بنك البلاد
Bank Albilad

Code of Principles and Rules of Professional and Ethical Conduct

4th Update, September 2022

Version No.	5 (4th Update)
Release Date	10/09/ 2022
Document Status	Approved

Contents

	Topics	Page No.
1	Introduction	3
1-1	Objectives of the Code of Principles and Rules of Professional and Ethical Conduct	3
1-2	Scope of Application and Approval.	4
1-3	Definitions	
2	Key Principles / Rules of Professional and Ethical Conduct:	5
2-1	Compliance with professional conduct and public morals.	5
2-2	Interaction with stakeholders.	5
2-3	Combating Financial Crimes and Financial and Administrative Corruption	6
2-3-1	Combating Money Laundering and Terrorist Financing Crimes and Suspicious Transactions	6
2-3-2	Combating Fraud, Corruption and Bribery.	7
2-3-2-1	Combating Fraud	7
2-3-2-2	2-3-2-2 Combating Corruption and Bribery.	7
2-4	Dealing with gifts and hospitality.	8
2-5	Compliance with Laws, Regulations, Instructions and Policies	9
2-6	Dealing with Conflicts of Interest	9
2-7	Confidentiality and Disclosure Mechanisms	9
2-7-1	Classification of Bank Information.	9
2-7-2	Classification of Confidentiality	10
2-7-3	Duties of Bank Employees.	12
2-8	Compliance with the Sharia Committee Decisions.	14
2-9	Social Responsibility.	14
2-10	Whistleblowing	14
2-11	Remuneration and Compensation	14
3	Consequences of Non-Compliance with the Principles and Rules of Professional and Ethical Conduct.	19
4	Final General Rules and Provisions:	19
5	Amending, Updating and Developing Code of Principles and Rules of Professional and Ethical Conduct.	19
6	Policies and Documents Related to the Bank's Code of Principles and Rules of Professional and Ethical Conduct.	19
7	Declaration of Compliance with the Code of Principles and Rules of Professional and Ethical Conduct	21

1. Introduction

The Bank continuously seeks to apply the banking principles and values derived from the provisions of Islamic Sharia. It complies with the rules, regulations and instructions of regulators, such as the Central Bank of Saudi Arabia and the Capital Market Authority to enhance its reputation and brand. It also applies the best standards and highest rules of professional conduct and ethics to serve the bank's customers and to ensure the provision of the best banking and financial services.

The principles of trust, responsibility, honesty and respect are essential elements and basic building blocks in the formation of the reputation and trust that the Bank has built and seeks to strengthen as a basic source of the value that the Bank provides to its customers and the obligations that it has placed on itself towards all stakeholders, in order to preserve the values and principles of the Bank. This is not achieved unless all the Bank's employees perform their personal and professional work in a manner that preserves the respect and dignity of others, reflects the best image of the Bank and its employees, safeguards its reputation, and avoids any harm as a result of any improper behavior inside or outside the Bank, or inside and outside the Kingdom.

1-1 Objectives of the Code of Principles and Rules of Professional and Ethical Conduct:

To make the performance of the bank's employees within a framework of a system of ethical values and principles in a way that achieves professional discipline, integrity, transparency, objectivity, efficiency, loyalty and effectiveness in the behavior of the bank's employees in performing their duties and job tasks.

1-1-1 To emphasize the contribution of these behavioral and ethical principles/rules to achieving the bank's vision and mission, protecting its reputation, ensuring that its employees comply with the principles of prudent behavior, realizing the concept of rational management, enhancing job performance and professional conduct of its employees, rewarding the hardworking, holding the negligent accountable, and improving the bank's image in general.

1-1-2 To turn these principles and rules into behavior and practices to be applied by the Bank's employees as a reference tool that draws the basic rules that guide them on how to deal with each other when performing their job duties and the qualities that they must possess.

1-1-3 To determine the professional and ethical standards to be followed by all employees of the bank.

1-1-4 To emphasize the commitment of all bank employees to the highest behavioral, professional and ethical standards such as honesty, integrity and responsibility.

1-1-5 To help in identifying ethical and behavioral problems and ways to address them.

1-1-6 To encourage all the Bank's employees to take responsibility for their actions and act not only in accordance with the provisions, regulations or legal rules, but rather they must take care to implement the spirit of these regulations and rules, and to adhere to integrity, impartiality, clarity and transparency when making decisions or performing their roles.

1-2 Scope of Application and Approval.

These rules, in accordance with the relevant regulations and instructions issued by the competent authorities, such as Code of Conduct and Work Ethics in Financial Institutions issued by the Central Bank and its updates, apply to all employees of the bank, including chairmen and members of boards of directors, committees, and full or part-time permanent or temporary employees, including contractors, such recruitment companies, security guards, hospitality workers, cleaners, etc.

These Principles set out the minimum rules of professional and ethical conduct. It is the responsibility of all managers within the Bank to make their employees aware of these principles and to determine whether more detailed instructions or procedures are needed within their departments to abide by these principles.

1-3 Definitions:

1-3-1 Work Ethics:

Ethical standards, rules and behavior that an employee has to comply with and show toward his/her work, colleagues and the society as a whole.

1-3-2 The Bank:

Bank Albilad and/or its subsidiaries, know as the Bank Group, and in accordance with the context and content of the text.

1-3-3 Bank Employees:

Members of the Bank's boards of directors, executives, employees (official and contracted "outsourcing employees"), consultants, and employees working through a third party.

1-3-4 Stakeholders:

Any person with an interest in the Bank, such as shareholders, creditors, customers, suppliers and any third party

1-3-5 Professional conduct:

Carrying out job duties with honesty, objectivity and integrity and working continuously to achieve the objectives of the Bank. It also means that practices conducted by employees shall be within their entrusted powers. Employees shall perform their duties in a manner that is free from negligence, and shall not violate laws and instructions, jeopardize the public interest or seek to achieve personal interest.

1-3-6 Insider Information

Any information, data, figures or statistics, whether verbal, written or electronic, obtained or accessed by any of the Bank employee by virtue of his/her work nature or because of being an employee at the Bank.

