transfer to their Related Parties (contractors, subcontractors, suppliers, supervisors, bidders and the like), the declarations and obligations of this Annex to the contractual documentation that governs the relationship between the suppliers and their Related Parties, when it is related, either direct or indirect, with the contracting and supply of goods and services required by CABEI.

Suppliers' Particular Declarations:

Suppliers declare that:

a. They know CABEI's Reporting Channel as a mechanism to report irregularities or the execution of any Prohibited Practice in the use of CABEI's funds or funds administered by CABEI.

b. They will keep all documents and records related to activities contracted by CABEI for a period of up to seven (7) years, beginning from the end of this contract.

c. As of the date of signing this contract, no Prohibited Practices have been committed in its own or through related parties (officials, employees, representatives and agents) or as any other type of analogous relationship.

d. All the information presented is truthful and therefore has not misrepresented or concealed any fact during the selection, award or execution processes of this contract.

e. Neither they nor their agents, their staff, contractors, consultants, directors, officers or shareholders (a) have been disqualified or declared by an entity as noneligible for the award of contracts financed by any other entity, or (b) convicted of crimes related to Prohibited Practices by the competent authority.

f. None of its directors, officers or shareholders has been a director, officer or shareholder of an entity that (a) is disqualified or declared noneligible by any other entity, (b) or has been convicted of a crime related to Prohibited Practices by the competent authority.

Suppliers' Obligations:

The following are the suppliers' obligations:

a. Not incurring in any Prohibited Practice when supplying goods and/or contracting services that are required by CABEI wither with its own funds or with funds it manages.

b. Report, during the selection process and execution of the contract, through the Reporting Chanel, any irregularity or execution of any Prohibited Practice related with the contracting and supply of goods and/or contracting of services that are required by CABEI with its own funds or with funds it manages.

c. Grant unrestricted access to CABEI or its duly authorized representatives to visit or inspect the physical installations of suppliers that are in charge of carrying out works, goods or services that had been contracted either with CABEI's own funds or with funds it manages. Likewise, they will allow and facilitate carrying out interviews with their shareholders, directors, executives or employees of any status or salary ratio. In the same manner, they will allow access to physical and digital files related with such contracts and must provide all the collaboration and assistance that is deemed necessary, in order to adequately execute the expected activities, upon CABEI's discretion.

d. Take care within the term that is established in CABEI's communications, of the consultations related to any inquiry, inspection, audit or investigation coming from CABEI or from any other investigator, agent, auditor or consultant, properly appointed, either in writing, virtually or verbally, without any type of restriction.

Declarations and Obligations from the suppliers, as indicated in section C above, are truthful and will remain in force from the date this contract is signed, during its effective term and until the termination of the contract upon the Bank's satisfaction.

D. Audit and Investigation Process:

CABEI shall reserve its lawful right of executing the audit and investigation procedures.

E. List of Prohibited Counterparts:

CABEI can incorporate Suppliers and its Related Parties in the List of Prohibited Counterparts, that, for such effect, it has created. The temporary or permanent blockage in such list of Prohibited Counterparts, shall be determined case by case by CABEI.

This Annex is an integral part of this contract, and therefore the Supplier accepts each one of the provisions stipulated herein.

CABEI's Information Security Policy

"RESOLUTION No. DI-135/2012

THE BOARD OF DIRECTORS, WHEREAS:

That, pursuant to Article 15 of the Constitutive Agreement, the Board of Directors is the body responsible of the Bank's direction and among its competences is the definition of the Bank's operational policies.

That, in conformity to the Regulation of CABEI's Organization and Administration, it corresponds to the Board of Directors the approval and modification of the norms and policies that are required for the Bank's sound operation, among which are included those, that in regard to risk management, it must observe.

That the best international practices recommend the need of managing operational risks that are derived from the use of information technologies (IT).

That the Board of Directors, by means of Resolution No. DI-44/2008 adopted by the CobIT Model as the standard for managing the Bank's Information Technology Governance and consequently under such framework it approved the Information Security Policy.

