



البنك السعودي للاستثمار
The Saudi Investment Bank

Employee Code of Conduct

General

- Banking is a business based on honesty, integrity and mutual trust. Employees at all times should conduct themselves in a manner that will safeguard the integrity and reputation of the Bank. Employees are required to make every effort within the scope of their position, to achieve the Bank's objectives, look after the Bank's interests and maintain its assets, properties and funds, as well as, all confidential information, documents and the integrity of Banks records. Employees should perform their duties satisfactorily and refrain from any prohibited acts, as stated below. Employees involved in any prohibited activities will be subject to disciplinary action and penalties in accordance with Bank policy and laws and regulations issued by the Ministry of Labor and other regulatory authorities in the Kingdom of Saudi Arabia.
- Compliance with local regulatory laws, rules and regulations is one of the most important factors for the success of the Bank. Compliance protects the reputation and credibility of the Bank, protects shareholders, clients and depositors, and provides safeguards to the Bank against legal, financial, reputation and regulatory risks.

Adherence to Policies, Procedures and Regulations

- Employees should observe the business hours of the Bank.
 - Employees should perform their duties honestly, accurately and properly and dedicate all working hours to perform their duties.
 - Employees should wear and exhibit SAIB ID card while on duty.
 - Employees should comply with departmental instructions.
 - Employees should comply with the Bank's policies and procedures and with laws, rules and regulations issued by SAMA, CMA and all other related regulatory authorities and avoid the violation of the policies and procedures, laws, rules and regulations intentionally or unintentionally.
 - Employees should comply with all Laws and Regulations of the Kingdom of Saudi Arabia and all rules and directives issued by the Government of the Kingdom of Saudi Arabia from time to time and abide by the traditions and public convention.
-
- Employees should inform their immediate supervisor or the management of any failure, offence, or violation by whomever in respect of the implementation of the laws, rules, regulations and systems.
 - Employees should not take any action that violates any applicable law, rule or regulation. To avoid legal or compliance difficulties, employees should seek any necessary advice from their immediate supervisor or the Head of Compliance prior to the commencement of business dealings.
 - Employees should cooperate with internal and external investigations, audits and regulatory examinations in a forthright manner and should provide honest, accurate and timely information.
 - Employees, unless preauthorized, should not provide information about the Bank to any external authority.
 - Employees should not participate in any religious or political discussion or debate during working hours.

- Employees should not sleep during working hours or excessively read newspapers or magazines at work.
- Employees should not leave the Bank during working hours without prior authorization from their immediate supervisor.
- Employees should not be absent from work or overstay their approved leave without prior permission of their immediate supervisor or Human Resources Group.
- Employees should not access Bank premises outside working hours without prior written permission from their immediate supervisor. This does not apply when an employee visits a branch to perform a normal banking transaction.
- Employees should not enter any restricted work areas designated for authorized employees unless their entry is related to a business need.
- Employees should not receive personal visitors at the work place during or after the Bank's business hours. In emergency cases, prior permission should be obtained from their immediate supervisor.

Co-operation and Respect

- Employees should maintain the dignity of the job, reputation of the Bank and deal with colleagues and management respectfully.
- Employees should cooperate with Management and colleagues in achieving the goals, improving the productivity and reducing costs of the Bank.
- Employees should refrain from spreading false or malicious rumors.
- Employees should strictly avoid any behavior, language or gestures that are offensive to other staff members, customers or the public. This includes all forms of discrimination, harassment, and other acts which might be interpreted as disrespectful to individuals or groups, men, or women. Strict adherence to the acceptable cultural norms in Saudi Arabia should guide the dealings with others of different gender.

Confidentiality

- Employees should maintain the confidentiality of information which belongs to or concerns the Bank's customers, suppliers, agents, distributors, employees, advisors, consultants, etc.
- Employees should not collect, record, publish, or communicate to any third party any such information or any other matter whatsoever without the written approval of the Bank.
- Employees should not retain any documents, reports or information related to the Bank, its customers or employees, without authority or divulges such information to any third party without the prior written approval of the Bank.