1-3-7 Confidential Information, Data or Documents

Any information or documents that is/are not available to the public, including those related to the Bank's work, administrative and financial arrangements or financial position

1-3-8 Conflict of interest:

A situation in which the objectivity and independence of any of the Bank Employees are adversely affected when performing his/her tasks by a personal, actual or potential, material or non-material interest that may relate to him/her personally or to one of his/her personal relationships. This situation also includes when the employee's performance is negatively influenced, directly or indirectly, by his/her personal considerations or after obtaining information related to a decision

1-3-9 Personal Interest:

Any personal benefit that can be realized by any of the Bank Employees by virtue of their work nature, position or granted powers

1-3-10 Disclosure:

Disclosing the cases that must be disclosed as determined by the Bank's disclosure policy to the competent department at the Bank by an employee

1-3-11 Legal Accountability:

Holding a person accountable for the acts he/she commits in contravention of the laws and policies in force, and in such a way as to harm others or damage the interests of the institution in which he/she works

2. Key Principles / Rules of Professional and Ethical Conduct:

2-1 Compliance with professional conduct and public morals:

The Bank Employees shall:

2-1-1 demonstrate and have the highest ethical standards and characteristics, including, transparency, integrity, honesty and good morals in all dealings with colleagues and Stakeholders

2-1-2 avoid any conduct that discredits the profession inside or outside the workplace, during or not during working hours, avoid any conduct that violates public decency or morals, avoid discussions on politics, religion and sectarianism and avoid incitement and all forms of racism

2-1-3 not hinder work progress, strike or incite such actions

2-1-4 perform duties accurately and objectively in a manner that serves the business interests, and improve the required skills through continuous learning and training

2-1-5 protect and not damage the reputation of the Bank by publishing information, statements or comments of its own using different media channels or communication means

2-1-6 not waste time at work during official working hours, additional hours or official tasks and dedicate it for performing and completing tasks

2-1-7 maintain the confidentiality of business information and not disclose any information that may damage the interests of the Bank if disclosed, whether during working at the institution or after leaving the job.

2-1-8 understand and adhere to the laws and not bypass, violate or neglect them

2-1-9 maintain an appropriate standard of dress and comply with the public decency laws in accordance with the Saudi laws during official working hours, training courses and all events in which the employee represents the Bank

2-1-10 obtain a prior approval from the Bank to publish information, statements or comments of its own using different media channels or communication means

2-1-11 commit to optimal and permitted use of the IT infrastructure and technical resources owned by the Bank without hindering the workflow.

2-1-12 demonstrate trust, credibility, respect, maintain a good appearance, and commit to decent behavior and good treatment.

2-1-13 Compliance with the provisions of the bank's work regulation.

2-1-14 demonstrate a great deal of responsibility in the use of social media in personal activities. The employee, especially who is well-known to customers, must ensure that his/her activities and contributions do not leave a negative impact on the bank's reputation.

2-1-15 2-1-3 Subject to the requirements of policies related to managing conflicts of interest, including the prohibition of participating in activities and businesses competing with the Bank or any of its activities, and in accordance with the relevant laws and regulations, the employee shall:

2-1-15-1 obtain a prior written permission when establishing any commercial company or commercial activity or owning a controlling share in it while working in the Bank, and notify the Bank if he/she owns non-controlling shares in them, with the exception of the listed joint-stock companies, in which case the percentage should be 5% or more.

2-1-15-2 notify the Bank upon signing the work contract of the above.

2-2 Interaction with Stakeholders:

The bank believes in providing the highest standards in serving stakeholders, especially the external and internal customers. This includes treating customers and various stakeholders in a manner that achieves transparency, integrity and cooperation using the highest professional standards.

2-2-1 The Bank also ensures that its products, services, brand and communications reflect its commitment to truth, justice, transparency, reliability and responsiveness, and to build reliable advisory relationships by caring for customers and understanding and meeting their needs and goals in the best way.

2-2-2 The policy of protecting the rights of stakeholders and handling their complaints at the bank defines the general principles and guidelines for its relations with stakeholders through:

2-2-2-1 Ultimate Objective: The Bank should be the Stakeholder's most trusted partner, and provide the best experience by making the business easy and fast

2-2-2-2 Engagement: The Bank should be a constructive partner for Stakeholders by providing clear and honest advice and giving the necessary information about products and services to make sound decisions

2-2-2-3 Response: The Bank should deal with the complaints and feedback received from Stakeholders immediately, effectively and fairly in accordance with the applicable laws and regulations to achieve the highest professional standards

2-2-2-4 Enhanced Trust: The Bank shall provide Stakeholders with clear, understandable, accurate and updated information within the framework of mutual trust in all the services and dealings, and ensure timely and full performance of services as time is an important factor in the financial system

2-2-3 The above can be applied to the customer as one of the key stakeholders as follows:

<u>Putting the customer's interest first:</u>

All bank employees must take into account the interests and needs of the bank's customers when providing financial, banking and investment advice, and be honest, professional and accurate in order to achieve the interests of customers in accordance with the bank's policies, instructions and instructions regarding sales and marketing practices. The recommendations must also be appropriate to the needs and capabilities of the customer in the light of his investment goals, financial knowledge, and degree of risk tolerance. These recommendations must reflect any other factors related to the customer that are known through the customer directly or through the "Know Your Customer" form. The Bank employees must also ensure that customers understand the nature and repercussions of any advice given to them, including risks, fees and commissions, with accuracy and clarity, and without attempting to influence the customer's investment decisions or directing him against his will to a specific investment. The customer must expressly understand that the Bank is not his first advisor and that his investment and financial decisions must be made by him and he is the one to bear all its

consequences. The Bank's employees must take precautions that limit the risks to the Bank, including the legal risks arising from the relationship with the customer.

