MISCONDUCT PREVENTION POLICY

Definition of Misconduct

In general, “misconduct” is defined as infamous offenses like embezzlement, extortion, bribery, theft, forgery, abuse of authority and all acts contrary to our bank's ethical principles.

Misconduct can be committed by an individual, a group, or by one or several organizations that provided services to the Bank. Misconduct can occur upon having an employee of the Bank act as an accomplice to a perpetrator, and it can as well be committed by having the persons who are not members of the Bank target it.

Controls for Prevention of Misconducts

The methods listed below will be used to prevent misconducts before they occur, after they occur to discover them.

- External Audit of Financial Statements and Financial Reporting
- Internal Audit and Control of Financial Statements and Financial Reporting
- Top Management Approved Financial Reporting
- Authorization Limits
- Separation of Duties
- Ethical Principles Regulation
- Corporate Management
- Independent Audit Committee
- Line for Informing Misconduct
- Misconduct Training for Personnel and Managers
- Misconduct Prevention Policy
- Official Misconduct Prevention Assessments
- Setting up a Reasonable Control Environment in the Bank on IT and Business Processes
- Surprise Audits
- Overseeing
- Physical Investigation and Agreements
- Information Security Policies
- Personnel Policies
- Resume Reference Controls
- Rotation / Compulsory Leave
- Indebtedness status controls

Misconduct Incident Types

Misconducts are classified in two main categories as internal and external (with respect to the Bank), and by taking the transaction and incident types at below as basis.

When defining the potential misconduct incidents, the classification developed by the Basel Banking Audit Committee has been adopted for operation-risk loss incidents, with the purpose of ensuring the uniformity of the risk quantifications made with respect to statutory capital.

Risk-control assessments regarding misconducts are defined in a separate internal legislation document, and thus provide the assessment of fraud risks in new product development processes.

Unauthorized Transaction

- Transactions Deliberately not Reported
- Unauthorized Transactions that Cause Financial Loss
- Positions Deliberately Reported Incorrectly

Incidents of Internal Theft and Fraud

- Misconduct and Fraud / Credit Fraud
- Theft / Blackmail / Robbery
- Inappropriate Use of Assets
- Damaging of Assets
- Forgery
- Check Fraud
- Smuggling
- Transfer the Accounts to Somebody Else's Name / Use of Accounts by Way of Forgery
- Failure to Fulfil Tax and Other Similar Legal Obligations
- Bribery / Commission
- Insider Trading

Theft and Fraud by External Persons

- Theft / Robbery
- Forgery
- Check Fraud
- Blackmail

System Security

- Hacking Loss
- Information Theft

In any event, incidents of misconduct are not limited to those listed above and; in case of doubt as to whether an activity is indeed misconduct, the Ethical Line must be used for support and to take advice on the phone.

Responsibility for Reporting

According to the principles of this Policy, each employee is required to report any finding or suspicion he/she might have regarding any act of misconduct, to the Internal Audit Unit, which is entrusted with the duty of inquiring, examining, investigating the acts of misconduct and reporting them to the authorities in charge.

When a person, who would report such actions or incidents or his/her strong suspicion that they existed, he/she can not only refer in his/her preliminary assessments to the specific misconduct types stated in this Policy, the general definition which says "an act of misconduct is any action by one or several persons, intended to derive unfair or unlawful benefits deliberately or by using deceitful methods, for himself/herself or themselves, or to to damage the tangible assets or the reputation of the Bank or to obtain benefit for the Bank" can as well be taken as the point of reference.

As shall also be understood from this definition, as long as it is deceitful or improper, the act that is intended to obtain a tangible or reputational benefit to the Bank will still be considered misconduct.

Reporting Procedures

1. Acts of misconduct must, without resort to an intermediary, be reported directly to the Internal Audit or the Internal Control Units – primarily to the Internal Audit Unit.

2. Depending on the nature of the particular incident and at the option of the person who reports, such reporting can be oral or written. Written reports must be sent by e-mail or fax, and the oral reports must be submitted either face to face or by telephone.

