POLICY ON THE PREVENTION OF ABUSE OF INSIDER INFORMATION

1. Introduction

The purpose of this Policy is to establish the framework for appropriate behaviour by all employees of the Central Bank of Malta (the Bank) in respect of matters concerning insider information and to protect both individual members of the staff and the Bank as a whole.

This Policy is based on the provisions of the Prevention of Financial Markets Abuse Act (Cap. 476) and Guideline (EU) No 2015/855 of the European Central Bank of 12 March 2015 laying down the principles of a Eurosystem Ethics Framework.

It should be noted that the Insider Information Policy does not replace due observance of Article 6 of the Prevention of Financial Markets Abuse Act (included as Appendix I of this Policy) and relevant legislation and directives as applicable and as amended from time to time. Members of staff should be aware that this Policy is not meant to provide any immunity from prosecution under the Act and adherence to this Policy should not be construed as exonerating a member of staff from any possible criminal proceedings under the Act. The Insider Information Policy should also be read in conjunction with the Anti-Fraud Policy. All members of staff are obliged to be familiar with the contents of this Policy and the provisions of the Prevention of Financial Markets Abuse Act.

This Policy applies to members of staff who, for the purposes of this Policy, include:

(i) All permanent and temporary employees;
(ii) Members of governing and decision-making bodies of the Bank; and
(iii) Other persons engaged by the Bank.

2. Definitions

For the purpose of this Policy:

"Eurosystem tasks" means the tasks entrusted to the Eurosystem according to the Treaty and the Statute of the European System of Central Banks and of the European Central Bank.

"Financial corporations" has the same meaning as defined in paragraph 55 of Chapter 2 of Regulation (EU) No 549/2013 of the European Parliament and Council on the European system of national and regional accounts in the European Union.

"Insider" means any member of a body or staff member who has access to insider information.

"Insider information" means any information of a precise nature which is either price or time sensitive relating to all activities carried out on behalf of the Central Bank of Malta and/or the Eurosystem, whether directly or indirectly, and which has not been made public or is not accessible to the public, including also information of a secret nature. For the avoidance of doubt it is clarified that expert market knowledge which is acquired in the course of business does not constitute insider information.

"Major incident" means any operational risk event that has occurred and has led to unexpected or unintended harm, business disruption, reputational impact and/or financial loss which has an impact level of 3 or above of the Bank's operational risk management framework.

"Market sensitive information" means information of a precise nature the publication of which is likely to have a significant effect on the prices of assets or prices in the financial markets.

"Members of governing and decision-making bodies of the Bank" means the members of the governing and decision-making bodies of the Bank which shall include the Board of Directors and the Policy Advisory Committee.

"Other persons engaged by the Bank" means any external consultant having a contract of service with the Bank or who provides any form of service to the Bank[1].

"Permanent employee" means an employee who is engaged with the Bank on a contract of employment of indefinite duration.

"Senior management" means employees who occupy the position of Chief Officer at the Bank.

"Temporary employee" means an employee who is engaged with the Bank on a contract of employment where the end of the contract is determined by reaching a specific date and which also includes workers who are still in full-time study and work at the Bank during the summer months.

[1] All contracts of service should include a reference to this Policy and the termination of the contract in case of any infringements to this Policy, without prejudice to any other measures that the Bank may take.

"Termination of employment" means the termination of employment proposed either by the Bank or the employee or the expiry of a contract of service or retirement of the employee or the dismissal of the employee by the Bank according to the provisions of the Collective Agreement.

"Third Party Auditor" means an independent external auditor appointed by the Bank to perform duties of compliance monitoring in terms of this Policy and who is not the statutory auditor of the Bank during the period.

3. General Principle

All members of staff are required to exercise caution in the management of their finances and not to undertake transactions that by their nature or purpose might affect the reputation of the Bank.

The Bank will ensure that access to insider information is restricted to those permanent and temporary employees, members of governing and decision-making bodies of the Bank and other persons engaged by the Bank who need access to this information for the performance of their duties.