2-3 Combating Financial Crimes and Financial and Administrative Corruption

2-3-1 Combating Money Laundering and Terrorist Financing Crimes and Suspicious Transactions

2-3-1-1 Money laundering and terrorist financing are considered criminal activities that do not only affect the Bank but also the community and the state. This is why they are prohibited under the Anti-Money Laundering Law and the Law on Terrorism Crimes and Financing and their Implementing Regulations Such laws and regulations include preventive measures that the banks and financial institutions and their staff must take The Bank has policies and procedures in place that ensure implementing strict measures to reduce the risk of misuse for financial crime purposes. The Bank Employees shall combat financial crimes, including money laundering and terrorist financing, avoid engaging in and report any unusual or suspicious activities to the Financial Investigation Unit in accordance with the legal requirements. The Bank Employees shall be responsible for applying the AML/CTF instructions, including reporting suspicious transactions and activities, and not carrying implication to inform someone that he has been reported. In case of unfounded reports made in good faith, the person reporting such transactions and activities shall have no liability to the reported person

2-3-1-2 The human resources sector and the concerned sectors/departments of the Bank shall only assign AML/CFT tasks to the employees only after joining specialized and accredited AML/CTF courses. The Bank shall also spread knowledge of AML/CTF by all appropriate means, such as training courses and bulletins

2-3-1-3 Relevant policies and procedures define the responsibilities and tasks of the bank's employees in combating money laundering and terrorist financing, and the Bank's obligations with regard to effective risk-based programs to prevent such crimes and avoid suspicious activities and detect and report them. These programs include Client Due Diligence (CDD) and Extreme Diligence for High-Risk Clients (EDD).

2-3-1-4 Duties and Responsibilities of the Bank Employees:

2-3-1-4-1 commit to the implementation of the Anti-Money Laundering Law and the Law on Terrorism Crimes and Financing, and SAMA's relevant instructions

2-3-1-4-2 perform the duties and tasks with honesty, integrity, accuracy and professionalism

2-3-1-4-3 not engage in any criminal, money laundering or terrorist financing activities

2-3-1-4-4 immediately report all suspicious transactions carried out by Stakeholders or the Bank Employees by the concerned department to the AML/CTF department, which in turn reports such transactions to the Financial Investigation Unit at the Presidency of State Security.

2-3-1-4-5 not carry implication to inform Stakeholders or staff that their activities that have been reported, will be reported to competent authorities or under investigation by the Bank are suspected

(See the relevant policies, procedures and rules on the Bank's intranet)

2-3-2 Combating Fraud, Corruption and Bribery

2-3-2-1 Combating Fraud

In view of the negative effects of fraud crimes on the bank and the financial and banking system, the bank has developed a comprehensive set of rules and policies related to combating fraud with the aim of achieving and activating controls that will help in detecting and preventing fraud activities, and strengthening a unified institutional behavior by setting strict rules for developing and managing the bank's internal controls and detecting and limiting potential fraud risks against the bank as well as conducting investigations related to fraudulent acts. The Bank shall comply with applicable laws, regulations, accounting standards, internal accounting controls and auditing practices. All employees are required to read, understand and adhere to the bank's anti-fraud policies and controls.

(See the rules and policies related to combating fraud, corruption and bribery on the Bank's intranet)

2-3-2-2 Combating Corruption and Bribery

Bribery is one of the most serious crimes causing corruption in societies. Therefore, the Bank shall condemn and fight bribery and corruption in all forms in any dealing or interaction with Stakeholders. The Bank shall also educate employees about the gravity and adverse effects of bribery and corruption. Duties and Responsibilities of Bank Employees

2-3-2-2-1 report any suspicion of corruption or bribery to the competent directors or compliance, anti-financial crime and money laundering in the Bank in case of suspicion of corruption or bribery (according to the relevant rules, controls and policies).

2-3-2-2-2 not to provide or accept facilities.

2-3-2-2-3 not exercise nepotism, cronyism or any forms of favoritism at work, which may adversely affect the confidence of the Bank's customers

2-3-2-2-4 Bank employees must report cases of corruption that they have been exposed to or that they have information about in accordance with the approved policies and controls.

2-3-2-2-5 not show any sign of financial, moral or administrative corruption whatsoever, or use any suspected or illegal means to accomplish tasks

2-3-2-2-6 not abuse job powers and report any abuse to the competent departments in the Bank.

(For more details, see the rules and policies related to combating fraud, corruption and bribery)

2-4Dealing with Gifts and Hospitality:

The Bank always seeks to strengthen the relationship and enhance trust with its customers, without neglecting or waiving compliance with the legal regulations and rules, the principles and provisions of Islamic Sharia, the rules and principles of professional and ethical behavior in general and the principles of disclosure, transparency and responsibility in particular. The bank, as a general rule, prohibits accepting, taking, offering or presenting any gift or promise thereof, except in limited and specific exceptional cases and in a way that does not violate legal regulations and rules and the relevant provisions of

Islamic Sharia, and the Bank's policy of dealing with gifts. One of the key controls and provisions that the bank follows in relation to gifts and hospitality and/or accepting them, from or by stakeholders, in order to protect the integrity of both the employee and the Bank and to protect the principle of professionalism, is as assessment to determine whether the gift or hospitality is reasonable, appropriate and justified or not, taking into account the value, nature, time and intended intentions of such gift /hospitality. The Bank Employees shall:

2-4-1 not request or accept any gifts invitation, service or anything of material or non-material value whether for himself/herself or his/her personal relationships from natural or legal persons that have or seek to have a relation with the Bank, which may directly or indirectly affect the objectivity of Bank Employees in implementing their tasks, the decisions made or may force them to commit to do something in return

2-4-2 understand that any current or former employee violating, participating or assisting in violating the laws related to requesting or accepting gifts and invitations will be held accountable for such actions

2-4-3 accept the gift presented if rejection would be offensive to the Bank, rejection is not practically possible or if presented to the staff in official visits, events or receptions, in accordance with the rules of etiquette and protocol followed in visits and events. However, the acceptance of the gift shall be subject to the following:

2-4-3-1 the gift shall not be cash

2-4-3-2 the gift and its value shall be according to the usual practices followed in a particular event, such as trophies

2-4-3-3 if the gift is a fee discount or exemption, it shall be related to an invitation to attend a conference or meeting that enhances knowledge, positively reflects on the business of the Bank and does not result in a conflict of interest

2-4-3-4 the gift shall not be presented due to the recipient's position or work at the Bank.

