



ZUMABANK

CODE OF CONDUCT

INTRODUCTION

In compliance with the ethical and moral principles that govern its business activity, Zuma Bank insures that the behavior of its Board of Directors, its Executives and Employees is governed by a correct, honorable, and totally transparent behavior in order to protect the trust placed by its clients and users. In order that it may meet this goal the Code of Conduct contains values, principles and minimum behavior regulations that must be observed in all operations processed by the Bank.

This code is a formal invitation to promote and reinforce the obligation to maintain a positive behavior, perform activities correctly, and insure that the Zuma Bank philosophy is fully understood. Therefore, it is mandatory that each and every one of the members of the Board of Directors, the Executives and the Employees in general place the observance of ethical and moral principles first and foremost before the achievement of any personal interest.

The facts or omissions referred to in the legal provisions that appear in this document are deemed as serious transgressions that allow Zuma Bank to terminate the work contract with just cause, in compliance with the Law and the Internal Work Regulation.

Sincerely,

President
Zuma Bank



ZUMABANK

CHAPTER I

GENERAL PROVISIONS

Article 1.- OBJECTIVE

Insofar as money laundering and the financing of terrorism, the objective of the Code of Conduct, hereinafter the Code of Conduct, is to establish the minimum bases of responsible behavior, as well as the principles, duties and ethical norms that the Board of Directors, the Executives and the Employees of Zuma Bank in general, shall become familiar with and comply for the satisfactory compliance with the prevention policies of money laundering and the financing of terrorism.

Article 2.- SCOPE

The Code of Conduct is applicable to the Board of Directors, the Executives and the Employees of Zuma Bank. It is also applicable to its suppliers, contractors and part-time employees, in compliance with the definition of the Code of Conduct herein.

Article 3.- COMMUNICATION

Zuma Bank, as a regulated entity, is obligated to communicate the laws, norms, internal provisions, policy manual and all information that it may consider relevant in the matter of prevention of money laundering and the financing of terrorism, to its Board of Directors, the Executives and the Employees in general, as they pertain to each one. Moreover, it shall deliver to each one a copy of the Code of Conduct, approved by the Board of Directors, in compliance with the norms that govern the matter, in order to facilitate their compliance.

The adequate communication of the Code of Conduct shall be supported by a signed acknowledgment and sworn statement of this document.

Article 4.- TERMINOLOGY

For purposes of application of the Code of Conduct, the following terms shall be used:

- a) Back Office: area of accounting records of treasury operations.
- b) End beneficiary: natural person in whose benefit a transaction is performed and/or who holds or exercises the effective final control over a client, a company or any other type of legal structure.
- c) Clients: are natural persons or companies with whom the bank establishes and/or maintains a legal or contractual relationship for the provision of any product inherent to its activity or for rendering a service.



ZUMABANK

- d) Employee: natural person who maintains a work or contractual relationship with the Bank, including the Bank executives.
- e) Financing of terrorism: any form of economic action, aid or mediation that may provide financial support to the activities of terrorist elements or groups.
- f) Front Office: Treasury Business area.
- g) LA/FT: money laundering and the financing of terrorism.
- h) Money laundering: to hide or conceal the nature, origin, location, property or control of money and/or assets obtained illegally.
- i) Manual: manual for the prevention of money laundering or the financing of terrorism.
- j) Compliance Official: employee in charge of directing all policies on the prevention and control of money laundering and the financing of terrorism adopted by the Bank.
- k) Unusual operations: operations in which the amounts, characteristics and their recurrence have no relation to the economic activity declared by the client at the time of its dealings with the Bank.
- l) Suspicious operations: operations in which the amounts, characteristics or their recurrence have no relation to the economic activity of the client; or transactions performed by users who, by their number, the amounts transacted or the specific characteristics, lead to a reasonable suspicion that the Bank is being used to transfer, manage, take advantage or invest resources of illegitimate origin or destined to the financing of terrorist actions.
- m) Regulated entity: natural person or company obligated to implement a system of policies and procedures to prevent money laundering and the financing of terrorism.
- n) UAF: Financial Analysis Department
- o) User: natural person or company that uses the Bank services without a contractual relationship.



ZUMABANK

CHAPTER II

ON THE PRINCIPLES AND ETHICAL DUTIES

Article 5.- ETHICAL PRINCIPLES

5.1 Zuma Bank, its Board of Directors, Executives and Employees shall act, in the development of its activities and functions, under the following principles:

5.1.1 Respect for and suitability of the norms

Complying with the norms that regulate the exercise of their activities, adapting their behavior in terms of respect toward the people, the Laws and the legislation in force in the matter of money laundering and the financing of terrorism, as well as the current Code of Conduct and the Policy Manual on the prevention of money laundering and the financing of terrorism.

5.1.2 Integrity

Exercising their functions with responsibility, acting with integrity, honesty and rectitude with the objective, at all times, that the Bank not be used in activities of money laundering and the financing of terrorism.

5.1.3 Confidentiality

Guaranteeing the strict confidentiality of client information, respecting the responsibilities assigned them by the Law, as well as in every matter related to suspicious operations reports (ROS) that they communicate to the Financial Intelligence Department of Dominica.

5.1.4 Fairness

Acting with justice and mutual respect in internal relations and with clients, with public and private entities, as well as with the supervising entity.

