INFORMATION HANDLING AND INFORMATION BARRIERS POLICY

For

RABOBANK in IRELAND ENTITIES

For Internal Use Only

Policy Owner	**Compliance Department**
Next review date	**31 July 2017**

Version Control	Issue Date	Completed by	Reviewed by:	Approved by
v 0.1	07.11.11	Compliance Department – based on revised Group Policy		
v 1.1	28.08.2014	Compliance Department – Review of Policy	Noel Glennon/Jason Palmer	Mairead Butler – Head of Compliance
V2.0	June 2014			Management Team
V3.0	July 2015	Compliance Department – based on revised Group Policy	Hugh Place	Management Team

Contents

1. INTRODUCTION

1.1 GENERAL BACKGROUND

This Policy applies to ACC Loan Management Limited, Rabobank Ireland plc and Rabobank Dublin (including RaboDirect) otherwise known as "Rabobank in Ireland".

Confidential Information generated and gathered in the course of business is a valuable asset. Protecting this information is critical to the reputation of Rabobank in Ireland and the relationship with its Clients. The proper handling of Confidential Information furthermore promotes and preserves market integrity. It helps to prevent insider dealing and other forms of market abuse and is vital to ensure that Rabobank in Ireland may continue to operate the different business lines in which conflicts are inherent.

This Policy is to be reviewed by Compliance at least once every two years.

1.2 SCOPE OF THE POLICY

This Policy aims to set out the minimum requirements in relation to the handling of Confidential Information and Information Barriers. All business lines and business units of Rabobank in Ireland (insofar as applicable to their business) must adhere to these standards.

This local Rabobank in Ireland Policy is based primarily on the Rabobank Group 'Policy on Information Handling and Information Barriers[1]', which covers all Rabobank Entities and Employees within the Rabobank Group. It is also based on the Rabobank Global WRR Standard on Conflicts of Interest, which further specifies the requirements of a number of related Group policies.[2] The local Policy also takes into account local requirements, in particular requirements of the Consumer Protection Code[3]. The Policy is written at a high level to address both the retail and wholesale businesses and cannot address every aspect of this topic.

For any questions related to this Policy, please contact Compliance:

fm.ie.acc.Compliance or fm.ie.dublin.complianceIFSC

This Policy (and associated documentation) is available on the Compliance SharePoint page.

1.3 PURPOSE OF THE POLICY

The improper handling of Confidential Information may lead to legal, regulatory and reputation risks resulting in criminal prosecution, civil claims by clients or other involved parties and administrative sanctions being imposed by financial supervisors.

[1] This Group Policy was approved by the Executive Board in February 2015.

[2] WRR Standard approved by MT WRR in May 2015. Includes requirements on 3 Group policies: Conflicts of Interest; Information Handling and Information Barriers; Personal Account Dealing.

[3] CPC (2012), See sections 3.33-3.34.

The purpose of this Policy is therefore to assist the business:

- To protect Confidential Information and to prevent that such Confidential Information becomes known outside the circle of persons who need to be aware of this information as part of their duties, profession or position; and
- To prevent or monitor the exchange of information between Employees performing different activities involving a risk of a Conflict of Interest.

1.4 RELATIONSHIP TO OTHER POLICIES

The handling of Inside Information and other Confidential Information, Conflicts of Interest and Market Abuse are closely connected. Confidential Information may, on occasion, constitute Inside Information.

Having access to Confidential Information may therefore lead to Insider dealing, other forms of Market Abuse or to Conflicts of Interest. Within this context, this Policy is closely related to the Rabobank in Ireland ***Conflicts of Interest Policy and the Market Abuse Policy*** and associated procedures, which are available on the Compliance page on SharePoint.

2. DEFINITIONS

For the purposes of this Policy, the subsequent words have the following meanings:

Business Partner

A natural person or legal entity that supplies goods to, and provides services for or on behalf of, an entity of the Rabobank Group or with which a Rabobank entity has an alliance.[4]

Client

A (legal) person obtaining products and/or services provided by a Rabobank entity based on an agreement. In the context of this Policy, a Client also includes prospects to which a verbal or written offering of a services or product has been made.

