Yapı ve Kredi Bankası A.Ş.

Policy on Protection of Inside Information and Prevention of Insider Trading

Contents

1 PURPOSE AND SCOPE

The purpose of the Policy on Protection of Inside Information and Prevention of Insider Trading ("Policy"), which is an integral part of the Yapı ve Kredi Bankası A.Ş. ("**Yapı Kredi**") Code of Ethics, is to set the principles and rules regarding the obligations of Yapı Kredi employees and executives, Business Partners, and all other stakeholders with access to inside information related to Yapı Kredi in relation to the use and protection of inside information.

The Policy has been prepared taking into account the relevant provisions of the Yapı Kredi Code of Ethics, as well as the regulations of the Capital Markets Board (CMB) of Turkey due to the issuance of capital market instruments locally and EU regulations due to capital market instruments trading abroad.

In case of failure to ensure the confidentiality of inside information, various sanctions may arise for all parties who have Inside Information related to Yapı Kredi and who use or disclose this information without complying with the relevant regulations, in addition to the potential reputational and commercial damages. This Policy has been prepared to explain the obligations of Yapı Kredi employees and executives, Business Partners, and all Yapı Kredi Group employees with access to inside information related to Yapı Kredi, in order to avoid such adverse consequences and includes information on closed periods, other transaction restrictions, and notification obligations.

All employees and executives of Yapı Kredi Group shall compy with this Policy. Yapı Kredi expects all its stakeholders, main shareholders, and Business Partners to act in accordance with the Policy to the extent applicable and takes the necessary steps to ensure this.

2 DEFINITONS

"EU regulations" refers to all directives, laws, decisions, and other regulations enforced by the European Union, including but not limited to the Market Abuse Regulation (596/2014) and Market Abuse Directive (2014/57/EU), regarding the public disclosure and confidentiality of information.

"Inside Information" is defined in the EU regulations and CMB regulations as information, events, and developments that have not yet been disclosed to the public and that may affect the value, price, or investment decisions of investors regarding capital market instruments. Detailed explanations can be found in section 3.1.

"Person discharging managerial responsibilities (PDMR)" refers to the members of the Yapı Kredi board of directors and individuals who, although not members of the board of directors, have direct or indirect regular access to the issuer's inside information and have the authority to make administrative decisions affecting the issuer's future development and commercial objectives. In addition, according to CMB regulations, the board members and other senior executives of the issuer's parent company, who have direct or indirect regular access to the issuer's inside information and have the authority to make administrative decisions affecting the issuer's future development and commercial objectives are considered within this scope. Positions classified as PDMR for Yapı Kredi are described in the Yapı Kredi Disclosure Policy[1].

[1] YKB_Disclosure_Policy.pdf

"Issuer" is defined in the Capital Markets Law as legal entities that issue capital market instruments, that apply to the Board for issuance or that have their capital market instruments offered to the public, and refers to Yapı ve Kredi Bankası A.Ş. in the context of this Policy.

"Persons closely associated with PDMR" refers to the following persons:

1) The spouse and children of the PDMR, and those residing in the same household as the PDMR during the transaction period,

2) Legal persons, institutions, or partnerships whose managerial responsibilities are assumed by the PDMR or persons mentioned in item (1), or are directly or indirectly controlled by these persons, or are established for the benefit of these persons, or whose economic interests are primarily identical to the economic interests of these persons,

3) PDMRs and persons[2] mentioned in items (1) and (2) of the Subsidiaries that constitute 10% or more of the total assets in the last year of the company with capital market instruments traded on a stock Exchange;

"Business Partners" include suppliers, distributors, dealers, authorized services, and other third parties with whom the company has a business relationship, and all kinds of representatives, subcontractors, consultants, etc. acting on behalf of the company, including but not limited to service providers such as auditors, rating agencies, consultants, as well as their employees and representatives.

"KAP" refers to the Public Disclosure Platform operated by the Central Securities Depository (MKK).

"List" refers to the "List of Persons with Access to Inside Information" kept by Yapı Kredi in accordance with CMB regulations.

"MKK" refers to the Central Securities Depository Inc.

"Disclosure" refers to the material events diclosure.

"Capital market instrument" refers to securities, derivative instruments, and investment contracts as defined in the Capital Markets Law, including but not limited to shares, bonds, and finance bills.