That, as required by CobIT, it is deemed appropriate to periodically review and update the Information Security Policy, with the purpose of adjust it to new changes and practices related to this topic.

That based on the positive recommendation of the technical areas, the Executive Presidency has deemed appropriate to submit to the consideration of the Board of Directors the following resolution and to recommend its approval.

HEREBY RESOLVES:

FIRST: To ratify the CobIT framework of reference as the standard for the Bank's Information Technology Governance.

SECOND: To approve the following:

INFORMATION TECHNOLOGY (IT) POLICY OF THE CENTRAL AMERICAN BANK FOR ECONOMIC INTEGRATION

CHAPTER I

General Aspects

Article 1: Purpose.

The purpose of this Policy is establishing the principles and norms that must be applied at the Central American Bank for Economic Integration, hereinafter called "The Bank", when generating and using information, in such a way that the following basic principles are fulfilled:

i. Integrity: It refers to the preciseness and fullness of the information and methods for processing it.

ii. Confidentiality: It refers to how the information is made accessible only for those persons that have due authorization.

iii. Availability: It refers to how authorized users have access to the information when it is required.

In order to achieve the above, control measures to manage the Bank's information will be established. These controls cover persons, processes and IT, in conformity to international standards and best practices in this matter.

Article 2: Scope and Area of Application.

This Policy, together with the manuals and complementary procedures, shall be applicable and enforced within all the activities of the Bank.

Every staff member working at the Bank, as well as staff with contract relationships such as interns, young professionals, contracted personnel, practice students, third-party personnel or consultants, shall be subject to formally accepting to comply and perform according to this Policy.

The Bank's retired personnel, investors in certificates of deposits issued by the Bank, clients and suppliers that carry out transactions with the Bank using electronic means, shall be required to sign a document establishing the use and confidentiality agreements that the Bank determines, as established in the manual for the application of this Policy.

The scope of this Policy does not include or protect the principles of confidentiality, integrity and availability of equipment, services and email accounts or otherwise tangible and intangible assets owned by third parties, unless expressly stated in writing by the Bank and the owner.

Article 3: Definitions.

Assets: Any tangible or intangible asset that has value for the Bank.

Information Asset: Asset that contains Information in an intangible form, including, but not limited to digital data, databases, internally developed applications, intellectual property, documentation, backup copies, images or video; as well as physical assets in the form of technological infrastructure, including but not limited to equipment, servers, personal computers, mobile devices (laptops, tablets, smartphones, etc.), storage devices, communications equipment, or access control systems.

Threat: A potential cause of an unwanted incident, which can result in damage to a system or organization.

Technical Log: Electronic record of the states, events and actions that occur during the execution of a process, work or task. This log includes the relevant events that occurred during the performance of said task and the failures that occurred, without reference to the content of the information being processed.

Control: Ways of managing risk, including policies, procedures, guides, practices or organizational structures, which may be administrative, technical or legal in nature.

Information Custodian: Person to whom the functions and responsibilities have been delegated to manage, on behalf of the information owners, the access controls to the information.

Information Security Incident: An identified occurrence of a Bank-owned system, service or communications, indicating a possible failure that has a significant probability of threatening the Bank's operation or the security of the Bank's information.

Guide: Descriptive document of greater detail, which clarifies what must be done and how, to achieve the objectives established in the policies.

Information: Refers to all communication or representation of knowledge including textual, numerical, graphic, cartographic, oral or audiovisual forms and in any transmission or storage medium, whether printed, magnetic, optical, digital or audiovisual.

Information Processing Facilities: Physical site where any centralized information processing system, service or infrastructure is housed.

Implementation Manual: Descriptive document of greater detail, which clarifies what should be done and how, to achieve the objectives established in the policies.

Responsible for the Information: Person or user of a role that creates or originates information assets that must be protected. He/she has ultimate responsibility for classifying access levels, granting access authorizations, and periodically reviewing access levels.

As a general rule, those responsible for the information will be the heads of each branch of the Bank, unless a specific person is appointed for that function.