Compliance Officers

Compliance Officers are those Employees who hierarchically and/or functionally report to (ultimately) Supervision & Compliance. This can thus be local, Group or Global Compliance Officer or Compliance specialist/analyst.

Confidential Information

Any (verbal or written) information (including Inside Information) obtained in the course of an Employee's employment, which is not in the public domain and which is related to Rabobank, its Employees, its Clients, or Business Partners, that is subject to confidentiality (either by agreement or otherwise).

Conflict of Interest

An actual or potential conflict of interest arises where two or more parties which (could) have competing interests. In this Policy, a conflict of interest means that acting in the interest of one of the parties can entail not (or not fully) acting in the interest of the other party (parties).

Employee

Anyone employed by Rabobank in Ireland (and the wider Rabobank International Group), whether under a permanent, secondment, contractual basis or temporary contract.

Information Barriers (Previously known as Chinese Walls)

The system of policies, procedures, and/or physical arrangements used to manage Confidential Information from becoming known outside the circle of persons who need to be aware of this information as part of their duties, profession or position ('need to know'). To also prevent and monitor the exchange of information between Employees performing different activities involving a risk of a Conflict of Interest and whereby the exchange of this information could be harmful to involved parties' interests.

[4] Some examples of Business Partners are, but not limited to, third parties such as intermediaries, charity organisations, sponsorship parties, consultants, representatives, distributors, consortia, contractors, suppliers or joint venture partners.

Inside Information

Specific information (also called: price sensitive information) that relates directly or indirectly to an issuer[5] of financial instruments to which the financial instruments pertain, or to the trade in those financial instruments. If the information has not been publicly disclosed and whose disclosure might have a significant influence on the price of the financial instruments or on the price of derivative financial instruments.

Insider

Any person who has or may have access to Inside Information on a regular or (in relation to financial instruments issued by any part of Rabobank Group) occasional basis.

MAC Unit

The expertise unit of Rabobank on the subjects of Market Abuse, Anti-Corruption and Conflicts of Interest. The MAC unit is part of Supervision & Compliance and is based in Utrecht.

Rabobank entity

Business Lines and (staff) departments within the Coöperatieve Centrale Raiffeisen-Boerenleenbank, B.A (CCRB), a member bank, foreign branch and/or a legal entity in which the CCRB holds a direct or indirect majority stake[6] (capital interest or voting rights) and any other Rabobank entity as appointed by the Executive Board of Rabobank.

Rabobank in Ireland

The organisation comprising of the Rabobank entities operating in Ireland: ACC Loan Management Limited, Rabobank Ireland plc and Rabobank Dublin (including RaboDirect).

Sensitive Transaction

A transaction where Inside Information is involved as input or which constitutes Inside Information itself, or transaction, which entails an identified or potential Conflict of Interest between different Clients or between Rabobank in Ireland and a Client or between Rabobank in Ireland and a Business Partner.

[5] Which, for the avoidance of doubt, may be a Client, a subsidiary or participation of Rabobank, Rabobank itself, or any other company having issued financial instruments.

[6] Majority: more than 50% capital interest or voting rights.

3. GENERAL PRINCIPLES

3.1 CONFIDENTIAL INFORMATION

All information obtained in the course of an Employee's employment, which is not in the public domain and which is related to Rabobank, its Employees, its Clients and or its Business Partners must be treated with care and diligence and must be kept confidential. Besides, it is an implied or explicit term of the contract between Clients and/or Business Partners and Rabobank in Ireland, that all information from and about Clients and/or Business Partners which is not in the public domain should be kept confidential.

This duty of confidentiality entails two related duties, not to:

- Disclose Confidential Information (except where the Rabobank in Ireland is compelled by law or has a public duty to disclose or where the client or Business Partner has agreed to the information being disclosed); and
- Use Confidential Information other than for the purpose for which it was given.

3.2 INSIDE INFORMATION

Inside Information may not be spread outside the circle of persons who need to be aware of this information as part of their duties, profession or position and utmost care must be exercised in dealing with Inside Information or information that could reasonably be suspected to classify as price-sensitive.