"CMB" refers to the Capital Markets Board.

"CMB regulations" refer to all laws, regulations, communiqués, guides, principle decisions, and other regulations put into effect by the CMB, primarily the Capital Markets Law No. 6362, the Material Event Disclosures Communiqué, the Market Abuse Communiqué, the Communiqué on Payment of Net Purchase and Sale Profits by Managers to Issuers, and the Material Event Disclosures Guide, regarding the public disclosure and ensuring the confidentiality of information.

"**Yapı Kredi Group"** refers the Yapı ve Kredi Bankası A.Ş. and Subsidiaries.

[2] The persons defined in this clause (3) are classified as "persons closely associated with the PDMR" only in terms of the CMB regulations, and the definition of a person closely associated with the PDMR in the EU Regulations does not include these persons.

3 GENERAL PRINCIPLES

3.1. What Should Be Considered as Inside Information?

Inside Information is broadly defined in local and international regulations as information, events, and developments that have not yet been disclosed to the public and may affect the value, price, or investors' investment decisions regarding capital market instruments. Since there is no restrictive definition, whether a situation is considered inside information should be evaluated on a case-by-case basis.

In principle, information, events, and developments that are:

- Related to a specific event,
- Considered significant by a rational investor when making an investment decision,
- Related to situations that have not been disclosed to the public,
- Providing an advantage to the person using the information compared to other investors who are unaware of this information,
- Capable of creating an impact on the value, price, or investors' investment decisions regarding the relevant capital market instrument if disclosed to the public,

are considered "Inside Information."

Below are some examples of events and developments that may be considered as Inside Information. However, it should not be forgotten that there may be other subjects that may also be considered Inside Information, and there may be cases where the following developments may not be considered as Inside Information. Detailed explanations, examples, and guidance on the subject can be found in the Procedure and the CMB's Material Event Disclosures Guide.

- Information regarding financial status and results,
- Information on dividend distribution,
- Information on business volume, production planning, pricing,
- Information on strategic transactions such as mergers, divisions, acquisitions, sales, investments,
- Information on significant disruptions in operations, such as closures or suspensions,
- Information on lawsuits, disputes, or audits.

In case of doubt about whether a piece of information is considered Inside Information, you should consult the Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management at BankacilikveSPKMevzuati@yapikredi.com.tr and ensure the confidentiality of the information until a response is received, treating it as Inside Information.

Yapı Kredi and Yapı Kredi Group Group employees and executives are also expected to comply with this Policy for the information they learn during their duties about companies other than Yapı Kredi, whether or not they are part of the Yapı Kredi Group, whose capital market instruments are traded on stock exchanges, , as this information may also be considered Inside Information for the relevant company.

3.2. Obligations Regarding the Confidentiality and Use of Inside Information

Yapı Kredi Group employees, executives, persons closely associated with them, or Business Partners who possess Inside Information must:

- Ensure the Confidentiality of Inside Information and Not Share it with Third Parties: The confidentiality of the information must be maintained until it is disclosed to the public and should not be shared with third parties in any way. The measures expected to be taken for this purpose are included in Section 4 below, titled *"Measures to be Taken and Document Security for Ensuring the Confidentiality of Inside Information."*

- Prohibition of Providing Comment/Advice Based on Inside Information: No advice or comments should be given for the purchase or sale of capital market instruments based on the Inside Information possessed.

- Prohibition of Trading Based on / Using Inside Information: Until the information is disclosed to the public, no transactions should be made in any way in Yapı Kredi shares traded on the stock exchange, capital market instruments based on shares, debt instruments traded in domestic or foreign markets, or other capital market instruments. This prohibition also covers derivative products such as options and futures transactions, as well as transaction types such as short-selling, leveraged transactions, pledges, and collateral. According to CMB regulations, the purchase and sale transactions of investment fund units that invest in capital market instruments and are managed by portfolio management companies and sold to a large number of investors are generally not considered within this scope. However, care should be taken not to use Inside Information when investing in special funds allocated to predetermined persons or institutions or similar capital market instruments.

If Inside Information is unintentionally shared with third parties or if it is learned that it has been shared, one shall contact the Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management immediately to take necessary measures and, if necessary, disclose it to the public, as the confidentiality of the Inside Information cannot be ensured.