Risk: It is the combination of the probability of occurrence of an event and its consequences.

File Records: Information created or received, kept as information and evidence in the development of the Bank's activities or by virtue of its legal obligations.

Information Security: The safeguard of the confidentiality, integrity and availability of the Information.

Physical Security: The safeguarding of information through the establishment of secure areas, protected by a defined security perimeter, with appropriate security barriers and income and expenditure controls.

Information Security Management System: It is a systematic approach to manage sensitive information of the organization, in such a way that it is kept safe, involving people, processes and information technology systems.

Information User: Person or user of a role that uses information assets, created by others, to perform their functions.

Vulnerability: A weakness in an asset or group of assets that can be exploited by a Threat.

Article 4: Revision of the Policy.

This Policy will be reviewed and updated periodically, as part of a continuous and feedback process that observes awareness, methods of access to information, monitoring compliance and acceptance of the guidelines and the implementation strategy at all levels. from the bank.

Article 5: Responsibilities to the Information Security Administration System.

The main responsibilities for the proper management of the Information Security Administration System are established, as follows:

a) Corresponds to the Bank's Board of Directors:

i. Approve the Information Security Policy, its updates and modifications.

ii. Authorize the necessary resources to maintain the security of the Information.

b) It corresponds to the Finance and Risk Committee:

i. Analyze and propose to the Board the approval of the Information Security Policy.

ii. Analyze and propose to the Board of Directors the authorization of the resources necessary to maintain the security of the Information.

c) It corresponds to the Executive Presidency:

i. Coordinate initiatives related to the topic of Information security.

ii. Periodically, review and raise awareness and approval of the Finance and Risk Committee of the changes in the Information Security Policy, to ensure that it remains in force and effective.

d) It corresponds to the Operations and Technology Division:

i. Manage the resources necessary to maintain the security of the Information.

ii. Propose the modifications that correspond to the Information Security Policy, as well as the procedures and activities related to said Policy.

iii. Design and implement the necessary and adequate mechanisms for the dissemination and knowledge of this Policy at all levels of the Institution, as well as to individuals and entities related to the Bank.

iv. Develop and implement the procedures, manuals and activities necessary to incorporate into the Bank's operations and processes that related to the security of the information generated and processed.

v. Develop and implement the procedures and activities necessary to incorporate into the Bank's operations and processes that related to physical security and the preservation of physical and electronic file records.

e) It corresponds to the Bank’s staff, to the Person Responsible for the information and the information user:

i. Produce, safeguard and make appropriate, confidential and responsible use of the Bank’s Information, in accordance with the provisions of this Policy and in the procedures, manuals and associated activities.

CHAPTER II

Norms for the Application of this Policy

Article 6: Confidentiality and Information Property Rights Provisions.

The officers and employees of the Bank, by their sole condition as such, are subject to compliance with the duty of confidentiality with respect to all the information owned by the Bank that becomes their knowledge, or that they themselves generate during their employment relationship, except for that information that is generally available and is in the public domain and knowledge (that is not the result of disclosure by officials and/or employees in infringement of the provisions of this Policy). The obligation of information confidentiality will subsist after the relationship between the Bank and the person has ended.

By definition, all the information to which an employee or official has access during their employment relationship is considered the property of the Bank. Said information includes, but is not limited to, all information internally generated, processed, transformed, edited or any other similar activity of creation, transformation or consultation and the information legally acquired or transferred voluntarily by any counterpart with which the Bank has relations.

Even if material property is considered, Bank's staff must take into account and is obliged to respect the intellectual property rights of third parties or other rights incorporated into simple physical property.

Article 7: Access to Information Assets.

The Operations and Technology Division will be responsible for establishing the basic information assets that must be granted to each of the subjects obligated to comply with this Policy (permanent employees, young professionals, contractors or any other category of human resource).

The access granted to other information assets, in addition to the basic ones, must be rational in terms of cost and security and will be authorized by those responsible for the information, limited exclusively to those information assets necessary to carry out official duties.