3.3 EXCHANGE OF INFORMATION

Without prejudice to the principles mentioned in paragraph 3.1. (Confidential Information) above, the exchange of information between Employees engaged in different activities involving a risk of a Conflict of Interest must be prevented or controlled, as the exchange of that information could harm the interests of one or more involved parties.

4. MINIMUM STANDARDS FOR THE HANDLING OF INFORMATION AND INFORMATION BARRIERS

Rabobank's minimum standards to protect and control the circulation of Confidential Information are summarised below:

4.1 THE "NEED TO KNOW" PRINCIPLE

The number of Employees with access to Confidential Information should be limited to the minimum extent possible. Only Employees who strictly require the information as part of their duties, profession or position should be given access to the information and access is limited to the necessary amount.

Steps must be taken to minimise the risk of outsiders finding out about, or speculating on impending Sensitive Transactions. Depending on the circumstances, these steps may include amongst others:

- Locating staff involved in Sensitive Transactions in secure areas that are separate from other Employees and public areas;
- Holding meetings off-site;
- Using specifically trained administrative and IT support staff that are dedicated to the project; and
- Specifically relating to conference calls regarding Sensitive Transactions, dedicated and one-off telephone numbers with secured (PIN) codes and passwords must be used.

The necessary systems and controls should be in place to quarantine Confidential Information from contractors and other third parties that share access to the company's systems.

Staff should be reminded not to have confidential discussions in places they could be overheard by others.

4.2 CLIENT ENGAGEMENT – RELEVANT FOR RABOBANK ENTITIES AND EMPLOYEES IN WHOLESALE

The Wholesale Engagement Standard is applicable to all Rabobank Entities and Employees in Wholesale business lines. Its purpose is to describe the key concepts and procedures relating to Client Engagement such as guidance on different market sensitivity level categories, commercial positioning, entering information in ClientLink and Compliance issues in relation to Client Engagement. Please refer to ***Rabobank Engagement Standard Wholesale process*** dated 24 March 2015.[7]

Internal Employee Movement

Management must ensure that where there is internal movement of staff, Compliance must be consulted before the transfer. This is to ensure that potential conflicts have been assessed and appropriate measures have been put in place and documented before the transfer. This will include the employee signing a rules of engagement form confirming they understand and accept the obligations required of the role. A copy of the signed form needs to be forwarded to the MAC Unit. This will be done in conjunction between HR and Compliance. This requirement on internal employee movement is only applicable to the Wholesale business lines in Rabobank in Ireland.

---

[7] http://meetingpoint.rabonet.com/news/Pages/Implementation-Engagement-Standard-Wholesale.aspx

4.3 INFORMATION SHARING

Within the same business line, business entity or department, or with supporting departments[8], Confidential Information (which, for the avoidance of doubt, includes Inside Information) may only be shared:

- If required in the normal exercise of duties, profession or position;
- If limited to the necessary amount of information; and
- Where the Client provided the information for a specific purpose and sharing of information serves another purpose, with the prior written explicit consent of the Client.

With (other) business lines, business entities or departments (other than supporting departments) separated by Information Barriers:

i. Confidential Information (which, for the avoidance of doubt, includes Inside Information) may only be shared:
   - If required in the normal exercise of duties, profession or position;
   - If limited to the necessary amount of information;
   - Where the Client provided the information for a specific purpose and the Client has provided written explicit consent.

ii. Where the Confidential Information consists of Inside Information there must be prior approval from:
   - Local management (the Head of Department or the 'The Deal Captain'); and
   - Compliance (who may impose conditions and restrictions, e.g. keeping insider lists).

iii. Without these approvals (Client and/or Business Partner/local management) Confidential Information may only be shared, in line with the 'need to know' principle within:
   - Credit Risk departments, if this is required for credit risk management purposes in relation to the Client to which the Confidential Information pertains;
   - Special Asset Management departments if this is required for risk management purposes in relation to the Client to which the Confidential Information pertains;
   - Risk Management functions generally if this is required for the proper exercise of risk management and oversight activities.

Where personal data is being shared in these circumstances, the Rabobank in Ireland ***Data Protection Policy*** should be consulted. Compliance may be contacted for guidance.

Management must develop, maintain and implement a procedure for how a (suspected) leak of Confidential Information is dealt with, including a leakage investigations procedure. Whether in a certain case, an investigation should be instigated and the level of formality and intensity of that investigation depends on the significance and impact of the detected leak.

