Code of Conduct

1. **Business Ethics and Compliance with the Law**

a) You must protect and enhance the assets and reputation of Pak EXIM.

i. Honesty and integrity are cornerstones of ethical behavior. Trustworthiness and dependability are essential to lasting relationships. Our continued success depends on doing what we promise.

ii. In our rapidly evolving businesses, each of us is challenged by a complex environment, which often requires a fast response under pressure. No written policy can anticipate every ethical dilemma or definitively set forth the appropriate action for all business situations. Accordingly, rather than a set of specific policies and procedures, this Code, emphasizes a standard of ethical conduct that must permeate all our business dealings and relationships. The Bank relies on your good judgment in applying these standards.

b) You must conduct business in accordance with applicable laws and regulations and the Code.

You should consult the Bank's Compliance and/or the HR Division whenever you have a question about the legality of a course of action. You must also exercise the utmost care to ensure that all statements you make are accurate.

c) Managers/Supervisors, by virtue of their positions of authority, must be ethical role models for all employees.

i. An important part of a manager's responsibility is to exemplify and exhibit the highest standards of integrity in all dealings with fellow employees, customers, suppliers and the community at large. An equally important responsibility is to obtain employees' commitment — and develop their ability — to make sound ethical judgments. Managers must communicate the seriousness of the Bank's expectations for ethical conduct and their own personal support of these expectations. Ethical leadership includes both fostering a work environment that encourages employees to voice concerns or otherwise seek assistance if faced with potentially compromising situations and supporting those who speak out.

ii. Managers/Supervisors must be alert to any situations or actions that may be unethical or potentially damaging to the Bank's reputation and must respond appropriately. Managers must take prompt action to address such situations and actions and must avoid even the appearance of implicit approval.

2. Treatment of Employees and Others

a) You must treat colleagues, employees and others with whom you interact with respect and dignity.

Treating all employees and others in the workplace with respect and dignity is part of the Bank's values that applies to everyone. This is particularly important for leaders, who must be role models for their direct reports. Employees are likely to treat their colleagues, including those whom they manage, as they themselves are treated. The Bank expects leaders to seek out the ideas of employees and to involve them in decisions whenever appropriate. At the same time, once a decision is made, everyone involved is expected to pull together and support it.

b) Safety, Health and the Environment

You must comply with all applicable laws and Bank policies relating to safety, health and the environment.

(i) The Bank is committed to high standards of safety and employee protection. Meeting this commitment is the responsibility of each employee. To that end, the Bank shall comply with all applicable government safety, health and environmental regulations, and establish systems to provide a safe and healthy workplace.

(ii) You also are responsible for working safely to avoid risk to yourself and colleagues, identifying and reporting unsafe working conditions or breaches of security, and reporting injuries in the workplace.

c) Diversity, Equal Employment Opportunity and Freedom from Harassment

You must support the Bank's commitment to diversity and equal employment opportunity. You also are expected to create a work environment free from intimidation and harassment.

(i) The Bank seeks and values diversity among its employees, recognizing that a mix of people enriches our Bank and is essential to creativity and business growth. We are committed to equal employment opportunity and unbiased treatment of all individuals based on job-related qualifications and without regard to race, color, gender, age, national origin, religion, creed, sexual orientation, gender identity, marital status, citizenship, disability, veteran status or any other basis prohibited by law.

(ii) The Bank's policy is to create a safe working environment that is free from harassment, abuse and intimidation. It will also enable higher productivity and a better quality of life at work.

Harassment includes behavior that is offensive and interferes with an employee's work performance or creates an intimidating, hostile or offensive work environment. Examples of potentially offensive behavior include unwelcome sexual advances or remarks; slurs, jokes or disparaging comments about race, ethnicity or sexual orientation; and business meals or entertainment at sexually suggestive venues.