In order to safeguard the principles of this Policy, the Operations and Technology Division shall ensure the conservation and monitoring of technical logs and file records at a general level and specifically, in order to ensure the reliability of the information, as well as monitoring and analyzing activities or transactions.

For technical purposes for the maintenance, backup, update, support or other similar activities, the custodians of the information will have access to all the information assets, except those whose access has been expressly established by the Board of Directors.

The custodians of the information and the supervisory bodies of CABEI may have access to the content of the official email accounts of employees and the information contained in the final user equipment, in those cases that are fully justified because of actual or potential risks to CABEI. The Executive President will give the respective authorization.

Access to the content of official email accounts, final user equipment, as well as any other communication or representation of knowledge, including textual, numerical, graphic, cartographic, oral or audiovisual forms and in any transmission or storage means, either printed, magnetic, optical, digital or audiovisual, whose Information officers are part of the staff of the Board of Directors and of CABEI's control bodies, may be carried out exclusively with the approval of the Board of Directors.

Access restrictions do not apply if the request is made for technical support purposes and comes from the Data Controller for access to assets under their responsibility or from the person who is assigned with final user equipment.

In the event of potential risks or security events, the Bank reserves the right, and the subjects bound by this Policy consent to access, to review final-user equipment owned by individuals that the subjects bound by this Policy use in the performance of their official duties.

Article 8: Technological Resources Use and Administration.

The Operations and Technology Division will be the unit in charge of the administration of the Bank's technological platform, which includes the computer equipment, applications and communications equipment.

To this end, the Operations and Technology Division shall establish procedures, protection mechanisms, inventories and activities aimed at managing and controlling the elements that are part of the technological infrastructure, in order to be used in an adequate security environment, technical standards and availability, aligned to the best practices in this matter.

Likewise, any acquisition, installation or update of the Information Assets that make up the Bank's technological platform must be authorized by the Operations and Technology Division through the Technology Sub-Division Office and its dependencies, as appropriate.

Article 9: Control and Classification of the Information.

All information owned by the Bank, regardless of the means in which it is located, prepared or distributed, must be managed in a confidential environment, in accordance with the provisions of article 6 of this Policy.

The Information is classified according to the following model:

i. Institutional Public Information: This is information owned by the Bank that, unilaterally and in order to suit its interests and needs, CABEI publishes or disseminates to the general public or to a specific population. This information, although it is not confidential, prior to its initial issuance, must be reviewed, approved and published by the corresponding instances, depending on each case.

ii. Public Information with Counterparts: It is the one which CABEI must administer (know, deliver, exchange, notify) in the course of its interaction with counterparts, for the development of its active, passive operations, services rendered, contracting of goods and services, administrative procedures, personnel recruitment and, in general, any activity with third parties that is necessary for CABEI's operation.

Although it is public information, it is confidential since it should only be known to the interested counterpart. If necessary, specific confidentiality agreements should be established, in matters that the parties agree on.

The delivery of information owned by CABEI due to judicial requests, requests from public law enforcement entities or similar instances, shall be analyzed by the Legal Counsel Office and approved by the Executive President.

iii. Internal Institutional Information: Is that information that is generated, received or processed in CABEI for the development of all internal institutional activities.

Internal Institutional Information can be classified as confidential, in which case it can only be known by the user or group of users determined by the Data Controller.

If necessary, for the development of their functions at CABEI, the Information Managers may share with third parties, in addition to those described in numbers 1 and 2 above, the Internal Institutional Information that is not confidential or restricted, being under their responsibility how it is used.

iv. Restricted Information: It is the information which dissemination is restricted to one person or a group of people and can only be accessed in the manner and by the group of users that is determined pursuant to the specific policies and norms that are established in each case.

The Governors, the Directors, the Controller and the Internal Auditor will have access to all the information required for the fulfillment of their functions related to the Bank, observing the particular provisions of the restricted information.

Specific activities for the administration of institutional information will be established in the complementary manual.