[8] Legal, Compliance, Credit Risk Management and such other departments as may be determined by Compliance WRR.

After discovery of a (suspected) leak of Confidential Information, Compliance must be contacted immediately. Compliance will determine if whether it is appropriate or not to inform Fraud & Corporate Security (F&CS) in Head office.

4.4 INFORMATION BARRIERS (CHINESE WALLS)

a. Chinese Walls between Business Lines

To prevent Confidential Information from becoming known outside the circle of persons who need to be aware of this information as part of their duties, profession or position. To prevent or monitor the exchange of information between Employees performing different activities involving a risk of a Conflict of Interest, there must be organisational, physical and personnel segregations up to the highest possible level between the different business lines:

- Management directly responsible for the day-to-day management of the business line must only act on one side of the Chinese Wall;
- Only members of the Rabobank in Ireland Management Team have unrestricted access to information, in line with the 'need to know' principle from all business lines, business units and activities within Rabobank in Ireland; They are thus placed 'above the information barrier' on a permanent basis and do not need prior approval to access Confidential Information.
- Employees work on one side of the Chinese Wall and report to the managers in their respective business lines only, unless otherwise agreed in writing and confirmed by Compliance;
- Employees of any business line work in office buildings or areas that are not accessible for Employees of other business lines or third parties without express authorisation;
- Employees of any business line make exclusive use of information obtained from data-storage systems that are not accessible to other business lines or third parties;
- Exchange of information only takes place in accordance with the rules for Information Sharing described in paragraph two (Information Sharing).

Each of the parts of the business so divided will take decisions without reference to any interest, which any other such part, or any person in any other such part of the business may have in the matter. The business may consult Rabobank in Ireland Compliance on these decisions, but must inform Compliance of any identified or potential Conflict of Interest that may be or is foreseen as arising between different clients or between Rabobank and a Client. Compliance will then inform the MAC Unit, as required.

Information Barriers segregate employees into two categories:

- Public side, which persons only have access to public information;
- Private side, which persons who, in the ordinary course of their work have access to Inside Information in relation to a Client and/or transaction they are working on.

An overview of both public and private departments within Rabobank in Ireland should be available and maintained.

For Rabobank in Ireland the following business areas are considered Private side:

Private Side departments
Global Corporate Clients – RI plc
Asset Based Finance (ABF) – RI plc
Global Client Solutions (GCS) – RI plc

Public Side departments
Treasury Ireland (TRG) – RI plc

All other Rabobank in Ireland entities are public side, i.e. ACCLM, Rabobank Dublin and RaboDirect. There is a physical segregation between the Public and Private side business areas.

Apart from Chinese Wall arrangements between business lines, specific Chinese Wall arrangements (like "Chinese boxes") may be necessary within business lines. Additional specific requirements can be set in conjunction with Compliance.

b. Wall Crossing

Crossing Chinese Walls must be justifiable and held to a minimum. For the execution of a transaction or duty to a Client, however, it may be necessary for an Employee who has Confidential Information to disclose that information to an Employee on the other side of the Chinese Wall. In this situation, the person receiving the information is taken "over the wall" upon receiving this information.

Likewise, it may be necessary to create a deal team, or set up a meeting for a specific transaction, that consists of staff members from different business lines, business units or departments. In these situations, both the sending and receiving management must approve such wall crossings beforehand in conjunction with Compliance as laid out in the specific Wall Crossing Procedure (Appendix I). Compliance may impose conditions and restrictions. Any wall crossing must be recorded and reported to Compliance prior to the wall being crossed.

Members of the Executive Board of Rabobank Nederland and members of the Management Teams of WRR, who stand on the wall by virtue of their function, should not be actively involved in or become part of a deal team.