2-4-3-5 the person presenting the gift shall not have private or public interest that he/she wishes to get from the Bank or one of its employees.

2-4-4 An employee may accept a prize from an entity with which the Bank has a relationship due to his/her achievement as follows:

2-4-4-1 the prize shall be awarded as part of an announced and recognized program on a regular basis.

2-4-4-2 the winner selection shall be according to an announced criterion

2-4-4-3 prior approval shall be obtained from the Bank.

2-4-5 The gift recipient shall submit a written disclosure form to the compliance, anti-financial crimes and money laundering department directly after receiving the gift in the following cases:

2-4-5-1 if the gift has a value and can be sold

2-4-5-2 if the gift is perishable and of a value exceeding SAR 1000

2-4-5-3 The Bank Employees shall not offer gifts, grants or invitations to those who personally have business relationships with the Bank, unless offered by the competent department as per the approved policy on this regard.

2-4-5-4 Gifts and grants that may damage the reputation of the Bank shall not be accepted or requested

(For more information, see the policy for dealing with gifts on the Bank's intranet).

2-5Compliance with Laws, Regulations, Instructions and Policies

2-5-1 Adherence to rules, regulations, instructions and policies is one of the most important bases and factors of success for the Bank that helps maintaining its reputation and credibility. The Bank Employees shall be aware of, comply with and understand the applicable laws, regulations, instructions and policies related to the work and tasks assigned, which shall also be applied without violation or negligence. In addition, any dealing that may violate such laws, regulations, instructions or policies shall not be carried out in the name of the Bank.

2-5-2 In the event that any policy or internal clause conflicts with the applicable law/regulation in any jurisdiction to which the bank is subject, or if it is less restrictive, the more restrictive law/regulation shall be applied. Some business units are entitled from time to time to set policies that are more restrictive than the Code of Conduct, and in such cases, the most restrictive policies shall be applied.

2-6Dealing with Conflicts of Interest:

2-6-1 Conflict of Interest Management:

To protect the Bank and Stakeholders, the staff shall be responsible for identifying any potential or actual conflict of interest that may adversely affect the Bank and/or Stakeholders. In cases where a conflict of interest is not possible to be prevented, the Bank shall properly manage such conflict through a set of controls, policies and procedures

2-7Confidentiality and Disclosure Mechanisms.

Information is an important asset to the businesses of the Bank and information protection is an important factor for its success and continuity In addition, all information related to the Bank's Stakeholders or employees shall be the property of the Bank. Accordingly, the Bank has adopted a set of policies, controls and procedures related to information, its confidentiality, classification, preservation, destruction, storage, etc.

The Bank classifies information in terms of confidentiality, according to the Central Bank's rules and instructions, as follows

2-7-1 Classification of Bank information:

2-7-1-1 General Information:

General information available to the public for free through the Bank's authorized channels

2-7-1-2 Insider Information:

Information not disclosed to any person outside the Bank.

2-7-1-3 Confidential Information:

All non-public information related to the Bank, staff or Stakeholders. The Bank Employees, with access to such information, shall protect and only disclose the information to other staff members as necessary Unauthorized disclosure of confidential information may result in legal ramifications, such as lawsuits, legal penalties or damage to reputation Examples of confidential information include: private information, Bank strategies, competitively sensitive information, trade secrets, specifications, stakeholder lists or research data. Unauthorized persons shall not have access to such information

2-7-1-4 Highly Confidential Information:

Information entrusted to some employees that could significantly affect the Bank if disclosed without permission. Such information should be made available to the staff only as required by the Bank's work. The Bank Employees shall comply with the information security policy, especially that addresses dealing with different types of information. Highly confidential information shall only be available to authorized employees.

2-7-2 Classification of Confidentiality.

2-7-2-1 Confidentiality of Stakeholder Information:

It shall be the duty and responsibility of the Bank to protect the confidentiality of stakeholder information. The employees shall be entrusted with the stakeholder important information which is also important to maintain the Bank's ability to provide quality products and services This information includes, but is not limited to, the following:

2-7-2-1-1 personal data, information on products; services; accounts; balances.

2-7-2-1-2 transactions; mergers or acquisitions; status of securities

2-7-2-1-3 pending requests or plans prepared to increase capital. Stakeholder information protection shall be the sole and collective responsibility of the Bank employees. Information shall be handled with the utmost confidentiality in accordance with the highest standards applied. The obligation to maintain the confidentiality of information shall continue even after the end of the work/ service of the employee. Stakeholder information shall not be shared with anyone who does not have access to it inside or outside the bank

2-7-2-2 Confidentiality of Property Information:

2-7-2-2-1 While working at the Bank, the employees may provide, develop and/or access information, ideas, innovations, systems, intellectual properties, technologies, policies, procedures, processes, software, hardware, operational processes, profitability results and forecasts, business plans, strategies, programs, staff data, reports, studies, records; stakeholder data, lists and information; trade secrets and other information related to the Bank, its products or services, Stakeholders, potential stakeholders or any other relevant parties that are not publicly available. Such information may be original, copy of the original, electronic, saved, written or any other type.

2-7-2-2-2 As a requirement for employment/ service, the Bank Employees shall acknowledge or agree that such information is the property of the Bank alone and shall not have any rights or interests with respect thereto. It shall be the duty of the Bank Employees to maintain property information and not use such information outside the limits of the Bank’s business. Furthermore, unauthorized use of property information shall be prohibited.

2-7-2-2-3 The Bank Employees shall not record any communications that include property information through the use of electronic devices or personal recording devices, including mobile phone cameras, and such information shall not be used, spread or disclosed to any unauthorized third party during working at the institution or after leaving the job. The Bank Employees shall not spread or destroy property information. In case of resignation, the Bank Employees shall

delete/ return property information in possession, including the information saved on personal devices, such as electronic devices or personal computers.

