II. Internal Rules for the Processing of Inside Information

C

3 July 2016

Index

Preamble

These *Internal Rules for the Processing of Inside Information* (the "***Rules***") form part of the Corporate Governance System of IBERDROLA, S.A. (the "**Company**") and are approved by the Company's Board of Directors upon a proposal of the Compliance Unit, elaborating upon the *Internal Regulations for Conduct in the Securities Market* (the "***Internal Regulations for Conduct***"), article 9.4.c) of which provides that security measures shall be established for the custody, filing, access, reproduction, and distribution of Inside Information, as such term is defined in such *Internal Regulations for Conduct*.

To such end, these *Rules* establish the rules governing the management, control, and internal and external transmission of Inside Information, whatever the location, format, supporting media, or means of transmission thereof, in order to protect the interests of shareholders and investors and to prevent and avoid any instances of misuse.

PRELIMINARY TITLE

Article 1. Definitions

Capitalised terms used in these *Rules* and not expressly defined shall have the meaning ascribed to them in the *Internal Regulations for Conduct*.

For purposes of these *Rules*, the following terms shall have the meaning ascribed below:

a) Director of the Area: means the director of the Area responsible for coordinating the work or transaction to which the Inside Information refers and for keeping custody of such information.
b) Guide: the *Guide to Protecting Inside and Confidential Information* prepared by the Company's Finance and Resources Division, which shall apply in the alternative to all matters not expressly contemplated by these *Rules*.
c) Insiders: the persons defined as such in the *Internal Regulations for Conduct*, including, for these purposes, External Recipients.
d) Authorised Persons: means, within the context of a specific transaction, internal process, or activity in which Inside Information is received, generated, or accessed, the group of Affected Persons and/or Insiders that are authorised to access such information.
e) External Recipients: means those persons who are not employees or directors of the companies within the group of which the Company is the controlling entity, within the meaning established by law (the "**Group**"), that need to know the Inside Information in order to be able to provide their professional services (for example, to give advice on or analyse a transaction) or to carry out transactions with the Group (for example, to finance a transaction), who shall not be required to comply with these *Rules* except for the provisions of article 10.4.b) hereof.

Article 2. Purpose

The purpose of these *Rules* is to establish the rules and procedures of the Company for the internal processing of Inside Information and the transmission thereof to third parties unrelated to the Group, in order to protect the interests of shareholders and investors and to prevent and avoid any instances of misuse. All of the foregoing shall be without prejudice to the provisions of the *Guide*, which shall apply in the alternative to all matters not expressly contemplated by these *Rules*.

Article 3. Scope

1. These *Rules* apply to all of the companies within the Group, including the companies in which the Group has an interest and exercises effective control, within the limits established by applicable regulations upon the regulated activities carried out by the Group in the various countries in which it is present.
2. Listed companies belonging to the Group that have corporate governance rules similar to those of the Company, as well as with the subsidiaries thereof, shall be excluded from the scope of these *Rules*.

Article 4. Dissemination

These *Rules* shall be communicated to and disseminated among Affected Persons and Insiders in accordance with the plan designed by the Unit for such purpose, and such Affected Persons and Insiders shall be required to be aware thereof and to comply therewith.

Article 5. Duties of Affected Persons and Insiders in Connection with Inside Information

Affected Persons who have Inside Information, and any Insiders, shall be required to:

a) Safeguard the confidentiality of the Inside Information to which they have access, without prejudice to their duties of communication and cooperation with court and administrative authorities under the terms set forth in the MAR and other applicable legal provisions.
b) Adopt adequate measures to prevent the Inside Information from being misused or abused.
c) Give immediate notice to the Unit of any misuse or abuse of Inside Information of which they are aware.

Article 6. Interpretation

1. These *Rules* shall be interpreted in accordance with the legal provisions applicable to the Group and the provisions set forth in the Company's Corporate Governance System, and especially those contained in the *Internal Regulations for Conduct*.
2. The Unit shall be responsible for responding to any inquiries or concerns that may arise in connection with the content, interpretation, and application of or compliance with these *Rules*.