In line with the 'need to know' principle and if required in the normal exercise of duties, profession or position, certain (risk) management functions may also be given access to certain Confidential Information without prior approval on a case by case basis by Management and Compliance. Management must implement and maintain an adequate policy and procedure in this respect approved by a higher level of management. Employees in the following functions do not need to be wall crossed:

- Compliance Officers;
- Legal;
- Credit Risk Management (for the avoidance of doubt, this excludes credit risk analysts).

c. Above an Information Barrier ('above/on the wall')

Management of Rabobank entities by virtue of their position and in line with the 'need to know' principle, do not need any prior approval to access Confidential Information within their Rabobank entity. They are thus placed 'above the Information Barrier' on a permanent basis for their Rabobank entity.

The table below gives an overview of management roles within the Rabobank matrix organisation that are deemed above the Information Barrier (above/on the wall').

Managers	General	Product	Sector
Global	**MT Business Line Heads (Head GCC/GWPC)** Permanently above the wall globally for own products in their business line	**Global Product Heads** Above the wall globally for own product	**Global Sector Head** Can only be above the wall for own sector globally as far as not involved in a deal team
Regional	**Regional MT Member** Permanently above the wall for all products in own region	**Regional Product Heads** Can only be above the wall for own product in own region as far as not involved in a deal team	**Regional Sector Head** Can only be above the wall for own sector in own region as far as not involved in a deal team
Local	**General (country) Managers** Permanently above the wall for all products in own location if role is not combined with SRB role and deal team involvement, otherwise only be above the wall as far as not involved in a deal team	**Local Product Heads** Can only be above the wall for own product in own location as far as not involved in a deal team	N/a
Client owners	SRB or Relationship manager in product line: e.g. RM LPG or RM TCF	Client owners should have full overview of all opportunities where the bank is engaging directly with the client. They are so to speak "Above the wall for their client only", provided: • their client is not the target in the opportunity and • conflicting opportunities with other clients in their portfolio are managed so that information of one client is never used for the purpose of another client • The client does not withhold consent to share opportunity information with the Client owner	

Above the wall, members only in very exceptional situations can get involved in a deal team, need to know all client names for role as manager in engagement, pipeline

Above the wall in a management role, but management roles are regularly combined with operational roles that require participation in deal teams

Never above the wall, always on the client side of the wall

d. Disciplinary sanctions

Where Chinese Walls are breached (other than pursuant to wall crossing procedures), Employees who are in a position to misuse the Confidential Information, should be notified of the prohibition to do so and steps should be initiated to monitor any violation. Appropriate disciplinary sanctions may be taken in line with Rabobank in Ireland ***HR policy***.

4.5 CONFIDENTIALITY, EXCLUSIVITY AGREEMENTS AND STANDSTILL AGREEMENTS

In case of Sensitive Transactions, all advisors engaged by Rabobank in Ireland should be required to sign transaction-specific confidentiality agreements. These agreements should specifically restrict the use of the Confidential Information, which is shared with them. With respect to the content of such agreements, the Legal Department may be contacted for advice.

In principle, exclusivity and stand-still agreements may only be entered into for the part of business or the activity one is responsible for. Before signing any non-disclosure (also known as confidentiality), exclusivity or standstill agreement/clause with a client or Business Partner, approval may be required from:

- Relevant senior management;
- The Legal Department;
- The MAC Unit via the Compliance department.

All NDAs should be approved by Legal, unless there are exemptions in place that have been pre-approved by Legal. This could for example entail pre-approved templates.

The MAC Unit will have to be notified if exclusivity and/or standstill clauses or agreements are agreed. NDAs without such clauses or agreements do not have to be sent to the MAC Unit. In case an exclusivity or standstill clause is requested, which exceeds the authorisation of Management the applicable higher level of management must be consulted for approval.

4.6 INFORMATION TECHNOLOGY CONTROLS

IT systems and practices should be sufficiently secure to ensure Confidential Information on IT systems is not inadvertently leaked and information is not accessible by Employees or other persons who do not need access for their duty, profession or position. This means that Confidential Information is to be stored on protected drives and access tightly controlled through password protection and other blocking mechanisms, where appropriate.

Separate passwords should be provided when transferring confidential documents electronically. Alternatively, such documents should be encrypted. All electronic equipment containing Confidential Information should be protected with passwords and have automatic locking after brief periods in accordance with applicable ***IT Security Policies.***

Access to documents (including electronic records and computer files) which may contain information privy to a client or to Rabobank in Ireland is to be restricted and the restriction monitored by Compliance and/or IT security and/or the Local Security Officer.