3. **Conflicts of Interest and Business Opportunities**

a) You must be alert to any situation that could compromise the position of trust you hold as a Pak EXIM employee, and avoid any kind of conflict between your personal interests and those of the Bank.

i. You must disclose all outside positions to the Human Resources representative, who will determine if a conflict exists. If a conflict does exist, you will not be permitted to continue in or accept that position.

ii. You should never use your position with the Bank, or information acquired during your employment, in a manner that may create a conflict (or even the perception of a conflict) between your personal interests and the interests of the Bank or its customers and clients. You also should be aware that actual or potential conflicts of interest may arise not just from dealings with external parties, such as customers or suppliers, but also from relationships or transactions with managers, direct reports or other employees (e.g., such as receiving loans that are not on generally available terms and conditions). If a conflict or potential conflict arises, you must report it immediately. You may report it to your manager/supervisor, who will review the matter with the Human Resources Division. You also may report a conflict or potential conflict directly to the HR Division. Any such discussion will be held in confidence to the extent possible and in a spirit of cooperation.

b) Gifts and Gratuities

You must not solicit, accept or give gifts that may influence business decisions.

i. You must not solicit or accept, directly or indirectly, any cash or monetary equivalents, objects of value or preferential treatment from any person or enterprise that has, or is seeking; business with the Bank where doing so may influence, or appear to influence, your business judgment. Indirect gifts can include gifts to your family members or a charity you support. Conversely, you also must not offer excessive gifts or entertainment to others whose business the Bank may be seeking.

ii. You may accept business-related meals, entertainment, token gifts or favors only when the value involved is not significant i.e., amount is not more than Rs. 5,000/- and clearly will not place you under any real or perceived obligation to the donor.

In general, you should pay for your own meal. In no event should you offer or accept business meals, or attend business functions, at establishments featuring sexually suggestive entertainment. Many customers and suppliers consider reasonable gifts and entertainment as a sensible and acceptable business practice without subjective intent to unduly influence the judgment of bank's employees in business matters. It is anticipated that this statement of policy, with its emphasis on how the situation might be reviewed at a later date by a disinterested third party, will enable you to discourage gifts and entertainment falling in the "grey area" without embarrassment to either you or to the customer or the supplier.

c) Exceptions to the general prohibition regarding acceptance of things of value in connection with bank business may include:

i. Acceptance of gifts, gratuities, amenities or favors based on obvious family or personal relationships (such as those between the parents, children or spouse of a Bank employee) where the circumstances make it clear that it is those relationships rather than the business of the Bank concerned which are the motivating factors;

ii. Acceptance of meals, refreshments, entertainment (including tickets to sporting events, arts, concerts, etc.), accommodations or travel arrangements (to be approved by relevant Group Head; President & CEO in case of Group Heads), all of reasonable value, in the course of a meeting or other occasion, the purpose of which is to hold bona fide business discussions or to foster better business relations, provided that the expense would be paid for by the Bank as a reasonable business expense if not paid for by another party;

iii. Acceptance of advertising or promotional material of reasonable value, such as pens, pencils, note pads, key chains, calendars, diaries and similar items;

iv. Acceptance of discounts or rebates on merchandise or services that do not exceed those available to other customers;

v. Acceptance of gifts of reasonable value that are related to commonly recognized events or occasions, such as a promotion, new job, wedding, retirement, holiday or birthday;

vi. Acceptance of civic, charitable, educational, or religious organization awards for recognition of service and accomplishment;

vii. Items on a case-by-case basis, not identified above, in which a Bank employee accepts something of value in connection with bank business, provided that such approval is made in writing (directly to the President & CEO) on the basis of a full written disclosure of all relevant facts and is consistent with Bank's policies.

viii. Any business-related personal benefit, which you or your family gives or receives, must be reported in writing within three working days to your immediate supervisor

or HR Division. An officer receiving such a report must promptly acknowledge receipt. The underlying principle is that the employee should not derive material gain from the Bank's business.

d) Family Members Providing Services to the Bank

You must disclose all instances in which you seek to hire or engage a family member or his or her firm to provide goods or services to the Bank.

(i) While there is no prohibition against the employment of close relatives or engagement of his or her firm to provide goods and services to the Bank, the integrity of the personnel process must be maintained.