TITLE I. RULES AND PROCEDURES FOR THE PROCESSING AND INTERNAL AND EXTERNAL TRANSMISSION OF INSIDE INFORMATION

Article 7. Procedure for Determining the Inside Nature of the Information

The Director of the Area responsible for coordinating the work or transaction to which the information that may qualify as Inside Information refers shall be charged with determining the inside nature thereof. For such purposes:

a) The Director of the Area responsible for coordinating any internal process that entails access to information susceptible of being considered Inside Information or any legal or financial transaction being studied or negotiated in which such information is received or generated, must engage in an analysis thereof in order to verify whether it has the characteristics to be considered Inside Information, and if so, shall declare the inside nature thereof.

b) If the Director of the Area effectively determines that it is Inside Information, the processing and transmission of the information must be in accordance with the provisions of these *Rules*. The Director of the Area must also, as soon as practicable, inform the Unit, through the director thereof, that there is an internal process or a project in which Inside Information is going to be received, generated, or handled, and that appropriate measures have been adopted in order to safeguard the confidentiality thereof.

c) In any event, the Director of the Area may consult with the Unit in those instances in which it cannot clearly be determined whether or not the information in question is Inside Information.

d) Without prejudice to the foregoing, the Unit may, at any time, request the Director of the Area to provide additional information regarding a specific project, as well as revoke, if appropriate, the status given to the information by the Director of the Area if the Unit concludes that it is not Inside Information, in which case the Unit must provide a duly substantiated decision and explain in writing to the Director of the Area the reasons for the divergence.

Article 8. Authorisation for Access

1. The Director of the Area shall be responsible for authorising or denying access to the Inside Information, and authorisation shall only be granted to those persons whose access is indispensable because of their work.
2. The authorisations granted shall be revised at such intervals as the Unit determines in order to ensure that there is no person who, beyond a reasonable period (which must be the minimum possible period), is authorised to access Inside Information without a justified need to hold authorisation for access thereto.

Article 9. Register of Insiders

The Director of the Area or the person acting by delegation therefrom must adopt the measures required in order for all persons accessing Inside Information to be duly included in a Register of Insiders, in accordance with the provisions of the *Internal Regulations for Conduct*.

Article 10. Management of Confidential Documents

1. Code name: the responsible Area shall assign a code name to each transaction in which Inside Information is received or generated. This name shall be used in all communications relating to the transaction, such that neither the parties involved therein nor the characteristics thereof may be identified.
2. Marking or labelling: confidential documents must be marked "CONFIDENTIAL" on the cover page and on each of the other pages, and must also include the date of issuance thereof.
3. Use, control of access, and storage
   a) General principle

      Access to confidential documents, regardless of the format, media, and storage location thereof, must be restricted to Authorised Persons.

      Systems administrators, systems technical staff, and the staff of other auxiliary services must be subject, to the maximum possible extent, to restrictions on the possibility of access to equipment or locations in which Inside Information is stored. In the event that access by any of the aforementioned persons is essential, the number of persons entitled to access must be kept to the minimum required, any such access must be recorded, and, in the case of a service provider from outside the Group, the service agreement must include clauses ensuring the confidentiality of any Inside Information to which access may have been gained during the provision of the service.

   b) Documents in electronic format

      Authorised Persons must use sites on the internal restricted access network for the temporary or permanent deposit of confidential documents to which only such persons may gain access. As regards e-mails containing Inside Information or having attachments with Inside Information, it is recommended to delete them from mailboxes and to save them within sites on the internal restricted access network. In no event shall memory sticks or USB drives be used to store or transmit Inside Information. Confidential documents in electronic format must be encrypted. In this regard, a document may be deemed encrypted if the media or location in which it is contained is encrypted.