Protection of Proprietary Information and Intellectual Property

- Employees should not access, use or disclose any restricted, confidential, or internal information about the Bank without the written approval from their immediate supervisor.
- Employees should not remove any proprietary information from the Bank's premises without approval of their immediate supervisor.
- Employees should not give testimony about the Bank or general industry policies or business practices in a legal proceeding not involving the Bank as a part without prior written approval from the Bank's legal counsel and
 - Executive Management.
- When employees leave the service of the Bank, they should continue to safeguard the confidentiality of both customers and employees, and protect the confidentiality of the Bank's business indefinitely.
- Employees should not use customer information including names, lists, profiles data, etc., in subsequent employment situations.
- Employees should return to the Bank any customer or proprietary information they have in their possession, when they leave the service of the Bank.

- Employees should understand that should they leave the service of the Bank, any intellectual property they created for the Bank or while using the Bank's resources or if compensated for, in case not using the Bank's resources remains the Bank's exclusive property.

Financial Dealings

- Employees should not borrow, lend, or stand as a guarantee from/to any of the Bank's employees, customers, contractors, or any party having a relationship with the Bank.
- Employees should promptly settle their obligations towards third-party debts.
- Employees should not be involved in any unauthorized transactions (commercial or otherwise) on the account(s) of other employees or any other third party.
- Employees should claim only those expenses that are eligible for reimbursement under the Bank's expense policy guidelines. Intentional use of expense accounts for personal purposes represents misappropriation of the Bank's funds.

Conflict of Interest

SAIB commits itself and its employees to make every effort to look after the Bank's interests as supreme, maintain its assets, funds, properties and integrity of Bank records in the best possible manner. SAIB's high level credit controls and overall operating environment (e.g. concept of credit committee approvals versus individual authorities, annual review of activity over staff accounts, involvement of at least two staff in negotiating/signing contracts, acceptance of gift policy etc.) minimizes the possibility of compromising the Bank's interests.

The following specific guidelines (dos and don'ts) must be complied with by the staff to ensure safeguarding of the Bank's and its shareholders' interests. In the event of noncompliance with the below established guidelines by an employee or the Bank noticing any instance of conflict of interest involving a customer and a Bank representative/employee, the Bank will investigate the matter and take appropriate action against the concerned employee and may disclose the findings to the concerned customer, if deemed appropriate or necessary.

- Employees should not make use of their position in the Bank for personal gains, which will be detrimental to the interests of the Bank, its shareholders, directors, customers or employees.
- Employees should not misuse their authority to grant more favorable terms to any client, colleague, relative, or any other third party.
- Employees should not hold directorships in any organization, commercially oriented or otherwise, without the prior written approval of the Bank.

- Employees should disclose the employment of relatives at the beginning of their employment with the Bank and whenever a relative is recruited by the Bank or whenever employees become relatives by way of marriage.
- Employees should not enter into contractual engagement in any professional, technical, or academic activities, other than their official duties, irrespective whether such activity attracts a fee or not, without the prior written approval of the Bank. This applies to within and outside working hours.
- Employees or associates should not receive or accept any commission, rebate, discount, gratuity, or profit from any person, company or firm having business transactions with the Bank.
- Employees should not derive any profit or benefit either directly or indirectly from knowledge acquired through their employment in the Bank.
- Employees should not act with self-interest whether direct or indirect when negotiating/concluding agreements, tenders or contracts that are related to the Bank's business.
- Employees should not accept any form of inducement from customers, suppliers or any other parties, doing or seeking to do business with the Bank if the underlying reason for the inducement is not strictly related to business on an arm's length basis. This includes out-of-office or out of working hours offers of social functions, meals or travel and excludes invitation to social events of a public nature.

Notwithstanding the foregoing guidelines, should an employee be approached by a customer/non-customer for a product or service that may contravene any of the above instructions and potentially create a conflict of interest situation, the concerned employee should document the instance and report the same to his immediate supervisor with copy to the GM, Human Resource who will decide on any further action if considered necessary.

Receiving Gifts

- Employees should observe the highest standards of integrity and fair dealing in the performance of their duties. Employees should neither solicit nor accept any gift or inducement in cash or kind from any party that may directly or indirectly affect their job performance.
- In case an employee is unable to refuse the gift, such employee should declare this matter to his/her immediate supervisor in writing with a copy to Human Resources Group. The information should include:
 - Description and value of gift.
 - Giver and receiver of gift.
 - Reason for giving/receiving gift.
- Whether prior written approval was obtained from senior management to accept the gift.
- Employees should not be involved in any act that could be interpreted as seeking, receiving or dispensing a bribe, kickback or questionable payment.