For a piece of information to be considered publicly disclosed, it must be announced on the Public Disclosure Platform (KAP) in accordance with the regulations. In cases such as the communication of news in the press or social media or press releases, the obligations regarding Inside Information remain valid as long as no announcement is made on KAP.

Yapı Kredi Group employees and executives are also required to comply with the principles set forth in this Policy regarding the Inside Information they acquire during their duties, even if they leave their jobs. In this context, even in situations such as leaving the job, the confidentiality of previously acquired Inside Information must be maintained, Inside Information should not be shared with third parties, and transactions should not be made based on such information.

3.3. Persons Obliged to Ensure the Confidentiality of Information

According to the CMB regulations, the obligations to ensure the confidentiality of Inside Information and the prohibitions on using or trading based on such information are not only defined for the employees and executives of the Yapı Kredi but also include a much broader scope, covering the executives and shareholders of the Bank's subsidiaries and parent companies, as well as employees of all institutions that the bank has a business relationship with, such as customers, suppliers, auditors, rating agencies, etc.

Therefore, anyone who posesses Inside Information in any way or knows that the information they possess is of Inside Information nature must adhere to the principles set forth in this Policy.

As per the CMB regulations, the information of individuals who are working for Yapı Kredi under an employment contract, service relationship, or in any other way, and who have regular access to Inside Information, is monitored through the "List of Persons with Access to Inside Information" ("List"), and the general list is reported to the Central Securities Depository (MKK). Persons added to the List are informed about their obligations and the applicable sanctions. However, it should be kept in mind that the obligation to ensure the confidentiality of Inside Information is valid for all parties who access Inside Information, not just those on the List, and compliance with the relevant regulations should be carefully observed, regardless of whether they are included in the List or not.

3.4. Obligations Regarding Transactions of Employees and Persons Discharging Managerial Responsibilities (PDMRs)

3.4.1. Obligations Applicable to All Employees and PDMRs and the Trading Windows

3.4.1.1. Prohibition on Trading Based on / Using Inside Information

Primarily Yapı Kredi PDMRs and employees, as well as all Yapı Kredi Group employees who have access to undisclosed Inside Information that could significantly affect Yapı Kredi's operations or financial results, should not engage in any transactions involving Yapı Kredi's capital market instruments during the period until the Inside Information is publicly disclosed.

3.4.1.2. Closed Period

In accordance with the CMB regulations, during the closed periods, which is defined as the time between the last business day of the period to which the annual and semi-annual financial reports are related and the public disclosure of these reports (i.e., from July 1 and January 1 until the relevant financial reports are publicly disclosed), individuals with access to Inside Information, or their spouses, children, or persons living in the same household, should not engage in any transactions involving Yapı Kredi's publicly traded shares and capital market instruments based on these shares. Although the 3 and 9-month financial reporting periods are not included in the closed period definition according to the CMB regulations, if there is undisclosed information in these financial reports that could affect the share price or investor decisions, those with access to such information should not engage in transactions until the mentioned financial reports are publicly disclosed, as required by the general regulations.

Similar restrictions are also present in EU regulations. Accordingly, for debt instruments (eurobonds) issued by Yapı Kredi abroad, the 30-day period before the public disclosure of the 3, 6, 9, and 12-month financial reports is applied as the closed period, and Yapı Kredi PDMRs should not engage in any transactions involving these instruments during this period.

The closed period dates concerning the CMB regulations are announced to employees and executives by Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management before the start of the relevant period.

3.4.1.3. Trading Windows when the Transactions are Allowed

Apart from the closed periods and periods when someone is in possession of undisclosed Inside Information, there are no legal restrictions on trading in Yapı Kredi capital market instruments.

While the obligations regarding the use of Inside Information and transaction prohibitions in the regulations are valid until the relevant information is publicly disclosed, it is recommended that transactions by employees and PDMRs be carried out at least one business day after the public disclosure of the Inside Information or financial reports, in order to ensure that investors have sufficient time to analyze the disclosed information and conduct transactions under equal conditions.

3.4.2. Other Obligations Applicable to PDMRs

3.4.2.1. Obtaining Pre-Clearence Prior to the Transaction

CMB and EU regulations include detailed obligations regarding the purchase and sale transactions of shareholders and executives of publicly traded companies, and there is a risk of administrative fines, imprisonment or judicial fines, and loss of reputation in case of non-compliance with these obligations.