2-7-2-2-4 Applications for the protection and confidentiality of proprietary information:

2-7-2-2-4-1 Bank Asset Protection:

Embezzlement, misuse of the Bank's assets, or unauthorized disclosure constitute a violation of honesty and integrity and constitute a fraudulent act. Therefore, the Bank's employees shall:

2-7-2-2-4-1-1 Preserve the Bank's assets and properties, and not use them for personal use or for personal benefit, and not to use the Bank's trademark, bank documents or name for unauthorized purposes.

2-7-2-2-4-1-2 not to perform any action transferring ownership or benefit, such as selling, lending, mortgaging, or donating any assets or property of the Bank, regardless of the status or value of these assets, unless they are authorized to do so in accordance with the authority delegation matrix.

2-7-2-2-4-1-3 avoid negligence, waste or unauthorized use of Bank assets.

2-7-2-2-4-1-4 not to abuse any product, automated system, or intellectual property that the employee created or developed during his work with the Bank, as it is considered the Bank's property. The employee will comply with that even after the termination of his relationship with the Bank.

2-7-2-2-4-2 Information and Communication Technology Protection:

2-7-2-2-4-2-1 The Bank's employees shall not:

2-7-2-2-4-2-1-1 use of unauthorized software/scripts/data entry and commands.

2-7-2-2-4-2-1-2 Install or distribute "pirated" or other software products not properly licensed for use by the Bank.

2-7-2-2-4-2-1-3 reproduce copyrighted material without proper permission.

2-7-2-2-4-2-1-4 use the Internet excessively for non-work purposes or accessing inappropriate websites.

2-7-2-2-4-2-2 The Internal Audit Department, the Information Technology Department, and the Information Security Department may collectively or individually randomly ascertain the nature of the visited websites or the content of e-mail that is not related to work in order to ensure compliance with the rules of conduct. The perpetrator of this act will be investigated and the penalties stipulated in the penalties and violations table will be applied against him.

2-7-2-3 Confidentiality of Insider Information:

2-7-2-3-1 The Bank Employees may sometimes be entrusted with material Insider Information. Such Information may be kept, but shall not be misused

2-7-2-3-2 The definition of "material Insider Information" is board. However, Insider Information is considered "material" if it is highly likely that an adult will consider it important to make investment/ business decisions or if the spread of such information will affect the price of the company/bank securities in the market Insider information may also be considered material if it is related to the future or potential or expected events; or if considered material only when combined with publicly available information. All information shall be considered "Insider" unless disclosed and enough time has passed. Examples of adequate information disclosure include: information submitted to securities

markets and regulators (such as Tadawul and CMA) or issued in a press release or through meetings with members of the media and the public

2-7-2-3-3 The Bank Employees shall not discuss or pass Insider Information on to any other employee unless the exchange of such information serves the purposes of the Bank.

2-7-2-3-4 The Bank employees should not trade in the shares or securities of a listed company, and shall not offer recommendations to do so based on Insider Information they have access to by virtue of their work/ service in the Bank.

2-7-2-3-5 The Bank Employees shall not make investment or business decisions, that are not related to the work of the Financial Institution, based on information they have obtained for the Bank. Such act is a punishable violation.

2-7-2-3-6 Therefore, if any member of the Bank believes that he/she has access to Insider Information, he/she shall not trade in securities based on such information, except after consulting the compliance department. In case of carrying out trading activities or owning securities before joining the Bank, the competent department shall be informed.

2-7-2-4 Exchange of Confidential Information on the Basis of Need:

2-7-2-4-1 The Bank Employees shall not disclose confidential information to other employees, supervisory and control authorities or external lawyers and/or advisors, except after obtaining the required approvals. Disclosure shall be in accordance with following cases:

2-7-2-4-1-1 if the recipient is authorized and has a legitimate need for such information in relation to his/her responsibilities of work/ service according to the relevant instructions.

2-7-2-4-1-2 if disclosing such information will not cause damage.

2-7-2-4-2-1 The Bank Employees shall not give any information about the Bank to third parties unless they have the authority to do so. As an exception, some information may be disclosed if disclosure is normal when carrying out the Bank's business, for example, information requested about solvency and/or by a supervisory or regulatory authority or if disclosure is in the interest of the Bank and its Stakeholders. The following are examples of cases that are subject to the exemption, however, the exception will only be applied after obtaining the approval of the concerned officials at the Bank:

2-7-2-4-2-2 general periodic disclosures requested by regulators.

2-7-2-4-2-3 information requested by competent authorities for investigation purposes.

2-7-2-4-2-4 Regulation and supervision information requests shall be referred to the compliance, anti-financial crime and money laundering department. Thus, no employee shall have the right to respond to any enquiry about regulation or supervision or provide such authorities with the requested information except through the compliance, anti-financial crime and money laundering department or if he/she is authorized to do so according to relevant policies and controls.

2-7-2-5 Duties of Bank Employees:

2-7-2-5-1 The Bank Employees shall be obliged to protect confidential information. In addition to complying with the detailed requirements stated in the information security policy prepared by the Bank, the employees, as a minimum, shall:

2-7-2-5-1-1 adhere to the information security policy and procedures, and the laws and instructions related to confidentiality

2-7-2-5-1-2 not access non-public stakeholder or property information for purposes unrelated to their work, as accessing such information must be within their powers and for work reasons.

2-7-2-5-1-3 not try to obtain confidential information that are unrelated to their work.

2-7-2-5-1-4 not provide any unauthorized person inside or outside the Bank with confidential information or facilitate his/her access to it.

2-7-2-5-1-5 provide authorized persons with information according to the required limits.

2-7-2-5-1-6 maintain stakeholder and property information or other confidential information in a way that allows access to authorized persons only.

2-7-2-5-1-7 not leave any confidential information in places where they can be accessed, such as shared offices or areas.

2-7-2-5-1-8 use envelopes, postal services or emails marked as confidential when exchanging confidential information within the Bank.

2-7-2-5-1-9 not copy any document or text that is not related to work before obtaining the approval of the direct line manager.

2-7-2-5-1-10 not enter vaults, strongrooms or other restricted areas unless authorized or required by their work.