Business Owners of an IT system must periodically perform a user account recertification, to update access rights related to joiners/transfers/leavers i.e. whether users should still have access to the relevant IT system. This means that all user groups are asked to validate a user account list.

Managers must check at least yearly whether employees store documents in the appropriate part of the department's hard drive, where it is only accessible for those who have a 'need to know'.

Rabobank in Ireland IT policies and controls must be able to support the Group policy and the WRR Standard.

4.7 PHYSICAL DOCUMENT MANAGEMENT

Physical copies of documents containing Confidential Information should be marked "Confidential" and securely stored when not in use. Where required by law such documentation must be disposed of when no longer required, with access restricted to authorised staff only ("Clean desk" policy).

Dedicated, or password-protected, printers and faxes should be used for printing and faxing of documents containing Confidential Information. Staff should be reminded not to read or use documents containing Confidential Information in public areas.

4.8 CLASSIFICATION OF DOCUMENTS

Sensitive Transactions documents must be classified according to the level of protection required. A document classification system must prescribe the specific requirements for creating, distributing, storing and disposing of each class of information, reflecting the risks relating to loss of confidentiality of that information.

Management must ensure that all Confidential Information has an appropriate information owner, who is responsible that the information is correctly labelled as Confidential Information, relating to a Sensitive Transaction and/ or as Inside Information and dealt with in line with this Policy and any other applicable policy and/ or procedure.

Labelling of information within WRR is deemed to be done when storing confidential Client Information on dedicated and access protected parts of a departments' hard drive and in ClientLink. Within ClientLink, all information is labelled confidential, as it is only visible to a restricted number of people that have a need to know. Access to Transaction specific information is moreover restricted to the deal team. Management of ClientLink is done centrally by Group IT in Utrecht.

Any other (physical and digital) information (not being public information) available in a Rabobank Entity should be deemed at least as confidential when relating to a Client. As a result of information being labelled as "Confidential Information" or "Inside Information", the need to know principle applies. This may trigger other requirements, such as clean desk, locked file cabinets, separate meeting rooms, data rooms etc.

4.9 CODE NAMES

Code names should be used to anonymise the parties involved in Sensitive Transactions, to preserve confidentiality and to prevent the improper use and dissemination of Confidential Information. A code name must not be related to the company or sector involved and the name must be neutral, appropriate and not suggestive. In case of doubt as to the acceptability of a code name, contact the MAC Unit via Compliance.

4.10 CONTACT WITH MEDIA

Rabobank in Ireland must have a local policy to control any interaction its staff might have with the media (including social media) in relation to the company and its affairs. This policy should explicitly cover who is responsible for media contacts and who may act as spokesperson. When an employee is approached by a journalist for a quote, reaction or interview, the employee must not give a response but must always contact the Head of Compliance and Corporate Affairs or press office first. In sensitive situations with potential publicity impact on the Business line, other parts of Rabobank Group or Rabobank Group as a whole, the press office of Rabobank Nederland in Utrecht must be contacted in time by the Head of Compliance and Corporate Affairs.

4.11 REPORTING INSIDE INFORMATION AND MAC UNIT

All Sensitive Transactions should be reported by the business to Compliance to allow Compliance to report to the MAC Unit without delay. All Inside Information (which is not related to a Sensitive Transaction) and every reasonable suspicion of the misuse of Inside Information must be reported to Compliance without delay.

Compliance keeps a list of (potential) clients on which Inside Information is available in a business line or activity ('The Restricted Client List').

4.12 INSIDER LIST

The number of staff who have access to Inside Information must always be kept to a minimum. Each business line and business unit must have a developed process for how and when Employees are designated as Insiders. Compliance maintains a list of people who are deemed as Insiders ('The Insider Lists'). The Insider Lists comprise of:

(i) Permanent Insider List – People who may have access to Inside Information on a regular (or, in relation to financial instruments issued by Rabobank, occasional) basis;

(ii) Sensitive Transactions List – A separate list will, in addition, be maintained for each Sensitive Transaction/Coded Project. The Sensitive Transaction Insider List will contain the names of the individuals who have knowledge of the transaction details and the client names.