Members of staff shall ensure that when conducting transactions (whether for personal investment and otherwise) on their own account or for the account of others, or when discussing such transactions with third parties or when recommending or inducing other persons to enter into private financial transactions, they do not in any way make use of or disclose insider information. The prohibition on misusing insider information shall also cover the disclosure of insider information to any other person unless such disclosure is made in the course of carrying out professional duties on a need-to-know basis. This obligation, which is also in line with the Declaration of Allegiance and Secrecy signed by staff on appointment with the Central Bank of Malta, shall continue to apply until the information retains its market sensitivity. Without prejudice to the provisions of the Prevention of Financial Markets Abuse Act, staff shall continue to be bound by this obligation for a period of one year following the termination of their employment.

4. Roles and Responsibilities

The Board of Directors

The Board of Directors attaches the utmost importance to a corporate governance approach that places accountability, transparency and the highest ethics standards at the centre of its strategy. Adherence to these principles is a key element of the Bank's integrity, credibility and reputation. As a result, the Board seeks to ensure that appropriate and effective internal control systems of compliance monitoring are in place to safeguard the Bank's reputation and ethics culture.

The Board is supported in its role by a Compliance Committee which shall conduct the compliance monitoring referred to in this Policy and this set up shall provide assurances to the Board of Directors on the standard of ethics within the Bank and that appropriate and effective internal control systems of compliance monitoring are operating.

The Compliance Committee

The day to day responsibility for the operation of the rules established by this Policy and more specifically the tasks relating to the compliance monitoring shall rest primarily with the Compliance Committee.

The Compliance Committee shall be composed of three persons, which shall include the Head of Internal Audit (as observer), the Compliance Officer, and a non-executive Director. In cases where one of the members of the Compliance Committee is involved in the transaction, a Governor will take his /her place on the Compliance Committee.

The Compliance Committee shall be responsible:

- To assess any request received from members of staff relating to a specific restriction as established by the Policy;
- To decide on any request received from members of staff relating to a specific restriction as established by the Policy on the basis of a proposal for a draft decision made by the Compliance Officer;
- To develop guidelines and best practices that can help members of staff to determine whether a particular situation can lead to an abuse of insider information;
- To adopt any best practices established by the Governing Council related to this policy, if necessary;

- To pay special attention to particular circumstances which may indicate an irregularity;
- To ensure that members of staff are continuously and fully aware of and adhere to the provisions of this policy;
- To conduct preliminary investigations on suspicious transactions made by members of staff and/or breaches to this Policy;
- To conduct the compliance monitoring through the Third Party Auditor as specified in the Policy by conducting regular and ad hoc checks and the necessary investigations;
- To request members of staff to provide copies of the documentation referred to in paragraph 7 of the Policy to the Third Party Auditor;
- To report to the Audit Committee of the Bank in accordance with the compliance monitoring procedure outlined in this Policy;
- To steer and contribute to the periodic review and updating of the Policy;
- To perform any other task as mentioned in the Policy.

Third Party Auditor

A Third Party Auditor shall be appointed by the Bank to assist the Compliance Committee in the performance of tasks related to compliance monitoring as directed by the Compliance Committee and as specified in this Policy.

The Third Party Auditor shall be responsible:

- To conduct the compliance monitoring as specified in the Policy by conducting regular and ad hoc checks and the necessary investigations as directed by the Compliance Committee;
- To receive and examine the necessary documentation required to conduct the function of compliance monitoring;
- To prepare a report to the Compliance Committee and the Governor on their findings relating to the compliance monitoring conducted, making any recommendations as necessary.

Senior Management

The Bank's senior management is responsible for the successful implementation of specific restrictions referred to in the Policy and the compliance monitoring designed to prevent abuse of insider information within his/her area of responsibility and to monitor that the controls established are working effectively.

The Compliance Officer

The Bank's Compliance Officer shall have the responsibility to provide advice in writing to members of staff upon a written request, who are in doubt whether any transactions to be carried out by them on their own account or for the account of others, or to be carried out by others on their recommendation or inducement, fall within the specific restrictions established by this Policy, prior to effecting any such transactions.

For the purposes of giving advice to staff as aforesaid in the above paragraph, in the absence of the Compliance Officer, Head of Internal Audit Department will assume this responsibility.