2-7-2-5-1-11 only put the documents they are currently working on on the desk, and keep the other documents in drawers, preferably in locked places.

2-7-2-5-1-12 turn off all devices and lock all drawers before leaving the office.

2-7-2-5-1-13 destroy all documents that are no longer needed and contain sensitive or confidential information, and keep other papers and documents in files inside lockers.

2-7-2-5-1-14 not disclose any confidential information about the Bank to any person, including the institution employees who are unauthorized to access or do not need such information.

2-7-2-5-1-15 take precautionary measures to avoid unauthorized disclosure of confidential information.

2-7-2-5-1-16 not discuss any sensitive or confidential information in public places, such as elevators, corridors and public transportations.

2-7-2-5-1-17 maintain the confidentiality of the Bank information during working at the institution or after leaving the job, and not share, collect, record or spread such information at any time or for any reason unless after obtaining a written approval from the competent department.

2-7-2-5-1-18 not access the premises of the Bank outside working hours unless after obtaining the approval of the direct line manager and the security and safety department.

2-7-2-5-1-19 understand and acknowledge that any intellectual property developed for the Bank or created using its resources are the property of the Bank alone.

2-7-2-5-1-20 maintain the confidentiality of the access codes and passwords of strongrooms, IT systems and any other codes or passwords.

2-7-2-5-1-21 prevent intentional or unintentional disclosure of confidential information.

2-7-2-5-1-22 obtain prior approval from the authorized person to copy or keep any document or text outside the Bank building to conduct work outside the building.

2-7-2-5-2 The information security department shall be informed when any employee receives confidential information he/she does not need at that time. In addition to the abovementioned duties, the Bank Employees shall be responsible for meeting the following security obligations:

2-7-2-5-2-1 comply with legal, regulatory and other contractual requirements applied in their field of business

2-7-2-5-2-2 maintain work ID and passwords of the IT systems and change them periodically; understand that they are responsible for any action carried out using their work IDs, and follow information security policies to prevent misuse of work ID.

2-7-2-5-2-3 not tamper with the security and protection of the IT systems.

2-7-2-5-2-4 take the necessary steps to protect the information stored on computers.

2-7-2-5-2-5 comply with the additional security procedures established to prevent unintentional disclosure of confidential information by employees who have laptops, remote access to the systems or permission to use any other portable devices to perform the business of the Bank.

2-7-2-6 Use and Leakage of Insider Information for Market Manipulation.

Bank Employees shall not engage in any act, or participate in or encourage the performance of any conduct that may give false idea of any investment, price or value of something by using or leaking Insider Information to obtain personal benefits for their own or for third parties.

(See the insider information ban policy on the bank's intranet)

2-8Compliance with the Sharia Committee Decisions:

All Bank Employees shall fully comply with the decisions of the Sharia Committee with regard to contracts, forms, procedures, and the provision of products and services. The Bank considers decisions and actions that violate the decisions of the Sharia Committee as a violation of the rules of conduct. Employees are required to refer to the Sharia department with regard to all new contracts, products and services.

2-9Social Responsibility:

The principles and rules of professional and ethical conduct are compatible and integrated with the principles of social responsibility. These rules confirm and implement the key principles of social responsibility approved by the Bank, such as:

2-9-1 Transparency: The Bank is obligated to disclose its policies, procedures, decisions, activities, and their known and potential impacts on the environment and society. This information shall be made available to the person affected (stakeholders), or likely to be substantially affected by the Bank.

2-9-2 **Ethical Behavior:** The bank builds its behavior and actions on the ethics of honesty, integrity, justice and integration towards all elements of society and commitment to achieving the interests of stakeholders, including its customers and employees.

2-9-3 **Respect Stakeholders' Interests:** The Bank takes into account the relationship between the interests of stakeholders and the greater expectations of the community in addition to the nature of the relationship of stakeholders with the Bank. It also takes into account the views of stakeholders that may be affected by a particular decision.

2-9-4 **Respect Order and Law:** The Bank and its employees comply with all applicable local and international rules, regulations, controls and standards, written, announced, enforceable, and in accordance with well-established, specific and documented policies and procedures.

2-9-5 **Respect International Standards and Norms of Professional Conduct:** The Bank respects the international standards and norms recognized by the state in providing its services and products and dealing with its customers, and even its employees and society in general.

(See the social responsibility policy on the bank's intranet)

2-10 Whistleblowing

2-10-1 Bank Employees shall use the methods of communication approved by the Bank to report any suspicious activities carried out by employees who have Insider or Confidential Information. In addition, cases of fraud or attempted fraud, money or business paper loss, potential violation of the laws, regulations, instructions or policies of the Bank or unusual transactions that the reporting employee believes that they do not conform with the financial status of Stakeholders shall be reported as well.

2-10-2 The Bank shall protect the confidentiality of whistleblowers, protect employees reporting in good faith and not tolerate any form of retaliation against whistleblowers.

2-10-3 The Bank shall hold employees who deliberately ignore reporting wrongdoings that violate the relevant laws, regulations, instructions or policies accountable

For more information, please see the policies, controls, and guides for reporting violations, fraud, corruption, and bribery.

2-11 Remuneration and Compensation

Bank Albilad believes in the importance of motivating its employees as they are the bank's human capital and represent a great competitive advantage for the bank. Therefore, the bank implements the best practices that contribute to establishing a valid and effective work environment that stimulates production and the spirit of initiative and creativity. The bank also operates in accordance with the provisions of the regulations, regulations, and instructions of the Central Bank and relevant regulatory authorities, in a manner that guarantees sound and effective risk management through an effective management structure to set goals and share them with employees / stakeholders. The Bank takes into account in its policies of remuneration and compensation the sound and effective risk management for remuneration, without focusing a specific category of employees, in accordance with the Bank's strategy, values, priorities and long-term goals.

2-12 Controls for the safe use of the bank's information assets in the scope of work and remote work.

2-12-1 Use of the information assets for personal purposes or any unauthorized viewing, printing or downloading without the express consent of the authorized person shall be prohibited.