      In addition, Authorised Persons shall take the utmost care to prevent unauthorised persons from seeing confidential documents while Authorised Persons are working with such documents on a computer. Confidential documents must be printed on local printers or printers that require the use of a password located in limited access zones, and must be collected immediately after the printing thereof. In the event that a unit of equipment containing Inside Information must undergo repair or maintenance work and such work is performed at the workstation itself, the user of the equipment must be present while such work is carried out. If the aforementioned work requires the removal of the equipment but does not

affect the memory unit on which the data are stored, it must be removed and left in the custody of the user, who must store it under lock and key. On the other hand, if the aforementioned work requires the removal of the equipment and requires or may require any action on the memory unit on which the data are stored, the equipment may only be removed with the express authorisation of the Director of the Area. Whenever possible, any Inside Information contained in the memory of the equipment must be deleted prior to the removal (see section 5 below).

c) Paper documents

Authorised Persons shall store confidential documents in a safe place when they are away from their workstation.

To the extent possible, Authorised Persons shall avoid placing confidential documents on meeting-tables or in meeting rooms, and must store such confidential documents in restricted access locations (such as offices and file rooms) and keep them in file cabinets (which, as a general rule, must be kept locked), the keys or combinations for access to which shall exclusively be available to such persons. If a risk of copies of keys or access codes is detected, such keys or codes must be replaced or changed.

d) Use during travel and in public places/on public transport

When Authorised Persons travel with confidential documents (both in electronic and paper format), they shall take the utmost care in public places and on public transport (airports, airplanes, trains, taxis, etc.) to avoid the forgetting, misplacement, or theft of confidential documents and to prevent any unauthorised persons accidentally or deliberately seeing the content thereof.

In particular, Authorised Persons must keep confidential documents under their control at all times, and must avoid storing them in luggage that is to be checked, leaving them inside a vehicle (even if such vehicle is kept locked), or in a hotel room when they leave it. If it is essential to leave confidential documents in a hotel, the safe must be used.

4. Copies, distribution, and transmission

a) General rules

The making of copies of confidential documents is prohibited, unless the Director of the Area grants prior express authorisation for the delivery of such copies to an Authorised Person. The recipients of the copies must be warned of the prohibition against making subsequent copies. Only Authorised Persons may make copies of confidential documents. Copies of a confidential document shall be subject to the same protection and control requirements as the original.

The internal or external distribution or transmission of Inside Information shall be carried out with the prior express authorisation of the Director of the Area.

The area in charge of coordinating the work or transaction to which Inside Information refers shall, as the area responsible for the custody thereof, establish a mechanism (whether manual or automated) for the control of the copying, distribution, and transmission of Inside Information, such that the traceability thereof may be ensured, i.e. that each copy made of a confidential document, the person responsible for it, the copies made of it, and the person responsible for each copy, can be identified.

In addition, when justified and feasible in the opinion of the Unit, mechanisms shall be established to enable the detection of leaks or the unauthorised sending of Inside Information, which mechanisms shall be designed to facilitate a subsequent audit of procedures allowing for the discovery of the source of the leak.

— Specific measures for documents in electronic format

Authorised Persons shall use safe channels (encrypted mail, VPN, secure FTP, etc.) for the distribution of confidential documents in electronic format and, in particular, sites on the internal network that are not under restricted access shall not be used for such purpose.

When electronic media are distributed, the measures set forth in the next point shall apply and, in addition, the content thereof shall be encrypted.

— Specific measures for paper documents

Confidential documents on printed paper must be transmitted in a sealed envelope bearing the name of the Authorised Person who is the recipient and marked such that the nature of the information contained therein is clear (for example, "CONFIDENTIAL INFORMATION"). The envelope must be a single-use envelope and of a type that allows the detection of any unauthorised opening. Moreover, an e-mail must be sent to the recipient stating that information will be sent thereto, without indicating the nature of such information, and the recipient shall be required to send a reply e-mail when receipt has effectively taken place. Confidential documents containing Inside Information must be collected and delivered by hand, such that they must not be deposited in trays or on the recipient's desk when not present.