The information will be classified by the Information User at the time of disclosure, according to levels of importance, sensitivity and criticality. If the information must be known by subjects not bound by the Policy, the transfer is the responsibility of the Information User. However, the Information User may not share that information classified as confidential or restricted, without first obtaining the authorization of the Information Manager, in accordance with the terms of this Policy and its supplementary manual.

Article 10: Physical Security of the Information Assets.

The physical security administration of the Bank's facilities is in charge of the Operations and Technology Division.

Any relevant change in the physical structure of the Bank's facilities must have the approval of the Operations and Technology Division, which must validate that the Bank's security is maintained.

The Operations and Technology Division shall establish protection mechanisms, as well as control procedures and activities aimed at reasonably protecting the assets owned by the Bank, in order to avoid unauthorized access, loss, damage or theft. Likewise, procedures will be established for the operation and maintenance of physical facilities.

Article 11: Periodic Security Revisions.

Given the rapidity with which, in the technological context, new information security threats are generated, the Operations

and Technology Division will annually conduct security reviews supported by firms or by specialized third parties in order to detect and control new threats that attempt against the Bank's Information Assets and to ensure the effectiveness of all the controls implemented at the physical and logical level to safeguard the Information Assets..

Article 12: Access Control to the Information Systems.

The Operations and Technology Division will establish procedures and manuals in order to control the assignment of access rights to information systems and services.

The Human Resources Office must promptly notify the Technology Department of any new personnel that originates the creation, modification or cancellation of access privileges for any user, in order for said agency to make the necessary changes to the technology platform.

A unique, personal and non-transferable identification will be assigned to each Information User that requires, due to their functions, to have access to the Bank's technological platform. This identification will be assigned and revoked in accordance with what is established in the Application Manual of this Policy, which will also establish the technical parameters of this identification.

Article 13: Retention and Conservation of File Records.

Information that is property of the Bank must be preserved to support future activities and decision-making, according to its degree of importance.

The management of filed records will be the responsibility of the Operations and Technology Division, which must maintain adequate administration for the registration, filing, classification, preservation and destruction of them, taking into account the obsolescence and technological limitations of both application systems such as technological infrastructure.

Information Users are responsible for the content of the personal computers assigned to them, following the technical instructions established by the Operations and Technology Division.

Article 14: Internet Use and Electronic Mail.

Access to the Internet is provided to Information users to help them with their duties. In this sense, the use of available resources in the Internet must be framed within the acceptable internet use guidelines, described in the Manual for the application of this Policy.

All information transmitted, received, processed, stored, and generally managed through institutional email is the property of the Bank. Institutional email is provided to information users as a support tool for the development of the Institution's business, administrative and technical operations, so its use must be framed within the guidelines for the acceptable use of email, described in the application manual of this Policy.

Article 15: Systems Development and Maintenance.

The information security administration, during the life cycle of the Bank's application systems, is the responsibility of the Operations and Technology Division, through the Applications Department, being of particular importance to have procedures and specifications for the following: i) identification of automated solutions, ii) change management, iii) data management, iv) version control, v) administration of the relationship with third parties and vi) technical and end-user documentation.

The Bank must have its own methodology for the acquisition, development and maintenance of applications, regardless of whether such tasks are carried out internally or on an outsourced basis. The development and updating of this methodology will be under the responsibility of the Operations and Technology Division.

To ensure the development and implementation of applications, there must be a separate processing infrastructure to have production, development and testing environments, and must have formal procedures and segregation of functions to carry out the transfer of software from the state. from development to production status in an interactive cycle.

Article 16: Business Continuity.

The Bank will have an Institutional Business Continuity Plan, based on a Continuity Strategy, which includes controls to identify and reduce risks, limit the consequences of incidents and ensure the timely resumption of operations essential for business continuity, with the support of an alternate technological platform. Said plan, as well as the management of budgetary resources for its maintenance, will be administered by the Risk Division, with the coordination of the Business Continuity Committee (BCP Committee).

The Operations and Technology Division will be responsible for maintaining a Disaster Recovery Plan for the Technology Platform, which will allow the critical applications, computer systems and communications to be restored in the time required to ensure business continuity.