2-12-2 Before opening any attachments in an email, the sender shall be verified.

2-12-3 Unauthorized, unlicensed or illegal software must not be installed on any of the Bank's machines.

2-12-4 Access to information or information processing systems and facilities for any purpose other than conducting business is prohibited, even if employees are so authorized.

2-12-5 It is the employee's responsibility to promptly report theft, loss, or unauthorized disclosure of the Bank's information assets.

2-12-6 Information processing equipment or software shall not be carried outside the premises, without prior approval.

2-12-7 Mobile devices shall not be left unattended in public spaces and must have access protection mechanisms in place.

2-12-8 Exploring or attempting to compromise any information security controls, whether internal or external, is prohibited unless specifically authorized.

2-12-9 Disclosing or posting confidential or proprietary information, trade secrets, or any other material shall be prohibited in blogs or social media.

2-12-10 Employees should not represent themselves explicitly or implicitly as an employee or representative of Bank Albilad while expressing their beliefs and/or opinions in blogs or social media.

2-12-11 All Users are responsible for all activities that are conducted under their User IDs on the Systems.

2-12-12 Theft or unauthorized copying of electronic shall be prohibited.

2-12-13 An employee shall not browse the private files or accounts of other users, except as provided by the appropriate authority within the Bank.

2-12-14 An employee shall not engage in informal activities that may harm the performance of the systems, such as playing electronic games.

2-12-15 Activities intended to circumvent security or access controls are prohibited, including possessing or using hardware or software tools intended to modify or destroy software copy protection, discover passwords, identify security vulnerabilities, decrypt encrypted files, or compromise information security by any other means.

2-12-16 It is prohibited to write, copy, execute or attempt to enter any computer code designed to self-replicate or to damage or impair the performance of or access to the Bank's computer, network or information.

2-12-17 It is forbidden to access the bank's network via modem or other remote access service without prior approval from the administration.

2-12-18 An employee may not use another person's user ID and password to access information resources including the use of privileged user accounts unless so authorized.

2-12-19 Attempt to gain unauthorized access to any bank or non-bank computer is prohibited.

2-12-20 In the event that an employee resigns voluntarily or his service with the Bank is terminated, all assets in his possession must be returned to the concerned department, in accordance with the relevant controls.

2-12-21 Every employee shall be responsible for ensuring the security of the information and information assets entrusted to him.

2-12-22 Information processing resources and media containing restricted/confidential data must have access protection and may not be left unattended in public places.

2-12-23 Any loss of information assets must be reported to the Information Security Department immediately.

2-12-24 No employee may use photographic, video, audio or other recording equipment within the secured areas of the Bank without prior permission

2-12-25 The use of escape methods to intentionally bypass the monitoring or filtering of the Bank's network and any such efforts to compromise the Bank's network are expressly prohibited and will result in disciplinary action.

2-12-26 No employee shall carry bank information processing equipment or software outside the premises of the company, without obtaining prior written/postal approval from the Chief Information Security Officer.

2-12-27 No employee may carry any non-electronic information outside the Bank's premises without obtaining prior written permission from the concerned business unit manager.

2-12-28 No person may use external devices such as DVDs / CDs / Memory Cards / any other removable media within the premises of the Bank. If the work requires so, the Information Security Control Center / Helpdesk should be contacted; The media should be scanned/cleaned for viruses before it can be used.

2-12-29 It is the responsibility of each person who carries removable media containing restricted/confidential information to ensure that appropriate and adequate safeguards are used to protect the confidentiality, integrity and availability of information during and after transmission.

2-12-30 Any person who carries computer media containing restricted/confidential information for disposal should ensure that the media is securely erased or rendered unreadable prior to disposal.

2-12-31 No user of the Bank shall store their passwords in any computer file, emails, mobile phones or on paper unless the passwords are electronically encrypted.

2-12-32 The password must be changed if the employee knows or suspects that their password has been compromised.

2-12-33 The password must be changed if temporary passwords are issued for the first-time login.

2-12-34 The password must be changed if the system administrators request a password reset.

2-12-35 Users shall not use the Bank's customer information for any unauthorized purposes, nor shall they disclose to any third parties any customer information, unless required by the laws and regulations of the Kingdom of Saudi Arabia.

2-12-36 To protect the integrity of the Bank's information assets, employees may not use proprietary software within the Bank's information assets, including purchased and licensed applications, free participation programs, downloads from bulletin

boards, the Internet, intranets, FTP sites, local area networks (LANs), or wide area networks (WANs); and other personally owned or controlled software.

2-12-37 It is forbidden to send information that violates the regulations / laws or the Bank policies.

2-12-38 It is forbidden to send unsolicited commercial advertisements or advertising materials, unless approved by the administration in advance.

2-12-39 It is prohibited to send any material that defames the Bank, the recipient, the sender or any other person, or defames, abuses, embarrasses, presents a bad image of the same.

2-12-40 It is prohibited to send pornographic, racist, offensive material, chain letters, unauthorized mass mailings, or malicious code

2-12-41 It is prohibited to enter into binding contractual agreements on behalf of the Bank via the Internet without obtaining prior written permission from the electronic executive management of the bank.

2-12-42 It is prohibited to use the Bank's logo or other Bank materials on any web page, online posting, or participation in discussion boards unless approved in advance in writing by the Bank's executive management.

2-12-43 It is prohibited to create Internet or other external network connections that could allow non-bank users to access the bank's systems and information assets.

2-12-44 Employees are not allowed to run software obtained from external sources (via the WWW or other untrusted sources) without prior written permission from Information Security Department.

2-12-45 It is forbidden to browse explicit or hate-based pornographic websites, hacker or spam websites, or other websites prohibited by the Bank.

2-12-46 It is prohibited to post, send or obtain sexually explicit or sexually oriented material, hate material, hacking related material or other material prohibited by the Bank.

2-12-47 Other services available on the Internet, such as FTP or Telnet, may not be used on desktop machines or other information assets for which the user does not have an account, or on systems without a guest or anonymous account for the service being used.