To prevent these risks, prior to any transaction that may be carried out on Yapı Kredi capital market instruments, Yapı Kredi PDMRs should obtain pre-clearence from the Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management at least two business days before a planned transaction on the compliance of the planned transaction with the regulations and the required disclosures if any, in order to assess whether a Disclosure obligation arises and to receive support for such Disclosure preparations if necessary.

The pre-clearence given is valid if the transaction is executed within the following two business days; if the transaction is planned for a later date, an opinion should be obtained again for the planned transaction in accordance with the specified periods.

3.4.2.2. Post-Transaction Disclosure Obligation

In accordance with the CMB regulations; all transactions carried out by Yapı Kredi PDMRs and closely associated persons with PDMRs, as well as Yapı Kredi's parent company, Yapı Kredi shares and other capital market instruments based on these shares, or publicly offered capital market instruments other than shares, should be immediately disclosed to the public through the PDP by the party executing the transaction.

Disclosure is not required unless the total amount of transactions reaches the threshold determined annually according to CMB regulations within the last twelve months. When calculating the total amount of transactions, all transactions carried out by each PDMR and closely associated persons shall be taken into account. The threshold applicable for each period will be specified in the announcements made by Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management to employees and executives.

Similar to CMB regulations, EU regulations also have a disclosure obligation for transactions exceeding a certain amount in debt instruments (Eurobonds) issued by Yapı Kredi abroad, carried out by Yapı Kredi PDMRs and closely associated persons with PDMRs.

3.4.2.3. Obligation to Return Short-Term Net TRading Profits (Short Swing)

In accordance with the CMB regulations, if a profit is made from the purchase and sale transactions of Bank shares by Yapı Kredi PDMRs during any six-month period, the net profit must be paid to the Bank within 30 days.

The regulation aims to eliminate the opportunity inequality between those who have earlier and easier access to Inside Information due to their positions and investors who can access this information only after it is announced to public, by requiring Yapı Kredi executives to pay the net profit obtained through short-term transactions to Yapı Kredi.

There are a limited number of exceptions defined in the relevant regulation regarding the obligation to return, and detailed information about the exceptions can be found in the circular.

3.4.3. Obligations Applicable to Major Shareholders

In the CMB regulations, additional obligations are defined for shareholders who directly or indirectly hold more than 5% of the shares of public companies.

Firstly, obligations similar to the disclosure obligation introduced for PDMRs in section 3.4.2.2 are also defined for major shareholders.

In order to ensure compliance with the relevant regulations, it is recommended that shareholders holding more than 5% of Yapı Kredi's capital also ask for pre-clearence as stated in section 3.4.2.1 above, for the purpose of evaluating whether a Disclosure obligation will arise and, if necessary, obtaining support for Disclosure preparations before the transactions are carried out.

In addition, if a natural or legal person, or other natural or legal persons acting in concert with this person, directly or indirectly reach or fall below 5%, 10%, 15%, 20%, 25%, 33%, 50%, 67%, or 95% of Yapı Kredi's capital or total voting rights, a Disclosure should be made by these persons. If the person's direct shareholding reaches or falls below these ratios, the disclosure to be made by these persons is made by the Central Securities Depository (MKK). However, if these ratios are reached or fallen below due to acting in concert, indirectly, or through voting rights, the disclosure obligation belongs to the relevant natural or legal person or other natural or legal persons acting in concert with this person.

4 MEASURES TO BE TAKEN FOR ENSURING THE CONFIDENTIALITY OF INSIDE INFORMATION AND DOCUMENT SECURITY

4.1. Main Measures

The main measures to be taken by all parties in possession of Inside Information to ensure its confidentiality are listed below.

- **Sharing the information only with those who need to know for business reasons (need-to-know basis):** Inside Information can only be shared with those who need this

information due to their job/duty. Even in this case, it should be carefully assessed whether the person concerned needs this information to perform their duty, and only such necessary amount of information should be shared. In order to avoid any leakage risk, it is deemed necessary that the information is not shared with anyone within or outside the Bank who does not need it for business purposes.