(ii) Therefore, no one shall serve on a committee; make personal recommendations or decisions, not report to each other, nor in any situation can influence the other's performance, reward or promotion decisions.

(iii) He/She should meet the required eligibility criteria, no conflict of interest should likely to arise.

4. Books and Records Accuracy and Completeness

a) You must ensure that the accounting and financial records of the Bank meet the highest standards of accuracy and completeness.

i. Reporting accurate, complete and understandable information about the Bank's business, earnings and financial condition is an essential responsibility of each employee. It is also your responsibility to make open and full disclosure to, and cooperate fully with, the Bank's outside accountants in connection with any audit or review of the financial statements of the Bank. If you have reason to believe that any of the Bank's books and records is not being maintained in an accurate or complete manner, you are required to report this immediately to your manager, the Chief Financial Officer, the Chief Internal Auditor or Chief Compliance Officer. Similarly, the Bank relies on you to come forward if you feel that you are being pressured to prepare, alter, conceal or destroy documents in violation of Bank policy.

ii. In addition, you must report to any of the individuals mentioned above if you have any reason to believe that someone has made a misleading, incomplete or false statement to an accountant, auditor, attorney or government official in connection with any investigation, audit, examination or filing with any government agency or regulatory body.

b) Financial Statements and Accounts

i. You must report transactions accurately, completely and in appropriate detail if you are involved in supplying any kind of supporting documentation, determining account classification or approving transactions.

ii. You must record all transactions appropriately to facilitate full accountability for all assets and activities of the Bank and to supply the data needed in connection with the preparation of financial statements. If you are involved in the preparation of the Bank's financial statements, you must apply applicable accounting standards and rules, so that the statements fairly and completely reflect the operations and financial condition of the Bank.

c) Travel and Expense Accounts

You may request reimbursement only for actual and reasonable business-related expenses that are properly documented, approved and in accordance with the Bank's policy.

5. Protection and Proper Use of Bank Property

a) You are entrusted with protecting the Bank's property.

i. Acts of dishonesty against the Bank or its customers involving theft, destruction or misappropriation of money, property, office equipment, supplies or any other items of value are, of course, prohibited.

ii. Falsification, alteration or substitution of records for the purpose of concealing or aiding such acts is also prohibited. If you suspect someone has committed such an act or if you witness such an act, you should report it immediately to supervisor/manager.

iii. You are expected to exercise usage of internet and email with caution and your personal internet usage should not interfere with the job tasks. It is extremely important for you to be careful when downloading received information or data and never rely on data gathered from internet until appropriate confirmation of source. You must adhere to the policies concerning Computer, Email and Internet usage released by IT Division from time to time.

iv. must protect and properly use the Bank's computer equipment, including Internet access. You also must take precautions to properly secure your computer. You also should follow the Bank's procedures for disposing of personal computers, personal digital assistants, mobile phones or other Bank assets.

6. Outside Pressure

You must refrain from bringing in outside pressure or influence to attain personal gains within the organization; any such attempt will be subject to immediate Disciplinary Action.

a) Influencing Others

i. You may not use your position to coerce or pressure employees to make contributions or support candidates or political causes.
ii. In certain instances, the Bank may encourage employees to support or oppose legislative issues that affect the Bank's businesses. In no instance, however, may you use your position of authority to make another employee feel compelled or pressured to work for, or on behalf of, any legislation, candidate, political party or committee, to make contributions for any political purpose, or to cast his or her vote one way or the other.

7. Customer Privacy and Information Security

You are responsible for protecting the privacy, confidentiality and security of customer information entrusted to the Bank.

a) In each of our businesses, we are entrusted with important information about our customers – information vital to our ability to provide quality products and services. The Bank owes a strict duty of confidentiality to their customers. You will not disclose to any third-party particulars of the identity or financial, business or personal affairs of a customer, except pursuant to a statute or regulation, or a valid court order or unless:

i. The customer has given prior written consent
ii. Disclosure is compelled by a court or statutory authority of competent jurisdiction
iii. Disclosure is compelled by law, due to money laundering, or by regulatory requirements, or
iv. Disclosure is necessary to protect the Bank's interest, for example disclosure to the police in case of suspected fraud.