5.1.5 Suitability

Guaranteeing the technical and moral suitability in the development of commercial activities, taking advantage of the opportunities for training for the due compliance of the functions, especially in the matter of prevention and control of money laundering and the financing of terrorism.

5.1.6 Objectivity

Evaluating objectively the information in their custody or available to them in order to detect unusual and suspicious operations and, wherever applicable, issue the corresponding reports, proving independence in their relation with persons and entities.



5.1.7 Veracity

Expressing themselves with the truth in the exercise of their commercial activities and the compliance of their functions, as well as with their clients, suppliers and third parties.

Article 6.- ESSENTIAL DUTIES

6.1 The Bank, its Executives and Employees shall comply with the duties established in the Law, its regulations and all applicable norms, with a special effort in:

6.1.1 Duty to Inform

Pay special attention to the detection of unusual operations and the prevention or detection of suspicious operations and inform the Financial Intelligence Department of Dominica in a suspicious operations report (ROS) when applicable, according to its policies and other applicable provisions on the matter.

6.1.2 Record Duty

Record all operations performed by the clients, without exception, in a precise, complete and chronological manner, according to the policies on the prevention and control of money laundering and the financing of terrorism, keeping them on file for the specified legal term and making them available to the competent authorities.

6.1.3 Confidentiality Duty

Under the responsibility of the Bank and its employees, it is banned to inform any person or entity, in any manner or modality, of the fact that information has been requested of the Financial Intelligence Department or that information has been received in compliance with the Law, unless it has been requested by the jurisdictional entity or competent authority, pursuant to the regulations in force.

The Bank shall adopt measures destined to support its employees in the development of their functions and the objective of complying with internal policies and the norms in force.

In compliance with the duties issued by the norms in force, the Bank shall adopt measures related to the following aspects:

6.1.4 Due diligence regarding information on the client:

- a. Identify fully and beyond any doubt, any client that may request a service or the provision of any good or product inherent to the commercial activity of the Bank, whether the person is a natural person or a company, request an appropriate identity document and verify it according to the internal policies of the Bank.
- b. The Bank shall also use the means it may deem pertinent in the verification of the identity of said natural persons or companies.
- c. Be aware of any changes in the regular behavior of the clients that may allow to detect significant changes in the normal operations in order to perform the analysis and evaluation pursuant to the regulations in force.



ZUMABANK

- d. Identify the end beneficiary and adopt reasonable measures to verify his identity, in order to be certain of the identity of said end beneficiary. As for companies, determine the natural persons who, in the end, have the control through the property, or the person or company who holds the control through other means. Only in the event that it has been impossible to identify a natural person, shall the person who exercises the functions of direction and/or management be considered.
 - e. In the event that, as a result of the aforementioned actions, an operation is identified as suspect, the corresponding report shall be issued to the Financial Intelligence Department.
- 6.1.5 On knowledge of the employee
- a. Insure that the employees have a high level of integrity.
 - b. Collect information on personal, work and patrimonial background of the worker consisting of his/her personal information, which shall be updated in order to guarantee the transparency of the information supplied. The information shall be updated as needed and shall be available to external authorities or auditors.
- 6.1.6 On preventive policies in terms of money laundering and the financing of terrorism
- a. Designate a Compliance Official who has the requisites necessary to occupy this position.
 - b. Identify warning signs and typologies of money laundering and the financing of terrorism and spread them among the employees, keeping them informed and aware of the risks that a permissive behavior may pose for the Bank.
 - c. Train employees at least once a year in the matter of prevention and control of money laundering and the financing of terrorism.
 - d. Be familiar with the legal framework in force regarding the prevention of money laundering and the financing of terrorism, and spread current updates among the employees.



ZUMABANK

CHAPTER III

NONCOMPLIANCE OF PROVISIONS OF THE CODE OF CONDUCT AND THE DISCIPLINARY MEASURES

Article 7.- NONCOMPLIANCE OF PROVISIONS OF THE CODE OF CONDUCT AND THE DISCIPLINARY MEASURES

Noncompliance of the provisions of the Code of Conduct is punishable by the Bank, pursuant to provisions in the Internal Regulations. The following constitute punishable infractions when incurred by employees:

- a) Failure to sign the acknowledgment and sworn statement of the Manual and the Code of Conduct for the prevention of money laundering and the financing of terrorism.
- b) Failure to comply with the procedures stated in the internal manuals established by the Bank in the matter of prevention of money laundering and the financing of terrorism.
- c) Failure to comply or violate the procedures, guides and guidelines established by the Bank in the matter of identification of clients.
- d) Unjustified failure to attend programmed sessions in the matter of prevention of money laundering and the financing of terrorism summoned by the Compliance Official.
- e) Hinder or attempt to prevent the work of the authorities in the supervisory visits.
- f) Violate confidentiality and divulge to any person or entity, by any means or modality, the fact that an information has been requested by the authorities.
- g) Failure to communicate to the Compliance Official of a possible suspicious operation of a client.

The Bank shall assess these violations of its internal regulations, should that be the case, according to their seriousness, whether they are light, serious or very serious, for purposes of imposing the corresponding sanction. The noncompliance resulting from a random event or caused by a duly documented *force majeure*, does not constitute a violation.