When submitting a report orally or in writing, attention must be paid to the following aspects regarding the contents and the procedure:

a) The reporting person can give his/her name;
b) The subject matter of the report and/or the person about whom the report is submitted must clearly and plainly be stated;
c) In the report, the basic elements that describe the misconduct, namely the person/incident, time, place, and method must be stated as clear, concretely and fully as possible and;
d) Concrete evidence, witnesses and documents, if any, regarding the report must also be provided or stated.

Reporting Channels

By e-mail: etikhat@pashabank.com.tr

1. Misconduct findings or strong suspicion of it, encountered during routine audits and controls by the Internal Audit Unit's or the Internal Control Unit's personnel, will be reported not individually, but through the management of that Unit.

2. Any report about acts of misconduct by anybody who is not an employee, submitted through any of the various complaint and reporting channels of the Bank, must directly be communicated in writing to the Internal Audit Unit, by the unit that is responsible for operating that channel.

3. Any report by the Board of Directors or the Audit Committee of the Bank about a misconduct finding or suspicion is not subject to any requirements as to the form.

4. In the event of hesitation whether if the discovered incident should be considered a misconduct or a breach of ethical rules, the communication channels stated in this Policy must be used along with the communication channels stated in the Ethical Principles Policy.

5. If it is discovered that the misconduct report is intended to violate the personal rights or to damage the position of an employee, the Bank's disciplinary provisions will be applied the person that had submitted the false report.

Researching Responsibility

The duty of researching, examining and investigating the irregularities, frauds, and misconducts that had occurred in the Bank, and which call for punishment according to the Bank's Policies and Procedures, and reporting the results to the concerned authorities, will be carried out by the Internal Audit Unit.

With respect to this, the responsibility to investigate the following falls on the Internal Audit Unit:

a) Actions of the Bank personnel, in violation of instructions and the general ethical rules that call for disciplinary punishment, or which discredit the Bank in the eyes of third persons, information about which had been obtained from open sources or had been reported by the customers/personnel;

b) Dealings or transactions that are discovered during routine examinations, and which call for disciplinary punishment for violation of the Bank's rules and regulations, or for having being carried out deliberately, or which constitute crime prosecutable by legal authorities or;

c) Transactions that are discovered during routine investigations, the transactions that are likely to cause material loss or have the potential to cause material loss, if no immediate action is taken, are within the scope of the responsibility of the Internal Audit Unit.

Apart from this, within the scope of this Policy, the Internal Control Unit and the Internal Audit Unit provides consultancy services for the continuous improvement of the initial control points that had been set up by any business unit of the Bank, for the prevention of improper transactions and acts of misconduct.

Confidentiality

All parties to which any act of misconduct has been reported must definitely keep the details of such misconduct as well as the results of the examination and investigation about it, confidential. All inquiry, examination, investigation and reporting activities of the Internal Audit Unit regarding the acts of misconducts duly reported within the framework of this Policy, will be conducted under strict confidentiality.

During the examinations and inquiries, the phases of the inquiry, and the identities of the suspected parties involved in it, and of the informer, cannot – except when inevitable like in the event of cross-examination and hearing the witnesses – be disclosed to anybody except those who are authorized by law or according to the rules and regulations of the Bank.

This purpose of this confidentiality principle is to protect the informer and the suspected person, considering the possibility of failing to find any wrongdoing or perpetrator at the end of the inquiry.

Providing information about the misconduct to the Audit Committee and to the Board of Directors will not be deemed a breach of confidentiality.

The Bank understands and respects the confidentiality concerns of the personnel, who reveals the incidents explained in this Policy. When an employee reveals such an incident, the Bank will, if necessary, with the help and cooperation of also that employee, conduct an urgent and extensive investigation. Even if the informer discloses his/her identity, this information will be kept confidential and will not be shared with anybody except those who are by law authorized to obtain such information.

Should sufficient evidence pointing out to misconduct or a misconduct attempt be found, the Bank will report this to the authorities mentioned in the pertinent laws.

Saving the Information

In order not to allow stealing, changing or destruction of the relevant records, immediate action must be taken upon any report of suspected misconduct. For this reason, it must be ensured that the person who sends these records saves them in a secure way.

Reporting

Regardless of the amount, the Internal Audit Unit will report all acts of misconduct to the Senior Management and the Board of Directors.