- **Signing a Confidentiality Agreement:** In cases where it is necessary to share Inside Information with any person/institution outside Yapı Kredi, before sharing the information, the Banking and CMB Legislation Department's assesment should be obtained regarding the appropriateness of sharing the data and the process for obtaining the approval of the Information Sharing Committee should be carried out in accordance with the legal regulations, a confidentiality agreement prepared by Yapı Kredi Legal Management should be signed with the person/institution with whom the information will be shared; the confidentiality agreement should state that the company and/or its shareholders are public companies subject to CMB regulations, references should be made to the relevant obligations and regulations they are subject to and the parties concerned should be reminded that they are responsible for complying with these obligations.

- **Adding warnings to emails:** In line with the Bank's Data Protection Policy and Information Asset Classification Guide, a data classification solution is used on all client computers. This ensures confidentiality classification for all documents and emails. All emails and documents shared within the institution or with external parties are subject to this confidentiality classification. When classifying information, the nature of the data (such as Sensitive Data, Special Categories of Personal Data, Customer Confidential Information and Personal Data, or Bank Confidential Information) is taken into consideration. To demonstrate that necessary measures have been taken to ensure the confidentiality of information, and to remind all parties accessing the information—especially those outside the Yapı Kredi—of their obligations and to prevent actions that could have negative consequences for themselves and the Yapı Kredi, warning notices must be included in messages when sharing Insider Information or information/events that may potentially evolve into Insider Information via email. Furthermore, particular attention should be paid to sending such email messages to third parties with the "Sensitive Data" label.

- **Communication in shared living and office spaces, clean desk and clean screen principle:** Care should be taken not to discuss Inside Information in public areas inside or outside the Bank (taxis, airplanes, airports, elevators, restaurants, etc.). Attention should also be paid to this issue in the use of shared offices. Unless necessary, printed copies containing Inside Information should not be taken, excessive photocopies or printouts and meeting notes should be destroyed in a way that ensures the confidentiality of the information after use (such as shredding instead of throwing directly/torn), and documents containing confidential information should not be left on desks or open areas. On the other hand, screen security should be preserved, especially during work in common areas, and necessary measures should be taken to prevent third parties from accessing information by seeing printed documents or screens.

4.2. Additional Measures to be Taken in Project Studies

Information and developments related to the listed companies' strategic projects (e.g., significant asset or company acquisitions and disposals, mergers and demergers, strategic partnerships, significant investments, changes in operations, etc.), or the existence of an intention in this direction (even if not yet regarded as an Inside Information) or the evaluations thereof may be considered as material information that investors may attribute importance to. Therefore, in project studies, it is important to take the following measures to ensure the confidentiality of information.

- Use of Project Code: The use of a project-specific code, which third parties cannot infer from, is important for ensuring confidentiality in communications related to the project

- Use of Project Group Addresses: To prevent risks of address slippage and sharing information with the wrong people, particularly in automatically filled addresses, a project group address should be created and correspondence should be made through these addresses

- Reminder of Trading Prohibitions and Confidentiality Obligations at the Project Kickoff Meeting and also via Email : It is important to inform all project team members via email at the beginning of the project to prevent information leakage in strategic projects and to inform those involved in the project about the prohibition of trading in capital market instruments due to access to project information. In addition, especially in projects with a large-scale working group, providing verbal information on the subject at the beginning of the project meetings is considered meaningful in terms of raising awareness.

4.3. Information Technology-Based Measures and Document Security

Considering that the majority of information is transferred and stored through electronic channels today, the importance of information technology-based measures to be taken for ensuring confidentiality is also increasing. In this context, Yapı Kredi Information Security Main and Sub Policies, which has been prepared to define the necessary requirements for ensuring the confidentiality, integrity, and accessibility of the systems, information, and assets operated by Yapı Kredi, has been put into effect with the approval of the board of directors, and the implementation principles have been determined by the Yapı Kredi IT Procedures included in the IT processes. In preparing these documents, national and international best practices, as well as the BRSA's Regulation on Bank Information Systems and Electronic Banking Services and relevant regulation, have been taken into account.

The basic principles determined in the IT Procedures prepared based on the Yapı Kredi Information Security Policies and related documents are as follows. These principles should be taken into account in terms of ensuring and protecting the confidentiality of all types of information, including, but not limited to, Inside Information:

1. Roles and Responsibilities: All employees, managers, and Business Partners are required to act in accordance with the relevant documents for ensuring information security and to pay attention to cybersecurity measures for protecting the confidentiality of information.

