Burgan Bank

Employee Code of Conduct

بنک بروقان
BURGAN BANK

Introduction

This Policy has been developed by and is exclusive property of Burgan Bank. The Policy is publicly intended solely for informational purposes. No part of this Policy may be copied, reproduced, distributed, modified, or transmitted in any forms or any means without the prior written consent of Burgan Bank. Any unauthorized use, reproduction, distribution, or modification of this Policy may result in legal action in accordance with applicable laws and regulations.

Policy Statement

Burgan Bank K.P.S.C. ("the Bank") believes that the reputation of any banking organization depends not only on its financial position in the market but also on its integrity and the level of trust it enjoys.

The Bank is committed to maintaining its reputation by upholding the highest ethical standards, transparency in all operations as part of our core values in addition to maintaining integrity and trust.

Purpose

This Code of Conduct (the "Code") sets out the basic principles for activities throughout the Bank. The Code also offers guidance on the personal conduct of employees and provides the outline for its implementation in order to:

- Safeguard the interests of the Bank's shareholders;
- Maintain the Bank's integrity in the market; and
- Combat all unlawful acts, including, but not limited to, corruption, money laundering and terrorism finance.

This Code is applicable to all employees of the Bank.

Application

1. General Standards of Conduct

The following standards of conduct are expected from all employees of the Bank:

- Employees shall act within the authority conferred upon them, and in the best interest of the Bank, in accordance with the applicable laws, regulations, policies and procedures;
- Employees shall act in accordance with the highest standard of honesty, integrity, fairness and ethical conduct while working for the Bank, without allowing their independent judgment to be subordinated, in accordance with the applicable laws, regulations, policies and procedures, and shall properly fulfil the fiduciary obligations conferred upon them;
- Employees shall not involve in any matter in which a conflict of interest with the Bank may arise. In the event of doubt of such conflict of interest, the relevant facts shall be disclosed in writing by the relevant employee to Senior Management and the Human Resources &

Development Group ("HRG"), explaining the circumstances that create or may create the conflict of interest for further directions of the Bank in the matter;

- Employees shall avoid any personal business relationship with colleagues, contractors or suppliers that can compromise the ability to transact business on a professional, impartial and competitive basis, or influence decisions to be made by the Bank;
- Employees are expected to devote their full attention to the best interest of the Bank within the applicable laws and regulations;
- Employees shall not use – for their own personal gain – opportunities, information or positions that are known or available to them in the course of their work with the Bank, unless the use of such opportunities/information/positions is approved in writing by the Bank's Senior Management and HRG;
- Employees shall comply with all applicable laws, regulations, regulatory instructions, or any other rules issued by a competent authority that has jurisdiction over the Bank;
- Employees shall keep all information, data, know-how, copyrights, ideas, designs, concepts, technology, marketing information, client information and any information (in whatever format) disclosed or accessed by them in the course of working with the Bank in full confidence, and shall not disclose any such information to any person(s) other than those permitted under applicable laws and the Bank's policies;
- Employees shall endeavor not to cause any loss to other Group companies in the pursuit of profit for the Bank;
- Employees are required to act in a professional manner towards other colleagues, and towards the Bank's customers, contractors and third parties;
- Employees are required to adhere to all policies, procedures and professional standards of conduct as communicated by the Bank
- Employees are expected to understand and imbibe these standards in their daily routine and make them part of their work life within the Bank; and
- Employees can report any incident which they think may negatively impact the Bank or any of its employees either to their direct managers or to HRG, or as per the Bank's Whistleblowing Policy. Employees shall be protected against any retaliation when making good faith reports.

2. Discrimination and Harassment

With the Bank being so diverse, each employee shall respect and value each other, and help to maintain and promote fundamental Human Rights across the Bank. The Bank has a zero-tolerance threshold for discrimination or the denial of equal opportunities.

Employees shall ensure that the workplace is free from harassment or offensive or disrespectful conduct. This is a matter not only of compliance with law and regulation, but also a matter of the Bank's policy.

An employee of the Bank can make a complaint of any perceived discrimination or harassment as per the Bank's Grievance, Problem Solving & Disciplinary Policy.

3. Disciplinary Action

The Bank will address problems that are associated with an employee's performance, attendance and / or breach of the Bank's policies and procedures. The Bank shall ensure that the recommended disciplinary action is progressive.