When documents are sent out, whether to other Company buildings or otherwise, the confidential documents shall be carried by authorised personnel and in compliance with security measures sufficient to ensure their safe carriage. If documents are sent to a location outside of the Company, they must be sent through a courier and a delivery receipt must be obtained. In any event, records must be kept of incoming and outgoing items in connection with documents so sent.

During the delivery process, the confidential documents must be stored in places that satisfy the access and storage requirements described above. In the event of loss or theft, immediate notice must be given to the issuer.

The use of fax machines as a means of transmission of Inside Information must be avoided. If the use thereof is essential, notice must be given to the recipient at the time of the transmission in order to ensure that the recipient collects the document at the same time it is printed at destination.

b) Additional provisions governing the transmission of Inside Information to third parties

Without prejudice to the rules and procedures described in the preceding sections of these *Rules*, the transmission of Inside Information to External Recipients must be restricted to those instances in which such transmission is essential in the opinion of the Director of the Area, and it shall particularly comply with the provisions of this section:

- Inside Information shall be transmitted to External Recipients as late as possible in given nature of the transaction in question.
- Prior to the transmission of any Inside Information, the External Recipients must sign a confidentiality undertaking with the Company unless the External Recipient is subject to legal or contractual rules that contain a duty of confidentiality. In any event, External Recipients shall be informed of and must state, at a minimum, that they are aware of: (i) the confidential nature of the information transmitted, (ii) the obligations stemming from the legal provisions applicable to the Inside Information, and (iii) the consequences of violating such legal provisions, and that (iv) they have the means required to ensure the confidential nature of the Inside Information. They shall also be informed of their inclusion in the Register of Insiders.

  The signing of such confidentiality undertaking shall also be required of those External Recipients with whom contact is made at a preliminary phase and to whom the general outline of a transaction is presented in order to request financing offers or advice, even if they do not ultimately participate in such transaction.
- In the event that Inside Information is transmitted to one or more External Recipients belonging to the same firm or entity, the confidentiality undertaking mentioned in the preceding section must be executed with the respective firm or entity, and shall equally bind all of the members of the organisation who come to know the Inside Information. In such cases, the prior express authorisation of the Director of the Area shall not be required in order to transmit the Inside Information internally to the members of the organisation that need to know it.

  Additionally, in the instances contemplated in the preceding section, the internal processing of the Inside Information shall be subject to the provisions established for such purpose by the organisations to which the External Recipients belong.
- The content and implications of the confidentiality undertaking must be explained orally in a clear and concise manner in the case of External Recipients that may not be acquainted with the applicable legal provisions.
- In any event, the transmission of Inside Information by an External Recipient shall require the prior written authorisation of the Director of the Area and the signing by the second External Recipient of an equivalent confidentiality undertaking.
- The Unit may condition the electronic transmission of Inside Information to External Recipients on the encryption of the confidential documents through any computerised procedure whereby access to the Inside Information by External Recipients is restricted.

5. Disposal: Authorised Persons who have had access to Inside Information must destroy any media containing such information at the time it ceases to be useful, unless there is a legal or business requirement that justifies the retention thereof. In this regard, it must be borne in mind that not only the final versions of the confidential documents must be destroyed but also all drafts, copies, excerpts, and other working documents containing Inside Information.

   When justified and feasible in the opinion of the Unit, confidential documents in electronic format must be disposed of by using a deletion tool that ensures that the deleted information is irretrievable.

   In the particular case that a computer of the Group (which contains or contained Inside Information) is removed or discontinued from use or the internal memory or any other data storage device is replaced, it must be destroyed such that the information stored cannot be retrieved.

   Confidential documents in paper format shall be destroyed by the means established by the Company for such purpose, consisting of paper-shredding machines (for small amounts of documentation) and of a centralised service for the mass destruction of documents (for large volumes).