The Executive Presidency will report annually to the Board of Directors the results of the tests of the Business Continuity Plan and the Disaster Recovery Plan.

Article 17: Security Incidents Reports.

Information users should report to the Operations and Technology Division in regard to incidents that result in a real or potential threat to information security, including loss or theft of equipment or storage media, virus attacks or other events.

The Operations and Technology Division will keep records and statistics of events that affect the security of information, such as attack attempts, inoperativeness of production systems and applications, discontinuation of services, data alteration or other security events.

Article 18: Implementation of this Policy.

It is the responsibility of the Executive Presidency to approve and publicize all the mechanisms necessary to implement this Policy, through the manuals, procedures, guides and guidelines it deems necessary, in order for all information users to know and apply this Policy. .

CHAPTER III

Additional Provisions Article 19: Legal

Actions

CABEI reserves the right to take the appropriate legal actions in case of violations of the provisions of this Policy that result in financial losses or damage of any kind.

Article 20: Disciplinary Actions.

Disciplinary actions for non-compliance to the provisions in this Policy, in its regulations and in the complementary procedures approved by the Executive Presidency, will be processed in accordance with the provisions of the General Regulation for Human Resources Administration and the Manual of Standards of Conduct. or in the Code of Ethics, depending on the type of offense.

THIRD: To annul Resolution No. DI-44/2008.

FOURTH: Instruct the Executive Presidency so that, within a period of two (2) months, is enforces the Manual for the Application of CABEI's Information Security Policy.

FIFTH: This resolution shall enter into force from the date of its approval". It is in conformity with its

original, with which it was duly proofread.

Tegucigalpa, Municipality of the Central District, November twenty two thousand twelve.

Money Laundering Prevention Policy of the Bank

RESOLUTION No. DI-57/2004

THE BOARD OF DIRECTORS, WHEREAS:

That, in accordance with Article 15 of the Bank's Constitutive Agreement, the Board of Directors is empowered to define the Institution's operational and administrative policies.

That, in accordance with the conclusions and recommendations of the diagnosis made by the Bank's Internal Audit on the risk of money laundering, it is necessary to issue a Money Laundering Prevention Policy.

That the Bank's Board of Directors and Administration consider it appropriate to adopt rules and principles aimed at preventing money laundering within the Institution.

HEREBY RESOLVES:

FIRST: To approve the following:

POLICY FOR THE PREVENTION OF MONEY LAUNDERING OF THE CENTRAL AMERICAN BANK OF ECONOMIC INTEGRATION

CHAPTER I
GENERAL FEATURES

Article 1: Purpose
The purpose of this policy is to establish the principles and regulations that shall be applied and generally observed at all levels of the Bank to prevent the Bank from being used as a means for money laundering, considering that it is essential to generate an institutional culture oriented to the application of norms and procedures for the prevention and detection of money laundering with good judgment, responsibility, common sense, prudence and opportunity.

Article 2: Application of this Policy
This policy, together with the Procedures Manual that is prepared, must be applied and observed in all active, passive, and acquisition of goods and services operations in which the Bank interacts or is a counterpart to another natural or legal person.

In those cases in which the Bank is affected by its interests, assets or contractual obligations, as a result of the action or omission of a member of its staff that leads to non-compliance with the principles and rules stipulated in this policy, the corresponding sanctions will be applied according to the Human Resources Administration Manual, without prejudice to the corresponding legal responsibility.

CHAPTER II

BASIC PRINCIPLES

Article 3: Special Conditions

The basic principles that will govern the conduct of the Bank's officials regarding the Money Laundering Prevention Policy in the Bank are the following:

a) Strictly abide by compliance with the mechanisms of control and prevention of criminal activities contemplated in the procedures manuals, which are defined for this purpose in the Comprehensive System for the Prevention of Money Laundering.

b) Observe due diligence regarding the client's knowledge in accordance with the respective Procedures Manual.

c) Refrain from recommending or, where appropriate, approving any active, passive or service operation when there is reasonable doubt about the lawful origin of the resources and assets of the counterpart or third parties with which the Bank maintains commercial or other relationships. nature. In these cases, the respective hierarchical superior must be informed of the suspicions and the elements of conviction on which such suspicions are based.

d) Keep due confidentiality in relation to the information provided by customers, as well as the records and documents related to the respective transactions in accordance with the Bank's policy that regulates the matter.