For grievances and disciplinary actions, the Bank's Grievance, Problem Solving & Disciplinary Policy shall have equal effect.

4. Workplace Violence

The Bank strives to provide a safe and secure workplace for all employees. The Bank shall not tolerate any type of workplace violence committed by or against employees or any customer/vendor/supplier of the Bank.

Employees are prohibited from making unlawful threats or engaging in violent activities. Any potentially dangerous situations must be reported immediately to a supervisor or to the General Manager - Human Resources Group ("GM- HRG") and/or the Employee Relations Manager ("ERM").

Employees can make anonymous reporting of any incident pertaining to workplace violence to HRG. All reported incidents shall be investigated by the GMHRG and/or the ERM, depending on the severity of the conduct in the opinion of the complainant. Reports or incidents warranting confidentiality shall be handled appropriately and information shall be disclosed to others only on a need-to-know basis for investigation purposes only. All parties involved in such a situation shall be counselled, and the results of investigations shall be discussed with them.

Any employee charged and established to have made an unlawful threat, or engaged in violent activity, shall be subject to disciplinary action as per the Bank's Penal Code.

5. Conflict of Interest

Employees shall not place themselves in a position where their own interests, or the interests of their first, second and third-degree relatives or a third party, can conflict with those of the Bank or any of its customers.

Employees shall make full disclosure to HRG, in writing (through Know your Employee Form (KYE)), of any situation that involves a conflict of interest, or appears as conflict of interest, between the employee, or any of his or her relatives, and the Bank.

Employees shall obtain approval from the respective GM/DGM, and the HRGDGM/GM of HRG, before undertaking any activity identified as a possible conflict of interest.

Areas of potential conflict of interest may involve, but are not limited to, the following:

- Holding unapproved financial interest and/or being a member of the Board or management in any enterprise without obtaining the Bank's prior written consent to the same. Financial holding is considered substantial when the shareholding is 3% or more of the enterprise regardless of the value, or more than KD 100,000/- in value.
- Having an unapproved personal, business, financial or other interest, activity or family relationship, inside or outside the Bank, that has or may have the potential of being in conflict with the best interests of the Bank.
- Rendering directive, managerial or consultative services to, or being employed by, any outside concern that does business with, or is a competitor of, the Bank, except with the Bank's prior written knowledge and consent given by authorized personnel representing the Bank.
- Representing the Bank in any transaction in which an unapproved personal, family, business or financial interest may exist.
- Competing with the Bank for the sale or purchase of any kind of tangible or intangible assets, or diverting a business opportunity from the Bank for personal interest.
- Using the Bank's assets, like funds, facilities, know-how or personnel, for personal profit and advantage.
- Acceptance of gifts by an employee, or by an immediate family member of an employee, in cash (or kind), loans (except from banks and other financial institutions), vacations, travel, excessive entertainment, service, payment for self-education or of family member education, from any customer, vendor, competitor or any other party doing business or seeking to do business with the Bank.

Employees shall inform the Bank in writing and obtain the Bank's prior written consent before being involved in any of the above activities.

6. Custodial and Fiduciary Responsibilities

Employees working as custodians of valuables/documents are expected to handle such valuables/documents as required by the applicable procedures. All employees of the Bank are custodians of their access cards, business cards, stamps, passwords and all other privileges provided by the Bank, and shall exercise due care and caution in their use.

Employees engaging in any dealings outside the Bank in their personal capacity shall not refer or use their Bank designations. These dealings include, but are not limited to, attesting / witnessing legal documents, referring to the Bank in online forums, etc.

The Bank believes that each employee has a right to have an active political or civil role. However, employees shall conduct any political activity only outside the workplace.

7. Prevent Misuse or Damage of Bank's Property (Sabotage)

Workplace sabotage occurs when employees intentionally damage a property or product owned by the Bank. Sabotage also occurs when an employee impairs the Bank's reputation and/or threatens its processes. Examples include, but are not limited to; destroying equipment; stopping or slowing work; lowering product quality; insulting the Bank, its management and/or employees through any channel of communication, publication or media; and violating work procedures.

All employees shall be responsible for the safekeeping, order and return in good condition of all of the Bank's property which is in their use, custody or charge.

Employees shall not use the Bank's property for activities other than those that are officially approved by the Bank.