8. Intellectual Property

a) You must protect and, when appropriate, enforce the Bank's intellectual property rights.

i. The Bank's intellectual property is among its most valuable assets. Intellectual property refers to creations of the human mind that are protected by various national laws and international treaties, in a fashion similar to real property (i.e., land). Intellectual property includes copyrights, patents, trademarks, trade secrets, design rights, logos, know-how and other intangible industrial or commercial property.

b) Confidential Information and Trade Secrets

i. You must protect confidential information and trade secrets and prevent such information from being improperly disclosed to others inside or outside the Bank.

ii. During the course of your employment, you may learn confidential information about the Bank that is not known to the general public or to competitors. Information of this sort is considered a trade secret if it provides the Bank with a competitive or economic advantage over its competitors. Confidential information or trade secrets may not be disclosed outside the Bank or used for your own or someone else's benefit.

iii. These obligations apply both during, and after, your employment with the Bank. When you leave the Bank, you must return all copies of materials containing the Bank's confidential information or trade secrets in your possession.

iv. Some examples of confidential information or trade secrets include:
   - customer lists;
   - the terms, discount rates or fees offered to customers;
   - marketing or strategic plans; and
   - software, risk models, tools and other system developments.

v. Within the Bank, confidential information and trade secrets may be divulged only to other employees who need the information to carry out their duties. When discussing confidential information or trade secrets, you must not do so in places where you can be overheard, such as taxis, elevators, the Bank cafeteria or restaurants. In addition, you should not communicate or transmit confidential information or trade secrets by non-secure methods (e.g., cell phones, non-secure e-mail, hotel faxes, etc.).

c) Trademarks, Copyrights and Patents

i. You must protect the Bank's trademarks, copyrights and patents.

ii. Publications, documentation, training materials, computer codes, and other works of authorship you develop for the Bank are the types of material that can be protected by copyrights. You may also create, discover or develop software, methods, systems or other patentable inventions when performing your responsibilities or utilizing information or resources available to you in connection with your employment. To the extent permitted by law, as an employee or a contractor, you agree that all such works of authorship and inventions, whether or not patentable or protectable by copyright, trade secret or trademark, are assigned to the Bank whether they be improvements, derivatives, designs, technologies, written materials, programs or any other works.

d) Intellectual Property of Others

i. You must respect the intellectual property belonging to third parties in a manner consistent with that outlined for Pak EXIM.

ii. It is Bank policy to not knowingly infringe upon the intellectual property rights of others. When preparing advertising or promotional materials, using the name or printed materials of another company, or operating a software program on a Bank computer, you must be sure that the use of any third-party intellectual property is proper. In addition, you may not copy software or bring in software programs from home. Only software properly licensed by the Bank is permitted on Bank computers.

iii. You also may not copy third-party newsletters or periodicals for broad distribution unless the Bank has a license to do so.

iv. You should not disclose to the Bank, or be asked by the Bank to disclose, confidential information or trade secrets of others (e.g., your former employer). You are not permitted to possess or circulate improperly obtained confidential information or trade secrets belonging to a competitor. Similarly, during performing your responsibilities, you may rightfully obtain information concerning possible transactions with other companies or receive confidential information about other companies. Such information should be respected in a manner consistent with that outlined here and you must not use that information for your own or someone else's benefit (refer to the Insider Trading section that follows for guidance).

9. Non-Public Information and Insider Trading

a) It is against Bank policy and illegal for you to buy or sell securities of any publicly traded company at a time when you possess "material" nonpublic information about the company and may result in immediate Disciplinary Action.

i. In the course of your employment, you may become aware of information about companies that is not public. Using such information for your financial benefit not only is unethical, but also may be illegal. Buying or selling securities while you possess "material" nonpublic information is known as "insider trading". Passing such information on to someone who buys or sells securities — which is known as "tipping" — is also likely to be illegal, even if you personally never trade in the securities. You may not engage in insider trading or tipping.