   The destruction of confidential documents shall be carried out exclusively by Authorised Persons; in particular, the destruction of confidential documents shall not be entrusted to persons who are not authorised to have access thereto. In the event that persons from outside the Company (for instance, companies specialising in document destruction in the case of the destruction of large volumes of documentation) participate in the documentation destruction process, the service contracts must include clauses safeguarding the confidentiality of the Inside Information to which such external agents may have had access during the destruction process. In addition, such external agents shall be required to issue a certificate evidencing the destruction of the confidential documents.

Article 11. Protection of Conversations

1. No matters relating to Inside Information shall be discussed in conversations with persons that are not authorised to access such information or in environments or under conditions where conversations may be heard by unauthorised persons.
2. Conversations in which Inside Information is discussed shall be held in rooms ensuring appropriate acoustic and visual isolation. Such rooms shall be locked from the inside in order to avoid unforeseen disruptions by unauthorised persons.
3. The discussion of Inside Information in telephone conversations shall be avoided to the extent possible. Any telephone conversation in which Inside Information is discussed must be held by using digital or mobile telephones at both ends. It should be borne in mind that voice mail systems can be tampered with. Hence, certain precautions need to be taken when using such systems:
   a) Change the voice mail system default access code.
   b) Never leave voice messages containing or relating to Inside Information.

4. In video-conferences or audio-conferences in which Inside Information is discussed, only the equipment provided by the Company for such purpose shall be used. The provisions of the preceding section 2 shall also apply thereto.

TITLE II. ACTION PROTOCOL IN THE EVENT OF A LEAK OR UNLAWFUL USE OF INSIDE INFORMATION

Article 12. Action Protocol in the Event of a Leak or Unlawful Use of Inside Information

In the event that any Authorised Person detects a possible leak or an instance of unlawful use of Inside Information, action shall be taken as provided below:

a) The reporting party shall, as soon as possible, give notice of the leak or unlawful use of Inside Information of which the party has become aware to the Unit through its chair or, in the absence thereof, through the director or secretary of the Unit. For such purposes, the Unit shall establish safe channels for the reporting of leaks or instances of unlawful use of Inside Information, and shall endeavour to ensure the utmost degree of protection of the identity of the reporting party.

b) The Unit shall analyse and verify the truthfulness of the information provided by the reporting party, for which purpose it may request such additional data and information as it deems necessary from the Finance and Resources Division and from any other Division of the Company.

c) If the reported information is found to be true and if the leak or unlawful use of Inside Information is attributable to a member of the Board of Directors of the Company, the Unit shall give notice thereof to the secretary of the Board of Directors, who shall adopt the appropriate measures in accordance with the Company's Corporate Governance System and the provisions of applicable law.

d) On the other hand, if the leak or unlawful use of Inside Information is attributable to an employee of the Group, the Unit shall give notice thereof to the Finance and Resources Division, which shall adopt disciplinary measures pursuant to the rules on infringements and penalties contemplated in the Collective Bargaining Agreement applicable to the company of the Group to which such employee belongs or otherwise contemplated in applicable labour laws. The Unit shall also give notice to the Company's Legal Affairs Division, which shall evaluate whether any legal actions should be instituted against the employee responsible for the leak or unlawful use of Inside Information under applicable law at any time.

e) Finally, in the event that, once the truthfulness of the reported information has been verified, the leak or unlawful use of Inside Information is found to be attributable to an External Recipient or to any other person or entity unrelated to the Group, the Unit shall give notice thereof to the Company's Legal Affairs Division in order to determine the adoption of any appropriate measures regarding the person or entity responsible for the leak or unlawful use of Inside Information.

f) Without prejudice to the foregoing, when a leak or unlawful use of Inside Information reaches the market, such that news or rumours are generated regarding an item of Inside Information that has not been previously communicated to the CNMV or unusual changes occur in the volumes traded in or the prices negotiated for the Affected Securities, the provisions set forth in the *Action Protocol for the Management of News and Rumours* shall also apply.