Use of the Bank's information technology ("IT") resources shall be done as per applicable laws and the Bank's policies. Any failure to comply with such laws or policies shall be

subject to the relevant disciplinary action. Employees shall not use IT resources or any other resources for the purposes of harassment, disclosure of information, or intellectual property theft.

Employees are required to take all reasonable precautions to protect information against unauthorized access, use, disclosure, modification, duplication or destruction.

Employees found misusing/damaging the Bank's property shall be subject to the relevant disciplinary action as per the Bank's Penal Code.

All employees are encouraged to report the misconduct of other employees to the relevant Group Heads and/or HRG so that the appropriate action may be taken as per the Bank's Whistleblowing and Grievance, Problem Solving and Disciplinary policies.

8. Work Etiquette

Work etiquette is related to the general appearance, behavior and daily conduct of the employees at work, and includes, but is not limited to, the following:

8.1 Dress and Personal Appearance

- Employees shall wear and display their identification cards visibly at all times while on Bank premises;
- Employees shall maintain a professional, business-like appearance while at work to preserve the Bank's public image;
- All clothing, footwear and accessories must be in clean and good condition, and consistent with that found in professional business environments;
- Employees shall maintain good personal hygiene and grooming habits. Favourable personal appearance is an ongoing requirement for employment with the Bank;
- Inappropriate clothing shall include, but is not be limited to, the following:
    - See-through or denim ("jeans") materials.
    - Dresses, pants, skirts, tops, blouses, etc. that are short, tight or sleeveless.
    - Shorts; T-shirts.
    - Daraat; Abayat.

- Quarter-length pants; knee-length pants.
- High-heeled slippers; flip-flops.
- Big accessories; Shiny Hijab.
- Includes revealing, torn, or overly casual attire
- Evening or heavy makeup.

- Personal discretion shall be used at all times to use the appropriate clothing.

8.2 Cleanliness and Office Etiquette

Cleanliness and office etiquette are important to promote the positive image of the Bank amongst customers, visitors and society at large. Employees shall:

- Keep their respective work areas and the Bank's premises presentable;
- Refrain from reading the newspaper or having snacks in front desks or in the presence of customers;
- Refrain from using mobile and/or office phones for personal matters in the presence of customers, and shall use mobile phones minimally during working hours; and
- Maintain a professional tone of voice while dealing with customers and/or colleagues.

8.3 Smoking in the Bank

The Bank has a vital interest in promoting employee well-being and maintaining a safe and healthy work environment, and it is expected that employees shall share the responsibility of promoting and maintaining such an environment.

- The Bank and its branches are smoke-free areas. Smoking is strictly prohibited inside the Bank's premises, including Head Office and branch buildings. This prohibition includes "electronic cigarettes";

8.4 Illegal Substance Abuse in the Bank

- Drug, alcohol or any other narcotic substances are considered illegal and are prohibited items. Employees shall not use an illegal drug or alcohol at the workplace or during the performance of their duties, or at the time of operating any of the Bank's assets;
- The unlawful manufacture, possession, distribution, transfer, sale, use or being under influence of any mentioned prohibited items on Bank premises/properties is strictly prohibited and shall lead to disciplinary action as per the applicable Penal Code; and

- The Bank aims to protect and promote the health and safety of all employees. Any incident involving drug, alcohol or substance abuse shall immediately be reported to the HRGGMHRG.

8.5 Office Telephone/Mail Systems

- Telephone courtesy is important. The Bank expects all its employees to be prompt and courteous at all times while using the telephone; and
- Employees are expected not to make and/or take personal calls during working hours or during interactions with customers;

8.6 Use of Bank Assets

- The Bank's assets, including equipment and vehicles essential to completing job duties, are expensive and in some instances deemed difficult to replace. When using the Bank's assets, all employees are expected to exercise due care, ensure the required maintenance is done, and follow the respective set procedure for operation of equipment and vehicles;
- The Bank's assets shall only be used for business purposes. Only authorized Bank personnel can drive the Bank's vehicles and shall practice safe and courteous driving habits abiding by all traffic laws. The use of the Bank's IT resources is subject to the same requirements;
- Employees shall report any damage, defect and/or need to repair any of the Bank's equipment under their care in order to avoid any potential work disruption and/or possible injury to others;
- The improper, careless, negligent, destructive or unsafe use or operation of the Bank's assets shall invite disciplinary action as per the Bank's *Penal Code*;
- Employees shall bear criminal responsibility for any misappropriation of funds/assets assigned for official duties, and shall not falsely claim expenses on the Bank. Employees shall not use the assets or resources of the Bank for personal benefits and shall not indulge in any fraudulent transaction or conversion of funds in Bank or client transactions;

8.7 Solicitation

There may be no general solicitation of funds on any of the Bank's premises, even for an established charity, unless the same has been cleared through HRG.