ii. The prohibition applies to stock, options, debt securities or any other securities of the Bank or another company. Violations can subject individuals to significant fines and even imprisonment. Employees in certain business units may be subject to additional specific requirements and restrictions on their personal trading as a result of their job responsibilities.

b) Material Non-public Information

i. You may not trade in the securities of a company about which you possess nonpublic information that would influence your decision to buy, sell or hold those securities.

ii. Material nonpublic information is information about a company that is not known to the general public and that could influence a typical investor's decision to buy, sell or hold that company's securities.

iii. Because the determination of "material" is made on a case-by-case basis depending on particular facts and circumstances, if you have any doubt or concern, you must not trade while you possess such nonpublic information. Examples of nonpublic information might include:

- the operating or financial results of the company, or of any of its major business units (including estimates of any future earnings or losses);
- the company's negotiations or its entry into an agreement for an acquisition or sale of a substantial business or other significant transaction;
- development of a major new product or service;
- an increase or decrease in dividends;
- a stock split or other recapitalization;
- a redemption or purchase by the company of its securities; or
- major management changes.

iv. Remember that information that may not be material to the Bank may in fact be material to a smaller company with which we do business.

Information stops being nonpublic when it has been effectively disclosed to the public — for example, by a press release, a filing with the appropriate government regulators, or a webcast — and is followed by a reasonable waiting period for the information to be absorbed by the marketplace.

c) Disclosure of Non-public Information and Tipping

i. You may not disclose nonpublic information to anyone unless that person has a need to know the information in order to perform his or her duties and you believe the person will not misuse the information.

ii. If you reveal nonpublic information to anyone (even a family member), and that person then buys or sells securities — or passes that information on to someone else who buys or sells securities — you may be liable for tipping, even if you never personally trade on the information. Liability could arise if you were trying to help someone profit from the information or if you were trying to gain something personally, even if only to impress someone with your knowledge.

d) Supervision of Others

i. You must be satisfied that those you supervise understand the insider trading prohibition.
ii. If you have supervisory authority in connection with a matter that involves material nonpublic information, you must take measures to direct the other employees working on the matter to take appropriate precautions to prevent insider trading violations. For example, you should clearly instruct all members of a working group that they possess material nonpublic information that they may disclose only on a need-to-know basis, and that they are barred from buying or selling securities of the companies to which the information pertains.

10. Money Laundering and Terrorist Financing

a) You must actively guard against the use of the Bank's products and services for purposes of money laundering or for the financing of terrorism or other criminal activity.
b) Money laundering and terrorist financing have become the focus of considerable attention by governments, international organizations and law enforcement agencies throughout the world. Money laundering is the process by which the proceeds of criminal activity are moved through the financial system in order to hide all traces of their criminal origin. Terrorist financing, by contrast, focuses on the destination and use of funds that may come from legitimate or criminal sources, or a combination of the two.
c) The Bank fully supports the international drive against serious crime and is committed to assisting the authorities to identify money-laundering transactions and, where appropriate, to confiscate the proceeds of crime.
d) You must report to the Chief Compliance Officer of the Bank suspicious activities such as, suspected insider trading, fraud, misappropriation of funds and money laundering.
e) You must be vigilant and exercise good judgment when dealing with unusual customer transactions. You must alert your manager/supervisor to any situation that seems to you to be inappropriate or suspicious. You should not let the customer know that you find the transaction suspicious, although you should ask whatever questions are necessary to better understand the customer's identity, source of funds and reasons for the transaction.
f) The key principles include the following:
    (i) The identity of a customer beginning a business relationship or conducting a single transaction should be established from official or other reliable identifying documents. The Golden Rule is to Know Your Customer,
    (ii) Business units must keep record of customer identification for at least five years after the account is closed and of transactions for at least five years after their completion, or longer if the local law requires.

These documents should be available to the competent authorities in the context of relevant criminal investigations and prosecutions.

(iii) If business units suspect that funds stem from money laundering, they should promptly report those suspicions to the competent authorities and record the circumstances in writing.