The Compliance Officer shall conduct all preparatory work for the performance of the tasks by the Compliance Committee and other tasks included in the Policy as may be required. He/she shall prepare draft decisions to be taken by the Compliance Committee.

The Compliance Officer shall provide periodic training to members of staff on the Policy.

Members of Staff

All members of staff are expected to demonstrate the highest standards of honesty and integrity at all times. Members of staff shall comply with all the rules established by the Policy and shall employ utmost caution and care when making private financial transactions for their own account or for the account of a third party to safeguard the reputation and credibility of the Bank as well as public confidence in the integrity and impartiality of its staff.

Members of staff shall seek the advice of the Compliance Officer, and in his absence Head of Internal Audit Department, when they are in doubt as to whether any transactions to be carried out by them on their own account or for the account of others, or to be carried out by others on their recommendation or inducement, fall within the specific restrictions established by this Policy, prior to effecting any such transactions.

Members of staff shall cooperate fully and assist the Compliance Committee in the performance of its tasks and shall ensure full compliance with the obligations under this Policy.

Members of staff at all levels are required to be familiar with this Policy in order to be able to contribute towards the Bank's implementation of this Policy.

5. Transactions covered by this Policy

Members of staff shall refrain from carrying out transactions in any financial instrument/s at a time when they have non-public, market-sensitive information acquired in the course of their professional duties in relation to those transactions.

Examples of information which is generally considered as being non-public market sensitive information include, but are not limited to, information relating to monetary policy issues, open market operations, financial stability analysis and reports, and unpublished statistics.

These obligations are valid as long as the information retains its market sensitivity, even in the case of members of staff who have ceased to belong to the category of staff deemed to have access to insider information.

All insiders shall be subject to specific restrictions as outlined in paragraph 6 below, with regard to critical private financial transactions. A private financial transaction shall be deemed critical when it is or may be perceived to be closely related to the performance of the Bank's and Eurosystem tasks. The list of such critical transactions shall include in particular:

a) Transactions in shares and bonds issued by financial corporations established in the Union;
b) Foreign exchange transactions, transactions in gold, the trading of euro area government securities;
c) Short-term trading, i.e. the purchase and subsequent sale or sale and subsequent purchase of the same financial instrument within a period of three working days;
d) Transactions in derivatives related to the financial instruments listed under (a) to (c) and collective investment schemes the main purpose of which is to invest in such financial instruments.

The list of critical transactions above may be adjusted by the Bank's Board of Directors at short notice to reflect the decisions of the Governing Council.

6. Specific Restrictions

Prohibited Transactions:

Members of staff shall not make any financial transactions outlined in 5(c) above, unless the subsequent sale is made in execution of a stop-loss order which the member of staff has given to their broker.

Transactions subject to prior authorisation:

Members of staff who by virtue of their duties, have access to insider information relating to data on an individual level of financial corporations established in the Union, including balance sheets and profit & loss or returns or any other information of financial corporations established in the Union which can be considered as market sensitive shall request the prior authorisation of the Compliance Committee before making the financial transactions outlined in 5(a) and 5(d), the latter in relation to transactions conducted under 5(a) above.

Members of staff who, by virtue of their duties, have access to insider information relating to exchange rate issues, transactions in gold and trading in euro area government securities which can be considered as market sensitive shall request the prior authorisation of the Compliance Committee before making the financial transactions outlined in 5(b) and 5(d), the latter in relation to transactions conducted under 5(b) above. This restriction shall not apply in cases of purchase or sale of foreign exchange of up to the equivalent of amount €5,000 in a period of thirty calendar days.

Transactions subject to an Embargo Period:

Members of staff involved in the market making function (including both trading and research) of the Bank shall be precluded from conducting any transactions in Malta Government Securities from the date a new issuance is published in the Government Gazette and / or local media up to the date when the fixed price is officially announced.

Members of staff who, by virtue of their duties, have access to insider information on ESCB/Eurosystem macroeconomic forecasts on the euro area shall refrain from making any transaction during the period in which that information is embargoed by the ECB.

Members of staff who, by virtue of their duties, have access to insider information about the monetary policies of the ECB shall refrain from making any transactions from the period of

seven days preceding the meeting of the Governing Council of the ECB discussing monetary policy issues until after the meeting of the Governing Council of the ECB.