9. Information and Media Awareness

9.1 INFORMATION SECURITY CODE OF PRACTICE

The Bank's Information Security Code of Practice, which governs the confidentiality, integrity and availability of the Bank's information systems, and ensures the legitimate use of IT, is an integral part of this Code and is to be followed by all employees.

9.2 Confidentiality of Information

As per the instructions issued by the Central Bank of Kuwait ("CBK") to local banks, referring to the confidentiality of clients' information and data; except for cases allowed by the applicable laws and regulations, employees shall not disclose any information, whether in full or in part, during the period of their employment or after leaving work at the Bank, regarding the affairs of the Bank or its customers, or other banks' affairs, which the employee may have become aware of due to the activities inherent in his or her position. Any violation to this obligation exposes the defaulter to legal accountability under the applicable laws that may – if proved – lead to imprisonment and/or fines. Employees are in possession of sensitive and confidential information about the Bank and/or of its customers. Each such information must be kept undisclosed in order to maintain the integrity of individual customer transactions and the Bank's business. Employees shall be under obligation to maintain the confidentiality of such information even after the cessation of their employment with the Bank.

- Employees shall use any information that may have been known to them during the course of regular/irregular work in the Bank strictly for the Bank's approved purposes, and shall share it only with functionaries responsible for such purposes;
- Employees shall, at all times, protect the confidentiality of professional information by disclosing it to only those persons who need to know such information in order to transact any business with customers;
- Employees shall not reveal information concerning a customer to a third party without the customer's consent in writing in accordance with the relevant trade, credit and information arrangements or where the employee is required to do so by law;

- Employees shall not use confidential information, or information acquired in the course of business, for personal gain or for the gain of any other person other than as intended by the Bank;
- Employees shall not destroy, erase and/or manipulate any information obtained in the course of business for the direct or indirect benefits of themselves or of any other person;
- Employees shall exercise due diligence in communication to clients and authorities. Employees are not permitted to convey a promise, forecast or opinion as the official position of the organization without the due authorization of the Bank;
- All internal circulars, notes, product notes or other information are for use solely within the Bank, and shall not be taken, dispatched or shared with anyone outside the Bank;
- Employees possessing confidential information shall not use it in any way that may influence any customer or third party to deal in any transaction; and
- Employees in possession of any unpublished "price sensitive information" are – without following the required disclosure as per the applicable laws and regulations – prohibited from trading in the Bank's securities. "Price sensitive information" is information that is generally not available publicly but, if it were, is likely to materially affect the price of those securities.

9.3 MEDIA AWARENESS

- Notices of an official nature and information of general interest are communicated to employees regularly through circulars, electronic media, the Intranet and other channels by HRG. It shall be the responsibility of each employee to frequently and regularly access various means of communications, including the Intranet, to keep themselves up-to-date with the information provided;
- Any information concerning the Bank's business, activities, financial performance, products, policies, processes, procedures, transactions, future plans, strategies, its customers, suppliers, copyright information (e.g. music, videos, text, photographs, etc.) which is not in the public domain, and to which an employee has access to or has possession of, including information designed as "Internal", "Confidential" and "Restricted", must be considered confidential. This information is for internal use only and not to be divulged to any person outside the Bank. In case of any doubt regarding the confidentiality of information, employees shall consult with the Corporate Communications Department;