(iv) Business units should not forewarn their customers when information relating to them is being reported to the competent authorities. (v) When a business unit reports its suspicions to the competent authorities, it should comply with their instructions.

(v) You must immediately contact the Chief Compliance Officer if you are approached in any manner by government agencies concerning a money laundering or terrorist financing investigation. There are strict regulations specifying time frames for complying with those inquiries, so your immediate action is vital.

11. Other Acts of Misconduct

a) It is not possible to list all the forms of behaviors that are considered as misconduct or unacceptable in the workplace. The following are examples of infractions of code of conduct that may result in disciplinary action, up to and including termination of employment: -

i. Theft, fraud, dishonesty with business or property of the Bank or any other organization/any person inside or outside the Bank or inappropriate removal or, unauthorized possession of property.
ii. Falsification of employment documents/data to obtain employment.
iii. Tampering the office records.
iv. Negligence or improper conduct leading to damage of Bank-owned or customer-owned property or damage to the reputation of the Bank.
v. Conviction for a criminal offence within or outside the office.
vi. Violation of safety or health rules.
vii. Smoking in prohibited areas.
viii. Spitting within Bank's premises.
ix. Unauthorized absence from duty.
x. Illegal strike or go-slow tactics.
xi. Misuse of Official Stamps /Letterheads /Telephones /Computers & other items.

b) The Bank, at its sole discretion, shall determine what act or omission constitutes misconduct, breach of trust or negligence of duty.

12. Compliance with Code

a) You must read, understand and comply with the Code. If you have any questions, you are responsible for asking your immediate manager/supervisor for clarification.

b) If you believe that you have violated the Code or any applicable law or regulation, you must report the violation so that the Bank can take appropriate action. The fact that you have reported the violation will be given consideration in determining appropriate disciplinary action, if any. In many cases, a prompt report of a violation can substantially reduces the adverse consequences of a violation for all involved — third parties, the Bank and you.

c) If you become aware that another employee, has, in all likelihood, violated the Code, including any law or regulation applicable to the Bank's businesses, you have a duty to report that violation in a responsible and effective manner so that the Bank can take steps to rectify the problem and prevent a recurrence.

d) You should report actual or suspected violations by surface mail or inter-office mail to the following address, marking the envelope CONFIDENTIAL. Such reports will be treated confidentially to the extent possible, and you will not be subject to retaliation for reporting a suspected violation in good faith.

Name:
Address:
Email:
Contact Number:

13. Disciplinary Action

a) If employee fails to comply with the Code or any applicable law or regulation, he/she will be subject to disciplinary action that may include;

- Withholding of increment and/or performance-based reward
- demotion
- reduction in salary
- temporary suspension without pay
- transfer
- compulsory retirement
- termination /option of resignation
- dismissal or termination notice

b) Disciplinary measures will depend on the circumstances of the violation and will be applied in a manner consistent with the Bank's policies.

Consideration will be given to whether a violation was intentional, as well as to the level of good faith shown by an employee in reporting the violation or in cooperating with any resulting investigation or plan of remediation.

c) Disciplinary action will be taken against any employee who:

(i) Authorizes, directs, approves or participates in violations of the Code of Conduct;

(ii) Deliberately fails to report, or conceals, violations of the Code, or deliberately withholds or mis-states relevant information concerning a violation of the Code;

(iii) Retaliates, directly or indirectly, against any other employee because of a report by that employee of a suspected Code violation;

(iv) Any employee who encourages others to do any of the above; and

(v) Any manager/supervisor who, under the circumstances, should have known about a violation by people under his or her supervision, or who did not act promptly to report and correct a violation.

14. Responsibilities After Leaving the Bank

a) Employees must not use their position to advance their prospects for future employment or allow their work to be influenced by plans for or offers of, external employment which would conflict or compromise in any way the best interests of the Bank.

b) Your professional duty while being employed by the Bank was to maintain confidentiality; therefore, you must maintain the same professionalism and secrecy after leaving the employment of the Bank and not disclose any official information. Former employees should not use or take advantage of personal, confidential or official information; they may have obtained in their capacity as the Bank employee.