2. Access Control: Access to information should be provided only to authorized persons and to the extent necessary for them to perform their duties. Access control lists and authorizations should be regularly reviewed and updated. The storage of documents containing information

in shared areas accessible only to those who may need the information for business purposes, the evaluation of measures that can be taken in terms of confidentiality in these areas from the perspective of information 11ccess1111s11es, and the evaluation of 11ccess rights and measures taken for 11ccess security to be provided to third parties should be considered to the extent applicable to the security of shared areas within the bank.

3. Encryption: Data in transit should be encrypted with appropriate encryption techniques The data in rest should also be encrypted, and encryption techniques should be used during data sharing.

4. Network Security: The organization's network and systems must be protected using firewalls and other security technologies. Policies and procedures controlling network access should be implemented.

5. Software Updates and Patches: Operating systems, applications, and other software components should be regularly updated and security patches applied.

6. Antivirus and Anti-Malware Software: All computers and devices should use up-to-date and effective antivirus and anti-malware software.

7. Training and Awareness: Individuals with access to information should participate in regular training and awareness programs on cybersecurity topics to protect the confidentiality of information.

8. Incident Management and Breach Notice : Procedures and plans should be established for the management and notification of cybersecurity incidents that may affect the confidentiality of information.

9. Data Classification: All bank data must be classified based on risk category and protected using the appropriate security measures consistent with the minimum standards for the classification category

10. Audit and Monitoring: Regular audits and monitoring should be carried out to assess the effectiveness of the practices and policies implemented to protect the confidentiality of information. Based on the audit results, policies and practices should be updated and improved. Data Loss Prevention (DLP) systems should be deployed to prevent the transfer of information outside the organization or to enable necessary investigations when information is shared.

11. Backup and Recovery Plans: Backup and recovery plans should be established and implemented. Backups should be taken regularly and tested.

12. Third-Party Service Providers: The cybersecurity practices and policies of third-party service providers that provide services that may affect the confidentiality of information should be evaluated, and it should be ensured that appropriate security measures are taken.

13. Physical Security: The physical security of hardware and devices that can provide access to information must be ensured. This should include appropriate locking mechanisms, security cameras, card access systems, and other physical security measures

14. Mobile Device and Remote Access Security: Security policies and practices should be established and implemented for mobile devices and remote access systems that provide access to information.

15. Destruction of Information: Policies and procedures should be implemented to ensure the secure destruction of information when necessary. This should include the secure deletion of data in electronic environments and the destruction of physical documents by shredding or burning.

16. Internal and External Audits: Regular internal and external audits should be carried out to assess the effectiveness of information confidentiality policies and practices. Based on the audit results, policies and practices should be updated and improved.

17. Risk Assessment and Management: A continuous process should be implemented to identify, assess, and manage risks that may affect the confidentiality of information. This process should include determining appropriate strategies and measures to reduce and maintain risks at an acceptable level.

18. Communication and Information Sharing: The confidentiality policies and practices of information should be communicated and understood by all employees, contracted personnel, Business Partners, and relevant parties. This should include regular training and awareness programs, sharing updates on policies and practices, and using open communication channels

5 SANCTIONS AND PENALTIES IMPOSED BY CMB IN CASE OF VIOLATION OF REGULATIONS

5.1. Sanctions for Non-compliance with the Disclosure Obligation

In case of non-compliance with the obligations set forth in CMB regulations regarding Material Event Disclosures, the bank and/or the responsible executives may be subject to administrative fines. Administrative fines are determined annually by the CMB, and current amounts are announced by Banking and CMB Legislation Department.

If a benefit is obtained as a result of non-compliance, the fine amount cannot be less than double the benefit.

If the actions requiring the imposition of administrative fines are repeated, the imposed fine is doubled, and if a benefit is obtained, the fine amount cannot be less than three times the benefit.

5.2. Market Abuse Actions and Related Sanctions

According to CMB regulations, actions that cannot be explained by any reasonable economic or financial reasons, and disrupt the trust, transparency, and stability of the stock exchange and other organized markets are defined as “market abuse actions” provided that they do not constitute a crime.