- Employees shall not provide any information, either formally or informally, to the press or any other electronic media, including on social media, unless specifically authorized. This confidentiality shall continue to apply to employees even after they cease to be in the employment of the Bank. All employees having, in one way or another, access to various internal information of the Bank's business, activities, products, policies, processes, procedures, transactions, future plans, strategies and the like, shall use this information for internal use only and shall not divulge it to any person outside the Bank. If such information is to be communicated, it shall be done through the official communication channels of the Bank only;
- Employees shall not make any defamatory/offensive remarks in any media, particularly through social media, concerning the Bank, its employees or former employees;
- Employees in general, with the exception of Management Executive Committee members, are not authorized to directly interact with the electronic or press media. Any query from the media must be routed through the Corporate Communications Department for response. The Corporate Communications Department only shall be responsible for interaction with the media and for giving any information concerning the Bank or its work;
- Employees shall maintain sanctity of information, whether written, oral or electronic, at all times. Any information being divulged, internally or externally, shall be regarded as a serious breach of trust and may, in serious cases and after adequate proof, lead to dismissal for cause as per the applicable laws and policies;
- Employees shall not commit any action on behalf of the Bank unless they are duly authorized to do so. In case of any doubt, employees shall consult with the Corporate Communications Department;
- Employee References generated by HRG shall be the only authorized channel to respond to any reference check from any third party, and to issue reference letters for current and former employees. For this purpose, HRG shall seek any required information from concerned departments;
- Employees, including managers, except in HRG, shall not provide any information about current or former employees of the Bank to anyone outside the Bank;
- HRG will release such information related to current employees only with the written consent of the employee;
- In addition to the forgoing, HRG may only provide information regarding employees to a

third party after obtaining the approval of the GMHRG;

- Employees shall immediately notify their Group/Department Head and HRG, through the Staff Information Form available on the Intranet, whenever any change in their personal status (including marriage, birth of child, change of place of residence, etc.) occurs that may affect the employee's benefits or has an impact on the communication address of the employee' and
- Employees should inform HRG immediately of any sensitive information related to staff accounts or an employee file that is visible/editable in the public domain.

10. Professional Principles

10.1 Dealing with Customers

- Employees shall carry out all transactions only within the guidelines and defined procedures of the Bank. Any transactions that entail any exception to the Bank's defined procedures shall be referred to the concerned persons and shall be carried out only after prior approval from the concerned authorities.
- All new clients are required to undergo an identification and approval process. The day-to-day responsibility for identification/approval of new clients in accordance with the Bank's processes lies with Account Managers and their respective Branch Managers;
- In maintaining relationships with clients, employees are expected to be prudent. No transaction shall be undertaken for customers who have failed to provide evidence for their identity or failed to provide the necessary information as required by "Know Your Customer" guidelines;
- Employees shall ensure that appropriate and clear instructions are obtained from clients prior to conducting any transaction;
- Clients shall be given reasonable time and notice of any variation in the terms and conditions of a transaction. Verbal notifications/requests shall be followed up by written confirmations;
- Employees shall not engage in any transaction for a customer which is unsuitable for that customer and shall report the incident to the Bank's Group Anti-Financial Crime Department as per the applicable policy;
- While serving customers, in their best interest, employees shall comply with all

applicable laws, regulations, policies and procedures, as well as all applicable banking standards. All information relating to any fees, costs, expenses and charges shall be made available to customers before they are accrued; and

- No written recommendations shall be issued to customers unless the employee issuing them is authorized by the Bank to do so, and is satisfied that the research is competent and reliable and that the recommendation area is among the Bank's licensed activities. All such recommendations must contain the Bank's standard disclaimer and additional clauses as required.

10.2 Monitoring Business Relationships of Employees

- Business relationships shall not be used for personal gain (financial or non-financial) by employees or their relatives or associates;
- The Bank shall have the right to examine employees' business relationships with any customer at any time throughout the association of the employee and customer with the Bank in order to determine whether the employee is performing his/her role as per the requirements of the business undertaken and the legal/social environment in the country;
- In a transaction where two or more customers come into competitive or opposing positions with each other, the employee shall not act for more than one customer without the consent of the each of them; and
- Employees shall not give investment advice to customers unless the employee has reasonable grounds to believe that the advice or transaction is suitable for the customer concerned. Any advice given by an employee to a customer shall include the Bank's standard disclaimers and shall be within the area of activities that the Bank is licensed to conduct.