Free Competition

- Employees, especially those who work in a sales function or as front line staff, should use only fair and honest sales and negotiating methods. At the same time, they should avoid any sales practices that could be misconstrued as an attempt to impose undue pressure on or coerce a client into obtaining a product or service from the Bank as a condition of closing a sale.
- Employees should avoid any collusive, anti-competitive discussions and/or agreements with competitors.

Bank Representation

- Employees should not make speeches or publications or issue media releases or accept any function as a representative of the Bank, whether remunerated or honorary, without obtaining prior written approval from the Bank.
- Employees should not give any testimony or offer any guidance or experience related to the business and activities of the Bank without obtaining prior written approval from the Bank.
- Employees should not use Bank stationery or other Bank property for purposes other than their official duties.

Prevention of Criminal Activities

- Employees should not be involved in any criminal activity or in money laundering transactions.
- Employees should report promptly all types of suspicious, fraudulent, dishonest, unethical, inappropriate transaction or conduct by colleagues, subordinates or supervisors to the Fraud Prevention & Detection Unit and to the Head of Compliance.
- Employees should familiarize themselves with the Fraud Prevention & Detection Policy Manual and The Whistle Blowing Policy issued by the Bank to ensure strict compliance.

- Employees should report promptly all types of compliance violations of local laws, rules and regulations and the Bank's rules and regulations by colleagues, subordinates and supervisors to the Head of Compliance Department.
- Employees should report promptly any suspected money laundering activity or transaction to the Bank's Anti-Money Laundering Unit.
- Employees must familiarize themselves with the Bank's Policy Manual on
- Prevention of Money Laundering & Combating Terrorist Financing to ensure strict compliance.
- Employees should not alert customers or other related parties about suspicions of their activities under investigation by the Bank or the reporting of suspicious transactions by the Bank to the regulatory authorities.

Bank's Properties & Asset

- Employees who hold funds or assets of the Bank under their custody will be personally responsible for the safety of those assets and funds. Employees should ensure they are used only for business purposes.
- The Bank Management has the right to inspect and check any Bank assets under employees' custody at any time including the safes and offices.
- Employees should protect Bank's properties and assets against any form of misuse. If an employee comes to know of any such acts, he/she should immediately bring it to the attention of his/her immediate supervisor or Senior Management.
- Employees should not photocopy any document or text not related to the employees' work without obtaining prior permission from the immediate supervisor.

- Employees should treat all inventions, improvements to techniques and information technology systems used or developed by the Employees during their services with the Bank as property of the Bank.
- Employees should not misappropriate funds, property or other assets, or knowingly assist another individual to do so.
- Employees should not convert any assets that do not belong to them, or use them for the benefit of their self or anyone other than the rightful owners. Employees should not knowingly assist another in this pursuit.
- Employees should not access the Bank's safes/vaults unless authorized to do so.

Insider Information

- Employees may sometimes be privy to confidential information concerning the affairs of the Bank, a client, a potential client, a supplier, or other company whose securities are publicly traded on a stock exchange. This knowledge is referred to as "insider information." Possession of insider information is legal, but the misuse of it is illegal. If an employee has access to insider information, he/she should clearly recognize this distinction.
- Employees should not discuss or pass on insider information unless the exchange is necessary for a specific Bank business purpose.
- Employees should not trade in stocks or securities or recommend or advise others to do so, on the basis of insider information they have acquired through their job. It is unethical and illegal.
- If an employee believes that he/she has come into possession of insider information, he/she may not execute any trade in the securities of the subject company without consulting the immediate supervisor and the Head of Compliance.

Copyright

- Employees should follow the specific terms of the licensing agreement issued by the publisher of any computer software program used in the course of business or on a computer owned by the Bank.
- Employees should exercise care when making copies of printed or recorded material and software, and they should respect any prior approval requests required by the copyright holder.
- Employees should not install or use any software not licensed for use by the Bank on any Bank-owned computer.
- Employees should not copy software programs licensed to the Bank for use by others, except as permitted by the copyright or licensing agreement. The use of any copies is to strictly comply with the licensing agreement and the Bank's guidelines.
- Employees should not use the Bank's name or logo to identify his self or herself in non-business social media forums.

Clean Desk Policy

- Employees should keep on their desk only the documents that are currently being processed. Other documents must be kept in a drawer or preferably under locked custody.
- Employees should sign-off their workstation terminal when leaving their desk.
- Employees should shred unwanted documents that contain sensitive or customer information.
- Before leaving office, employees should file all processed transactions and documents in their respective files and keep them in locked cabinets. They should keep their desk drawers locked.
- All customers' security documents should be kept in fire-resistant cabinets overnight.