Transactions not requiring reporting

Members of staff may at all times freely enter into investment transactions in collective investment schemes in respect of which they have no influence on the investment policy without the need to observe any reporting obligations under this policy.

7. Record Keeping

Members of staff shall keep records for the preceding six months of the following:

a) transactions related to their bank accounts, including shared accounts, custody accounts and accounts with stockbrokers, subject however to the member of staff obtaining the authorisation of the joint holder of shared accounts to divulge information thereon. If such consent is not forthcoming, the member of staff shall make a signed declaration listing the transactions related to the shared or joint bank account which pertain to him or her;
b) any powers of attorney which third parties have conferred on them in connection with their bank accounts, including custody accounts;
c) any general or specific instructions or guidelines given to third parties to whom responsibility for managing their investment portfolio has been delegated;
d) any sale or purchase of financial assets or rights at their own risk and for their own account, or conducted by them at the risk and for the account of others;
e) statements for the abovementioned accounts;
f) their dealings in relation to retirement plans.

8. Compliance Monitoring

In order to monitor compliance with the rules established by this Policy, the Compliance Committee shall, on a regular and also ad hoc basis, request a selected number of members of staff to provide a written declaration (through the completion of the form in Appendix III) of the transaction/s carried out in the preceding six months. The completed form shall be sent by the staff member/s directly to the Third Party Auditor within a period of ten working days.

The Third Party Auditor shall report to the Compliance Committee on these submissions and can request further information. Upon such communication, the Compliance Committee shall either inform the staff member/s that no further information is required or request the staff member/s to provide information which includes the submission of copies of the documentation referred to in paragraph 7 for the preceding six months, as specified in the request, directly to the Third Party Auditor. Members of staff shall furnish the documentation requested to the Third Party Auditor within a period of ten working days. The submission of electronic copies or photocopies of requested documentation shall be sufficient. The Third Party Auditor shall report the outcome of any monitoring strictly in accordance with this policy to the Compliance Committee and to the Governor. This documentation shall be returned to the member of staff upon completion of the compliance monitoring.

The Third Party Auditor shall conclude the compliance monitoring within a period of three months from the date of receipt of the documentation from the staff member.

The Compliance Committee shall communicate to the staff member the outcome of the compliance monitoring conducted by the Third Party Auditor at the appropriate time as long as this is not harmful to the investigation.

The Compliance Committee reserves the right to conduct compliance checks even if there is no suspicion of non-compliance with the rules of the Policy, via the process outlined in the preceding paragraphs.

The Compliance Committee shall report the outcome of the compliance monitoring to the Bank's Audit Committee at least twice yearly in June and December or more frequently as the need arises.

In the case of members of governing and decision-making bodies of the Bank and external consultants working within the Bank, the Governor shall assume the compliance monitoring responsibilities of the Compliance Committee outlined in this paragraph via the Third Party Auditor.

In cases where a member of staff does not comply with the requirements of the Compliance Committee and/or Third Party Auditor or with the rules established by this Policy, the Compliance Committee shall report this finding immediately after the incident to the Governor and the Audit Committee. Upon receipt of this report from the Compliance Committee, the Governor shall report any major incident related to non-compliance with the provisions of this

Policy without undue delay to the Governing Council via the Organisational Development Committee. In urgent cases, the Governor may report a major incident related to non-compliance directly to the Governing Council. The ECB Audit Committee shall be also informed in parallel.

These rules established in paragraph 8 do not prejudice any disciplinary action that may be taken by the Bank in accordance with the provisions of the Bank's Collective Agreement.

9. Reporting Cases of Non-Compliance with the Provisions of this Policy

Any member of staff may report cases of non-compliance with the provisions of this policy in accordance with the procedures established by the Bank's Policy on Whistleblowing.

10. Liability

The Bank, members of the Compliance Committee and members of staff entrusted with a function under this Policy acting in good faith and in performance of functions as established by the Policy shall not be liable for any claims for losses sustained, or profit not achieved, in relation to constraints it places on an individual's ability to undertake transactions.