10.3 Periodically Update Customer Information

- Any alteration to the Bank's records shall be made only in accordance with the authorization procedures laid down;
- Employees shall not make, or allow to be made, any entry, alteration or deletion in the records of the Bank which is false, misleading, or which may obscure the nature of any transaction; and

- Documentation on customer relationships and transactions shall be maintained such that:
    - Any transaction affected can be reconstructed and retrieved.
    - Any enquiry and order from the authorities relating to disclosure of information can be satisfied within reasonable time.
    - It is possible to identify a person as a customer/beneficial owner of an asset deposited with the Bank; it shall also be possible to identify the current/deposit account and safe deposit facilities of the customer.
    - It is possible to identify and take action/recognize customers who have availed certain facilities from the Bank.

10.4 Bribery

- Employees shall not bribe customers, or solicit or receive favors from them, in exchange for granting favorable terms and/or conditions or any other services which are generally not extended to other customers;
- Employees shall not seek or accept any offer, payment, promise to pay, or authorization to pay any money, gift, donation, remuneration, hospitality or favor, in whatsoever form and howsoever described, from customer, suppliers, shareholders/stakeholders or similar, that is perceived as intended, directly or indirectly, to influence any business decision, any act or failure to act, any commitment of fraud, or opportunity for committing any fraud. Gifts include all items with the exception of items such as diaries or calendars with a corporate logo; and

- Wherever it is unavoidable to accept gifts due to client sensitivity, or the value of the gifts received is more than KD 250/- (approximately), such gift items are to be declared to HRG by completing the form available on the Intranet.

10.5 Interaction of Employees In/Out of the Bank

It is the policy of the Bank that all employees shall be able to enjoy a work environment free from all forms of misbehaviour, including discrimination or harassment from supervisors, colleagues, vendors, consultants, visitors and customers.

Discrimination and harassment, whether based on a person's race, gender, gender

identity or expression, color, religion, national origin, citizenship, age, disability, marital status, sexual orientation or ancestry are repulsive and completely inconsistent with the Bank's tradition of providing a respectful, professional and dignified workplace.

- Employees shall not misbehave with clients or colleagues inside or outside the Bank's premises;
- Employees shall not use their position to intimidate or secure undue advantage from any other employee or external person inside or outside the Bank;
- Misbehavior by employees may result in disciplinary action up to and including termination of the employee who misbehaved, in accordance with the Bank's Penal *Code*;
- False accusations of misbehavior shall lead to severe disciplinary action, up to and including termination in accordance with the Bank's Penal *Code*;
- Sexual harassment can consist of a single instance or multiple, persistent or pervasive acts, and does not have to be explicitly sexual in nature. Any behavior which ridicules or denigrates a person because of his or her gender may be deemed harassment; and
- Any form of sexual advance or request for sexual favors by colleagues and/or line managers with a fellow employee is unacceptable and shall be dealt with the appropriate disciplinary action as per the Bank's Penal Code;

11. Personal Account Dealings and Financial Transactions

11.1 Managing Personal Staff Accounts

The Bank's policies regarding personal account dealings apply to:

- Any person on secondment to the Bank;
- Any person working under contract with the Bank; and
- Any person on temporary employment with the Bank.

Employees shall maintain financial discipline and complete transparency and integrity in all their financial transactions.

- Employees shall be allowed to open only one salary account upon joining the Bank. The employee's salary account is provided primarily to facilitate salary and other credits from the Bank;

- Employees shall be provided one Client Identification File ("CIF") number. Any other account opened by the employee shall be linked to the employee CIF number;
- Employees shall use this account only for their own personal transactions and not for those of their family, relatives, friends or other known persons;
- Any transaction in the employees' salary account shall be subject to scrutiny for AML purposes and under this Code by the Bank's Payroll Department, and employees are required to provide suitable explanation and documentation for specific debits or credits. Employees shall respond to any query raised by HRG related to any transaction done through their salary accounts. Failure to provide response shall lead to escalation to the employee's General Manager, and shall attract further investigation as may be required;
- Any employee engaging in a large financial transaction that is to be routed through his/her personal account is expected to inform the Payroll Department in advance, via E-mail, of the details of the transaction. In certain cases, where deemed necessary, the employee may be asked to provide supporting documents pertaining to the transaction;
- As bankers, employees shall ensure that they maintain the required amount of balance in their accounts at all times. If any cheque issued by the employee bounces due to inadequate balance, the employee may be exposed to legal accountability as per the applicable laws, and disciplinary action as applied pursuant to the Bank's *Penal Code*;
- Employees shall be permitted to open a fixed deposit account under their employee CIF number only;
- Charges on employee accounts shall be waived as per the applicable policies of the Bank;
- Under no circumstances should employee accounts be overdrawn. However, the employee account is overdrawn by forced debit or other methods, the employee shall be allowed 3 working days to clear his/her accounts after due written notification. Any exception shall require the approval of HRG; and
- Any employee with an overdrawn balance shall receive a warning letter for the first two incidents from HRG. Thereafter, the employee shall be subject to disciplinary action as per the Bank's *Penal Code*.
- Except as provided for herein, or in any relevant policies, employees' personal banking transactions shall be governed by the same rules and procedures as are set for the general public.