2-12-48 Confidential telephone discussions should be conducted in separate secure meeting rooms, especially when it comes to audio conferences/meetings.

2-12-49 Users must confirm the identity of the person they are communicating with.

2-12-50 The conference call leader must ensure that only authorized users are on the call

2-12-51 The user must change the default access codes and initial passwords immediately upon receiving a new voicemail, system account, or app.

2-12-52 It is strictly forbidden to use the access code associated with personal details such as birthdays, anniversaries or parts of the National ID number / Iqama number.

2-12-53 It is strictly forbidden to use an access code using sequential numbers such as 1234 to avoid being accessed by hackers by guessing the access codes.

2-12-54 Confidential information should not be left in telephone voice mail or telephone answer messages; Instead, the intended recipients of the message should be asked to make contact with the caller to obtain more information.

2-12-55 It is prohibited to disclose employee or customer details, such as names, job titles, salaries, user ID, etc., through any means of communication to an unknown caller.

2-12-56 Users shall not misuse the telephone facility for personal reasons.

2-12-57 Messages may not be kept on the system for longer than necessary, especially messages that contain sensitive, confidential or personal information.

2-12-58 Users must know who they are communicating with.

2-12-59 If the user does not know the caller personally or suspects that the caller may not be valid, the legitimacy of the caller should be verified by insisting on the callback number before calling back.

2-12-60 It shall be verified that the caller has a business need to know the information they are requesting until the caller's need to know is proven

2-12-61 Bank and customer proprietary information may not be sent or replied to unknown or unverifiable email addresses because the name and address received or sent by email may not be the real name and email address. .

2-12-62 Users who have fallen victim to social engineering or attempts of social engineering must report the incident immediately to the Information Security Department.

2-12-63 61.12.2 Users shall not communicate with unknown and unauthorized entities.

2-12-64 Telework devices must be securely used and protect.

2-12-65 The data stored on telework must be protected and handled according to its classification and the procedures and policies of the entity

2-12-66 Avoidance of teleworking using unreliable public devices or networks or while in public places.

2-12-67 Secure handling of home networks, making sure it is configured in a secure way.

2-12-68 Secure handling of applications and solutions used for telework such as: virtual conferencing and collaboration, and file sharing solutions.

2-12-69 To Communicate directly with the cybersecurity department If a cybersecurity threat is suspected

2-12-70 Mobile devices should not be used in the Bank's business unless a mobile device management system (MDM) is in place.

3 Consequences of Non-Compliance with the Principles and Rules of Professional and Ethical Conduct.

Violation of the principles and rules of professional and ethical conduct may lead to disciplinary action or other corrective action in accordance with the approved rules, regulations, policies and controls of the Bank and may lead to dismissal from work and non-criminal and criminal prosecution, if necessary. The application of disciplinary and/or judicial measures depends on the nature and severity of the violation and its impact. These issues are addressed in consultation with the Compliance and Anti-Financial Crimes Department, Legal Department, and Human Resources Department. An assessment shall be made of whether the act was voluntary or accidental and whether it resulted from good faith, as considerations that contribute in mitigating punishment.

4 Final General Rules and Provisions:

4-1 All Bank Employees, when representing the bank externally or through the media, social media, or other means of media, shall abide by the Bank's relevant instructions. No employee may represent the bank in any external forum unless authorized

the Bank. Any discussion about the bank's activities and performance must be presented to relevant department and marketing and communication department before making it available to public. Employees are required to communicate with relevant department or the Director of Marketing and Communications in case they have any questions about the guidelines for internal and external communication, and to abide by the "Information Security Policy".

4-2 Bank employees shall take into account the principles, requirements and objectives of social responsibility when dealing with bank customers and providing its services and products. They shall also preserve and maintain the environment, and adopting best practices in this regard.

4-3 New employees shall sign an official acknowledgment that they have received and read a booklet of the Code of Principles and Rules of Professional and Ethical Conduct and understand their obligations specified therein. The Human Resources Department shall annually request all employees to read this code and related policies and sign manually or electronically an acknowledgment to that effect. Any breach or non-compliance with these rules shall be recorded and reported in accordance with the Bank's policies.

5 Amending, Updating and Developing Code of Principles and Rules of Professional and Ethical Conduct.

The General Secretariat and Governance Department, in coordination with the Human Resources Department, shall be responsible for reviewing and developing the Code of Principles and Rules of Professional and Ethical Conduct regularly, and submitting the same to the Compliance and Governance Committee to recommend its approval by the Board of Directors.

6 Policies and Documents Related to the Bank's Code of Principles and Rules of Professional and Ethical Conduct:

The Code of Principles and Rules of Professional and Ethical Conduct must be read in accordance with the relevant policies and guides below:

6-1 Anti-fraud, early warning, whistleblowing, and whistleblower protection rules and policies guide.

6-2 Gift handling policy.

6-3 Policies related to information security and confidential information handling.

6-4 Know your customer policy.

6-5 Anti-money laundering and terrorist financing guide.

6-6 Disclosure policy.

6-7 Insider information policy.

6-8 Conflict of interest and related parties' transaction policy.

6-9 Social responsibility policy.

6-10 Compliance policy.

6-11 Compliance guide.

6-12 Compensation and benefits policy.

6-13 Sharia governance rules and policies guide.

6-14 Information technology governance rules and policies guide.

7 Declaration of compliance with the Code of Principles and Rules of Professional and Ethical Conduct

I....., ...the undersigned, declare by signing this document that I have read the Code of Principles and Rules of Professional and Ethical Conduct and understood and agreed to its provisions and my duties in complying with it and with the policies and controls referred to therein and other documents, and tom implement the same with full due diligence, care, accuracy and honesty. I undertake not to do any act or refraining from doing any act that may violate any of these rules, or regulations, decisions, instructions and policies approved by the Bank and the decisions of the Sharia Committee. I acknowledge that if I commit any violation or breach of the Code of Conduct, the Bank shall have the right to apply appropriate penalties against me as stipulated in the table of penalties and violations.

Name	: ....
Title	: ....
Administrative Unit	: ....
Signature	: ....
Date	: ....