Use of Telephone and Fax

- Use of telephone and fax at the Bank should be for official business and work purposes only.
- The duration of any international calls on business matters should be kept to a minimum.
- Employees should obtain prior written approval of the department head for any international calls and the cost of any personal calls will be borne by the employee.
- Employees should not allow any customer or third party to use the Bank's telephone or fax. In case of emergency or for business related matter, employees may allow a customer/third party to use the Bank's telephone/fax provided the employee is present during the full conversation/has seen the content of the fax document.

Use of Electronic Mail System

- The Bank maintains an electronic mail system. This system is provided by the Bank to facilitate the conduct of its business. It should not be used for any personal matter.
- The electronic mail system is the property of the Bank. Additionally, all messages composed, sent, or received on the electronic mail system will remain the property of the Bank. They are not the private property of any employee.
- Employees should not use the Bank's electronic mail system to create any offensive or disruptive messages.

Note:

A message may be construed as offensive or disruptive, if it contains sexual implications, racial slurs, gender-specific comments, or any other comment that offensively refers to someone's age, sexual orientation, religious or political beliefs, national origin, disability or any other matter that is detrimental to the interests of the Bank or its stakeholders.

- Employees should not use the Bank's electronic mail system to send or receive jokes, humor, politics or pornography, nor engage in Internet shopping or chatting of a personal nature.
- Employees should familiarize themselves with the Bank's Guidelines on the Use of Bank E-Mail to ensure compliance.

Use of Information Technology/Information Security

- Employees should follow the Bank's policies, procedures, and standards relating to Information Technology, Information Security and Confidentiality.

Any observed or suspected Information Technology, Information Security Or Confidentiality incidents or lapses should be reported promptly to the Bank's Information Systems Security Officer.

- Employees should not use the Bank's computer systems to access, transmit or download games or obscene or offensive material.
- Employees should not abuse, compromise or share the passwords issued to them by the Bank.

Dress Code and Personal Appearance

- Employees should ensure that their appearance projects a professional image including clothing and personal grooming.
- Employees should wear clean and well-pressed clothes at work in the Bank.
- Employees should be conscious of and sensitive to the local culture, traditions, and customs.
- The Dress Code Policy is designed to guide employees on the standards of dress and appearance. It is SAIB's intent that work attire should complement an environment that reflects an efficient, orderly, and professionally operated organization.
- In accordance with this policy, discretion and professional common sense must be used with regard to appearance, grooming, hygiene, appropriateness, style, etc.
- Failure to adhere to the rules of this dress code policy will result in corrective action. Employees who show up to work and are dressed inappropriately based on the specified guidelines will be verbally warned. Additionally, a note documenting the incident will go into the employee's personnel file.
- The employee will receive a warning letter if this occurs a second time. Should adherence to the dress code continue to be a problem, further corrective action will be taken as per human resources policy, up to and including

Termination of employment.

General guidelines for all branches employees (including non-customer contact staff):

- Good personal hygiene and grooming is required.
- Clothes must be clean, neatly pressed and in good condition.
- All employees are supplied with SAIB nametag, which must be worn and visible at all times when on duty.

Saudi Male Employees:

- Shmagh/ghutra to be always worn.
- Only white or cream white thobe with no extreme embroidery is allowed. However, dark color thobe is allowed during the winter.
- Thobe collar buttoned up at all times.
- All staff are required to wear closed-toe shoes (dress up shoe), shoes must be worn at all times.
- Hair must be off the face, cut over collar and not visible underneath shmagh/ghutra.

Non-Saudi Male Employees:

- No t-shirts nor jeans are allowed.
- Only long sleeve shirts, not rolled up, of plain colour are allowed; May wear a jacket and during the winter a sweater.
- Should wear a neck tie. (no butterfly ties)

Female Employees (Branches):

- Long formal black skirt.
- Black vest.
- Black formal jacket.
- Closed formal shoes.

Female Employees (other than branches):

- The traditional dress code (Abaya + Head Cover) is a must for all female staff in all public areas of the bank.
- Closed formal shoes.
- Hair must at all times be fully covered.
- There should be no excessive use of cosmetics, makeup, or accessories