- Employees are expected to carry out their financial obligations promptly so that creditors shall not have to ask for the Bank's assistance in collecting amounts owed to them. In case a creditor obtains a garnishment on an employee's earnings, the Bank is required by law to deduct the necessary payments. Repeated garnishments are indications of financial irresponsibility and may lead to disciplinary action as per the Bank's *Penal Code*.
- Employees are expected to be prudent in their personal borrowing, investments, business and other activities to ensure that they do not put themselves in a position in which their personal interest, financial or other, might influence or give the appearance of influencing any action they take, judgment they make, or advice they give on behalf of the Bank.

11.2 Employee Misrepresentation

Employees shall not act or engage in any course of conduct which creates a false or misleading impression as to the market in any investment or the price or value of any investment. Examples of this kind of behavior include, but are not limited to:

- Creation of a false or misleading appearance of active trading;
- Stock market manipulation;
- Willfully making or disseminating statements or information that are false or misleading; and
- Fraudulently inducing persons to deal in securities by any dishonest concealment of material facts.

11.3 Financial Dealings

- Employees are prohibited from dealing in an investment if they know that the Bank, or an organization or individual associated with it, intends to publish a research recommendation, and that the recommendation is likely to cause a price change in the investment, and shall not derive benefit or assist others to derive benefits by giving investment advice from the access to and possession of information about the Bank not in public domain and therefore constitute insider information. In such a situation, the employee shall not deal until the recommendation has been published and the customers for whom it was principally intended have had an opportunity to react to it. As per CMA law 7/2010 and its executive bylaw, all employees are required to comply with CMA insider information requirements. Employees involved in any aspect of

research shall always have access to sensitive information of an investment or sector in which they deal. Dealing in personal investments in such companies/sectors by an analyst shall be prohibited in the following scenarios:

- While they are actively researching the investment.
- While they are involved in a company visit.
- While they are preparing a research report.
- While they are advising customers on the merits of that investment.

Additionally, such analysts are prohibited from counselling or procuring any other person (other than customers of the Bank) to deal in such investments.

- If an employee is aware that the Bank has accepted a customer's order or has made a decision to deal for a discretionary investment service on behalf of a client, then the employee shall not make a personal deal until the relevant customer order or decision has been executed or cancelled;
- Employees are prohibited from making a personal deal in any investment or related instruments if they know that the Bank intends to acquire a position in that investment or related instruments;
- Employees shall not sell investments to, or buy investments from, a client for the benefit of their own or a connected person's account. Employees shall not operate a personal dealing account with any broker/dealer with whom they have a professional dealing relationship as part of their normal duties as employees of the Bank; and
- All employees shall avoid personal guarantees for others' indebtedness, and when inevitable shall seek prior permission from the Group Anti-Financial Crime Department for the same.

11.4 Speculative Transactions

- Employees shall not engage in speculative dealings (as distinguished from investments), whether on a margin or a cash basis, or in securities, commodities, real estate or exchange. Frequency of trading and use of credit shall be significant factors in determining whether dealings are speculative;
- The Anti-Financial Crime Group and HRG can investigate an employee's securities trading activity if it seems to indicate that there is excessive personal account trading or any other unusual pattern of transactions; and

- HRG shall ensure monitoring of the accounts and report any action to the HRGGM - HRGG, who shall in turn put forward recommendations to the GCEO with a copy to the Board Audit Committee ("BAC") and the Board Nominations & Remuneration Committee ("BNRC").

12. Money Laundering and Corruption

The rules concerned with money laundering are defined to encompass any intentional conversion, transfer, concealment, possession, or the aiding of any such action, of the proceeds of criminal activity, whilst knowing that such proceeds are derived from criminal activity.