11. Discipline

Members of staff who fail to adhere to this policy shall be deemed to have acted in breach of the Bank's rules and practices and the Bank may, after taking into account the gravity of the breach, the findings and/or the recommendations of the Chief Officer responsible for human resources, invoke disciplinary procedures as stipulated in the Bank's discipline policy in accordance with the Collective Agreement and subject to the provisions of the Prevention of Financial Markets Abuse Act.

August 2016

APPENDIX I

CHAPTER 476

PREVENTION OF FINANCIAL MARKETS ABUSE ACT

Article 6

6. (1) No person shall use inside information to trade in any financial instrument admitted to a regulated market or in any other way to acquire or dispose of, or attempt to acquire or dispose of such financial instrument, whether for his own account or for the account of a third party, either directly or indirectly, if he is in possession of information related to such financial instrument by virtue of:

(a) his membership of the administrative, management or supervisory bodies of the issuer;

(b) his holding in the capital of the issuer;

(c) his having access to the information through the exercise of his employment, profession or duties; or

(d) his criminal activities.

(2) Any person who possesses inside information by virtue of any of the reasons listed in subarticle (1)(a) to (d) shall be prohibited from –

(a) disclosing inside information to any other person unless such disclosure is made in the normal course of the exercise of his employment, profession or duties, whether or not he knows or has reasonable cause to believe that such person or any other person will make use of the information for the purpose of dealing;

(b) recommending or inducing another person, on the basis of inside information, to acquire or dispose of financial instruments to which that information relates;

(c) counselling or procuring any other person to deal, on a regulated market in those financial instruments.

(3) The prohibitions of subarticles (1) and (2) shall also apply to an individual who is in possession of inside information even if this is not derived by virtue of any of the circumstances listed in subarticle (1)(a) to (d), in the event that such individual obtained or received such information directly or indirectly, from another person where the individual knew that he was receiving inside information or had reasonable cause to believe or ought reasonably to have known that he was receiving inside information.

(4) Where the person referred to in subarticle (1) is a legal person, the prohibition laid down in that subarticle shall also apply to the natural persons who take part in the decision to carry out the transaction for the account of the legal person concerned.

(5) This article shall not apply to transactions conducted in the discharge of an obligation that has become due or to acquire or dispose of financial instruments where that obligation results from an agreement such as an agreement granting a share option concluded before the person concerned possess inside information.

(6) (a) In relation to derivatives on commodities, inside information shall mean information of a precise nature which has not been made public, relating, directly or indirectly, to one or more such derivatives and which users of markets on which such derivatives are traded would expect to receive in accordance with accepted market practices on those markets.

(b) Users of markets on which derivatives on commodities are traded, are deemed to expect to receive information relating, directly or indirectly, to one or more such derivatives which is routinely made available to the users of those markets or required to be disclosed in accordance with legal or regulatory provisions, market rules, contracts or customs on the relevant underlying commodity market or commodity derivatives market.

(7) The provisions of this article shall also apply to:

(a) any public employee or former public employee who holds inside information by virtue of his position or former position as public employee; or

(b) any person who directly or indirectly obtained or received information from a public employee or former public employee who he knows or has reasonable cause to believe held the information by virtue of any such position.

APPENDIX II

LIST OF FINANCIAL INSTRUMENTS

1. Transferable Securities.

   Those classes of securities which are negotiable on the capital market and include:

   (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depository receipts in respect of shares;

   (b) bonds or other forms of securitised debt, including depository receipts in respect of such securities;

   (c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities (including gold) or other indices or measures.

2. Money Market Instruments.

   Those classes of instruments which are normally dealt in on the money market, such as treasury bills, certificates of deposit and commercial papers and excluding instruments of payment.

3. Units in collective investment schemes.

4 Options, futures, swaps, forward rate agreements and any other derivative contracts relating to securities, currencies, interest rates or yields, or other derivative instruments, financial indices or financial measures which may be settled physically or in cash.

5. Options, futures, swaps, forward rate agreements and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event).

6. Options, futures, swaps, and any other derivative contracts relating to commodities, that can be physically settled provided that they are traded on a regulated market, within the meaning of the Financial Markets Act (Cap. 345) and, or a Multilateral Trading Facility within the meaning of the First Schedule of the Investment Services Act (Cap 370).