In cases where transactions are made on the stock exchange by persons who have directly or indirectly obtained Inside Information prior to public disclosure of such information in accordance with the regulations;

a) persons with Inside Information or continuous information providing this information to others, or
b) persons who directly or indirectly obtain Inside Information or continuous information from persons with such information and trade in the relevant capital market instruments,

are considered as market abuse actions.

Furthermore, as stated in section 3.4.1, trading in shares traded on the stock exchange and derivative products based on these shares during the closed period by persons with Inside Information or continuous information, or their spouses, children, or persons living in the same household, is also considered as a market abuse action.

During the period between the finalization of Inside Information or continuous information and its disclosure to the public in accordance with the regulations, transactions in shares traded on the stock exchange and derivative products based on these shares by persons with Inside Information or continuous information, or their spouses, children, or persons living in the same household, are considered as market abuse actions.

On the other hand, providing false, misleading, or deceptive information, spreading rumors, giving news, making material event disclosures, commenting, or preparing reports related to stock prices, values, or indicators that may affect investors' decisions, and giving any order and/or carrying out transactions in the relevant capital market instruments before or after performing these actions by those who performed them, are considered as market abuse actions.

Lastly, failure to disclose information that may affect the prices, values, or investors' decisions of capital market instruments, which are required to be disclosed within the scope of CMB regulations, is also considered as a market abuse action.

Persons who commit market abuse actions will be subject to administrative fines imposed by the CMB. Administrative fines are determined annually by the CMB, and current amounts are announced by Banking and CMB Legislation Department. If a benefit is obtained through market abuse, the fine amount cannot be less than double the benefit.

5.3. Capital Market Crimes and Related Sanctions

Capital market crimes are defined in the Capital Market Law, and those related to the confidentiality of Inside Information are “Insider Trading” and “Manipulation” crimes.

Using Inside Information to benefit oneself due to asymmetric information distribution caused by non-disclosure of Inside Information is considered as “Insider Trading”. The two main elements of this crime are: (i) trading based on information and (ii) obtaining a benefit as a result. The sanction for this crime is determined as imprisonment from 3 to 5 years or a judicial fine of no less than double the benefit obtained.

Trading with the purpose of creating a false or misleading impression regarding the prices, price changes, supply, and demand of capital market instruments (transaction manipulation) or providing false, misleading, or deceptive information in order to affect the prices, values, or investors' decisions of capital market instruments and obtaining a benefit through this (information manipulation) are considered as “Manipulation” crimes, for which imprisonment from 3 to 5 years and judicial fines are applied.

Similar crime definitions and sanctions are also included in EU Regulations, and monetary fines or more severe sanctions may arise according to the regulations of the countries where capital market instruments are traded.

6 AUTHORITY AND RESPONSIBILITIES

All employees and executives of Yapı Kredi Group are obliged to comply with this Policy. Yapı Kredi expects and takes necessary steps for all Business Partners and main shareholders to act in compliance with this Policy, to the extent applicable to the relevant party and transaction.

In case of any discrepancy between this Policy and local legislation applicable in the countries where Yapı Kredi Group operates, the more restrictive of the Policy or the relevant legislation will apply, to the extent that the application does not violate local legislation.

If you become aware of any action that you believe is contrary to this Policy, current legislation, or Yapı Kredi Ethical Principles, you may consult or report the matter to your immediate supervisor. Alternatively, you can report to Yapı Kredi Ethics Communication Channels via phone and e-mail address.

Yapı Kredi Group employees can consult the Banking and CMB Legislation Department for questions about this Policy and its implementation. Violation of this Policy by an employee may result in significant disciplinary penalties, including dismissal, in addition to the regulatory authority sanctions mentioned in section 5. In case any third party, who is expected to act in compliance with this Policy, violates this Policy, the relevant contracts may be terminated.

7 EFFECTIVE DATE AND REVISION HISTORY

This Policy takes effect on 23.07.2025 upon approval of the Yapı Kredi Board of Directors. Banking and CMB Legislation Department under the responsibility of the Assistant General Manager in charge of Compliance, Internal Control and Risk Management is responsible for the implementation of this Policy. Material changes to the Policy must be approved by the Yapı Kredi Board of Directors.

Revision	Date	Description
-	23.07.2025	Policy Approval