The Bank is required, under the applicable laws and CBK regulations, to take steps to combat money laundering and terrorism financing. The Bank gives AML training to each employee and provides copies of the prevailing laws and CBK regulations to its employees to read and comply with the guidelines therein.

Employees shall be fully alert to the possibility that funds handled in transactions by financial institutions might be used for, derived from, or intended for, criminal or terrorist purposes.

The Bank strives, hand in hand with employees, to prevent money laundering & terrorist financing by endeavoring to thoroughly identify the parties being transacted with along with the identification of transactions contemplated thereby, as per the standards published within the Bank's related Policies and Procedures.

- Transactions involved in money laundering are difficult to distinguish from normal, everyday transactions. Employees are required to diligently follow the procedures laid down for accepting funds, account transactions, inward/outward remittances, and especially large or unusual transactions;
- A similar approach must be followed in verifying the consistency between customers' assets held by the Bank and what is known about their financial situation and objectives as stated in Account Opening Forms;
- Employees are required to report any suspected case of money laundering, with respect to a specific transaction or a customer, immediately to their line manager/General Manager and the Group Anti-Financial Crime Department; an
- The Bank is determined that none of its constituent operations shall be a channel for funds for a criminal origin. The bona-fides of all customers shall be established and any

suspicious transaction shall be reported in line with the current operating procedures. The Bank shall not overlook any discovery of transactions where criminal involvement is suspected.

13. Prevent Misappropriation of Funds/Assets of The Bank

Employees shall be liable for any misappropriation of funds/assets assigned for official duties as per the applicable laws and regulations.

Employees shall not falsely claim expenses on the Bank.

Employees shall not use the assets or resources of the Bank for personal benefits.

Employees shall not indulge in any fraudulent transactions and unlawful conversion of funds in Bank or client transactions.

14. Compliance with this Policy

It is a condition, whether express or implied of the statement of terms and conditions of employment of each person employed with the Bank, and a condition of secondment of staff from other Group offices and entities, that they shall comply at all times with the Bank's Employee Code of Conduct. The document shall be made available to all employees on the Bank's Intranet. It shall be the responsibility of each employee to make himself or herself aware of the provisions of the Employee Code of Conduct and comply with the same.

This policy may not necessarily cover all the appropriate behavior for every situation which an employee may confront. The Bank shall rely on each employee to make an individual judgment of what is right and proper in a particular situation, and in case of doubt, seek guidance from his/her supervisor for direction.

15. Implementation of this Policy

The Bank, in the event of violation of these rules, shall take corrective, disciplinary or legal action(s) as appropriate.

Employees desiring guidance and interpretation of these rules may contact their respective General Manager. General Managers can contact HRG management for any clarifications.

Senior Management shall be responsible for implementation of this Code throughout

the Bank. They shall ensure that employees in their respective groups are fully aware of, and are following the provisions of, the Code. Senior Management shall monitor compliance and initiate action whenever the desired standards of integrity are not being met. They shall, as soon as possible, inform HRGGM - HRGG of any deviation from the standards set in this policy for necessary action as per regulatory requirements and the Bank's policies.

Similarly, individuals who have concerns about the operation of this policy shall raise these through their managers. In the event that these concerns remain unresolved, employees shall contact respective GM/ AGM/ DGM. If the concerns are still unresolved, GM - HRGG HRG shall be contacted. Any violations or doubts can be also reported as per the Bank's Whistleblowing Policy. Anonymity shall be ensured, subject to legal and regulatory disclosure requirements.

The decision of GM - HRGG HRG shall be treated as the final interpretation of the alleged breach or violation of the Employee Code of Conduct at management level, and GCEO at Senior Management level.

Any employee not satisfied with such decision may request it to be reviewed by the Chief Internal Auditor ("CIA"). Applications for such review shall be sent in writing to the GCEO with a copy to GCHRGO and CIA together with all pertinent documentation for further in-depth studies.

Abbreviations

Abbreviation	Description
AML	Anti-Money Laundering
BAC	Board Audit Committee
BNRC	Board Nominations & Remuneration Committee
CIF	Client Identification File
CIA	Chief Internal Auditor
Code	(Employee) Code of Conduct
ERM	Employee Relations Manager
GCEO	Group Chief Executive Officer
GM-HRG	General Manager – Human Recourses Group
Group	Burgan Bank Group
HRD	Human Resources & Development Group