7. Options, futures, swaps, forwards and any other derivative contracts relating to commodities, that can be physically settled, are not for commercial purposes, are not included in paragraph 6 of this Appendix, and, which have the characteristics of other derivative instruments, having regard to whether, inter alia, they are cleared and settled throughout recognized clearing houses or are subject to regular margin calls.

8. Derivative instruments for the transfer of credit risk.

9. Rights under a contract for differences or under any other contract the purpose or intended purpose of which is to secure a profit or avoid a loss by reference to fluctuations in the value or price for property of any description or in an index or other factor designated for that purpose in the contract.

10. Options, futures, swaps, forward rate agreements and any other derivative contracts relating to climatic variables, freight rates, emission allowances or inflation rates or other official economic statistics that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event), as well as any other derivative contracts relating to assets, rights, obligations, indices and measures not otherwise mentioned in this Schedule, which have the characteristics of other derivative instruments, having regard to whether, inter alia, they are traded on a regulated market within the meaning of the Financial Markets Act or a Multilateral Trading Facility within the meaning of the First Schedule of the Investment Services Act, are cleared and settled through recognized clearing houses or are subject to regular margin calls.

11. Certificates or other instruments which confer property rights in respect of any instrument falling within this Schedule.

12. Foreign exchange acquired or held for investment purposes.

APPENDIX III

COMPLIANCE MONITORING FORM

In accordance with Section 8 of the Policy on the Prevention of Abuse of Insider Information

Surname (in block capitals), First Name:	**Office Telephone Number:**
Office and Department:	
Reporting period: the information below is valid as for the following period *(The reporting period must tally with the request made by the Compliance Committee).*	
Information Required:	
a) List all bank accounts[2]:	

Name & Address of bank/stockbroker/financial institution	**Account number(s)**	**Type of account**

[2] Please include: Current Accounts, Savings Accounts, Debit and Credit Accounts, Accounts held with the Malta Stock Exchange, Accounts with investment advisors both local and foreign. Accounts relating to the CBM should be limited to current accounts (i.e house loan or unsecured loans accounts should be omitted).
In the case of joint accounts, it is important to note that these too should be included, clearly stating that the account in question is a joint account (for the sake of clarity, accounts in the sole name of spouses or partners should be omitted).
Please exclude any fixed term accounts.

b) List any powers of attorney which third parties (including your spouse) have conferred upon you in connection with any bank account, including custody accounts.

Name of Principal Account Holder	Name and address of bank/stockbroker /financial institution	Account number(s)	Type of account

c) If at the time of this declaration, you have given instructions to a financial institution/broker to execute financial transactions, these should be declared below:

Name and address of third party	Details of Instructions

I hereby declare that the information provided is correct and complete and I am hereby granting my consent for this information to be processed in accordance with the Central Bank of Malta Policy on the Prevention of Abuse of Insider Information (referred to as the "Policy").

I hereby certify that this information is exhaustive and in compliance with this Policy.

[please sign here]

Date: [insert day-month-year]

Privacy Statement

The Central Bank of Malta (the "Bank") guarantees that any personal data processed in this form shall be in accordance with the requirements of local and EU legislation on data protection in force at the time of the data processing, including the General Data Protection Regulation - GDPR (Regulation (EU) 2016/679). Processing of personal data in this application form is being carried out solely for the compliance monitoring exercise, in accordance with Section 8 of the Bank's Policy on the Prevention of Abuse of Insider Information. This form will be available only to the Third Party Auditor. No personal data will be passed on to third parties. All documentation pertaining to the employee shall be returned to the employee by the Third Party Auditor upon completion of the compliance monitoring. The applicant has the right to access and port his/her personal data, rectify, erase and restrict his/her personal data and to object to processing in terms of the GDPR. Failure to provide personal data as required in this form shall result in the Bank invoking disciplinary procedures as stipulated in the Bank's discipline policy, in accordance with the Collective Agreement and subject to the provisions of the Prevention of Financial Markets Abuse Act (Cap. 476 of the Laws of Malta). Complaints on data protection may also be addressed to the Office of the Information and Data Protection Commissioner via *www.idpc.org.mt*.