CHAPTER III

NORMS FOR THE APPLICATION OF THIS POLICY

Article 4: General Provision

The general provisions for the prevention of money laundering are the following:

4.1) Compliance with policies

All staff will rigorously apply this policy, in order to ensure full transparency and validity in the development of the Bank's business and operations.

4.2) Adoption of prevention procedures of international groups and the laws of member countries

The Bank and all its personnel will act according to the guidelines established in the Procedures Manual, which will contain the international recommendations on the prevention of money laundering and will duly comply with the legislation on the prevention of money laundering. establish the authorities of the countries where it operates, as well as the international recommendations of the Financial Action Group (FATF) and the Basel Committee.

4.3) Customer Knowledge

The Bank and all its personnel must endeavor to have as much knowledge as possible about its clients, individuals and legal entities, including the knowledge of its majority partners and their business and professional activities, as well as related companies or control groups, in order to implement an effective customer awareness policy.

4.3.1) Customers' Activity

The Bank's Administration will adopt a Procedures Manual in order to implement a "customer awareness" policy, considering, among others, the following aspects:

a) The criteria for the customer or client selection with whom the Bank wishes to carry out operations and the information requirements that allow its knowledge must be specified.

b) The Bank will only carry out operations with people or companies from which it has received sufficient information to enable it to know about its activity and the origin of its resources and that of its main shareholders.

c) The Bank will refrain from carrying out any type of operation with potential clients about whom it has reasonable doubt in regard to the origin of its resources or who refrain from supplying the requested information.

d) The Bank will exercise due diligence on clients that carry out high risk activities or activities susceptible to money laundering, in accordance with international recommendations, especially from the Basel Committee.

4.3.2) Control and monitoring of clients' operations

The Administration must carry out a permanent supervision and control of the activities with the clients or third parties involved, in such a way that the reasonableness between the operations it carries out and the activity and information they provide is established.

Bank officials and employees have the duty to immediately inform their superiors and the Compliance Officer when unusual or suspicious transactions of clients are identified, in accordance with the provisions of the Manual of Specific Procedures for the prevention of money laundering.

Officials and other personnel who have a direct or indirect relationship with clients are obliged to apply the control measures and specific procedures outlined in the Procedures Manual for the Prevention of Money Laundering.

4.4) Risk Management and Compliance Verification

The Bank's Administration must adopt a risk management system of money laundering and compliance verification. For these purposes, the Executive President will integrate an "ad-hoc" Committee on Money Laundering Prevention and will designate a Compliance Officer who will administer and monitor the Comprehensive System for the Prevention of Money Laundering, informing the Bank's Board of Directors of such appointment.

4.5) Collaboration with the authorities

The Bank shall provide, pursuant to its Constitutive Agreement and the regulations norming its activity on this matter, every collaboration to the legal, tax, and banking authorities or of any other nature, so that they can take timely and efficient actions in suppressing a money laundering crime.

4.6) Conservation of supporting documents of the operations

The Bank will consider the conservation of all documents, with the corresponding safety measures, related with money laundering prevention, for up to a period of seven years.

4.1) Knowledge of suppliers

The Bank shall not acquire goods or services from persons or companies where there is evidence to make it doubt the legality of the operations or legality of its resources or where individuals and companies are included in the international lists of criminals and terrorists. In addition, the Bank will refrain from trading when the supplier refuses to provide the information required by the Bank.

The Bank shall only enter into a business relation with a supplier after successfully verifying its identity and that of its main partners.

SECOND: This policy shall enter into force from this date and annuls any resolution, agreement or provision of equal or lesser rank that opposes or contradicts it".

It is in conformity with its original, with which it was duly proofread.