Insider lists should state the identity of the person, the reason why they are on the list and the date the list was created. The lists must be complete, accurate and regularly updated.

Employees on insider lists must be made aware of the duties and obligations in relation to the handling of Inside Information, the prohibition on insider dealing and the restrictions on personal account dealing.

4.13 TRAINING

Appropriate measures should be taken to assist Employees in the proper handling of Confidential Information and understanding and applying the procedures and measures (including Chinese Walls) designed to protect this information.

Management of the local business line or business unit, supported by Compliance, must ensure that relevant staff are adequately trained. Training is to be an ongoing process that is updated regularly to reflect current developments and changes to laws and regulations, as well as to reinforce internal policies and procedures. Training can be done in different forms depending on the scale and size of each business, e.g. new joiners training sessions, e-learning, refresher training and targeted training.

5. RESPONSIBILITIES FOR COMPLIANCE WITH THIS POLICY

The overall roles and responsibilities with regard to the Rabobank in Ireland Compliance Function are outlined in the Terms of Reference available on SharePoint. This Part summarises the roles and responsibilities related to the handling of Inside Information and other Confidential Information and Information Barriers.

The Management Team

- Compliance with all legislation and regulations and the proper handling of Confidential Information;
- The endorsement and approval of this Policy for all business units and business lines of Rabobank in Ireland.

Line Managers

- Direct compliance with this Policy;
- Translating this policy into effective operational guidelines, procedures and work instructions, as well as for effective training for the staff involved.

Compliance

- Supporting management in translating the Policy into operational guidelines and procedures;
- Providing advice upon request and appropriate training, as necessary;
- Monitoring compliance with this Policy and relevant operational guidelines and procedures;
- Reporting incidents pertaining to violations of this Policy and related guidelines and procedures in periodic reports to Compliance WRR (i.e. Rabobank Group Compliance);
- The Policy, the guidelines and procedures will be reassessed by Compliance in the event of organisational changes.
- The policy itself will be reviewed on a bi-annual basis.

Internal Audit

- Independent review of this Policy and associated controls at their own discretion or as directed by the Audit & Compliance Committee.

Legal

- Providing advice on any legal issues arising from this Policy.

Compliance WRR

- Monitoring developments in relevant (inter)national legislation;
- Formulating and updating (on the basis of new or changed legislation and regulations) a policy for WRR;
- Supporting Rabobank in Ireland Compliance in translating the policy and creating input for training and e-learning.

APPENDIX I – WALL CROSSING PROCEDURE

Wall Crossing Procedure (Public to Private) & (Private to Private)

Wall Crossing Procedure is to be used when wall-crossing a Public side Employee into a (Private side) deal team or a Private side Employee into a (Private side) deal team.

1. (A) seeks initial approval to wall-cross (B) from Compliance by providing the following information:

    a) Name of individual(s) whom you intend to wall cross;
    b) The reason for needing to wall cross the person (i.e. why does this person need to know);
    c) The name of the Issuer(s) that the inside/relevant information relates to;
    d) The nature of the inside/relevant information (i.e. what characteristics of the information make it inside/relevant);
    e) Any project name assigned to a transaction;
    f) The name of (B)'s line manager.

2. Compliance checks with the MAC Unit that (B) is not involved in any conflicting transaction or conflicted otherwise. If (B) is involved in a conflicting transaction, Compliance will decline initial request. Otherwise, Compliance will approve the initial request if the conflict is manageable.

3. If the request is approved by Compliance, Compliance will seek approval from (B)'s line manager (or appropriate senior manager in line manager's absence). Line manager must be given limited information.

4. If the request is approved by the line manager, Compliance will send the request to (B) and inform him/her of any relevant restrictions applicable to (B) should he/she accept the request. (B) must be given the right to decline the Wall Crossing request.

5. (B) must either accept or decline wall-crossing request.

    If (B) agrees to be wall-crossed, Compliance will send out confirmation email to all parties concerned confirming that the wall-crossing is effective and that (B) is deemed off-side until the transaction is made public or information provided has gone stale.

6. If ClientLink is used the deal team captain adds the wall crossed person to the ClientLink deal team.

In all cases there must be a full audit trail available.