Internal Rules for the Processing of Inside Information

C

26 April 2022

These *Internal Rules for the Processing of Inside Information* (the "***Rules***") form part of the Governance and Sustainability System of IBERDROLA, S.A. (the "**Company**") and are approved by the Company's Board of Directors upon a proposal of the Compliance Unit (the "**Unit**"), elaborating upon the *Internal Regulations for Conduct in the Securities Market* (the **"*Internal Regulations for Conduct*"**), Article 5.3 of which provides that security measures shall be established and complied with for the custody, filing, access, reproduction and distribution of Inside Information, as such term is defined in the *Internal Regulations for Conduct*.

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. Notice of Information: a notice sent by the Company to the CNMV for publication and dissemination to the market of Inside Information or other relevant information.

b. Leak: unapproved premature, partial or distorted disclosure to the market of all or part of the Inside Information, regardless of whether or not such information is known by the company to which it pertains.

c. *Guide*: the *Case Processing Guide of Iberdrola, S.A.* approved by the Unit.

d. News: information disseminated by the news media or social media regarding the Company, the Group or Affected Securities that could have an impact on the listing prices thereof.

e. Authorised Persons: means, within the context of a specific operation, transaction, internal process, project, activity or event in which Inside Information is received, generated or accessed, the group of Affected Persons or Insiders that are authorised to access such information.

f. Rumour: speculation without identified author or provenance disseminated to the market regarding the Company, the Group or Affected Securities, that could have an impact on the listing prices thereof, whether or not picked up by the news media.

Article 2. Object

The object of these *Rules* is to establish the rules and procedures for the internal processing and management and the control of the internal and external transmission to third parties outside of the Group of Inside Information, whatever the location, format, 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.

Article 3. Scope

1. These *Rules* apply to the Company and to the other companies within its Group.

2. Listed country subholding companies that have adopted equivalent rules (which may be adapted to the particularities of the legal provisions of the market on which their securities are traded) and subsidiaries thereof shall be excluded from the scope of application of these *Rules*. In any event, said rules must be in accord with the principles set forth in these *Rules* and ensure a level of protection equivalent to that of Inside Information.

Article 4. Dissemination

These *Rules* shall be communicated to and disseminated in accordance with the plan designed by the Unit for such purpose among Affected Persons and Insiders (other than External Advisors), who shall be required to be aware thereof and to comply therewith, as well as within the Finance, Control and Resources and Corporate Security divisions.

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

Affected Persons who have Inside Information, and in all cases Insiders (other than External Advisors), shall be required to be aware of and comply with the regulations and internal procedures established to protect the confidentiality of Inside Information, and particularly these *Rules*.

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

a. comply with the duties established in the *Internal Regulations for Conduct;*

b. 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;

c. limit knowledge thereof strictly to those persons, inside or outside the Group for whom access to the knowledge is essential, with special care taken to ensure that no Treasury Share Manager has access thereto;

d. adopt appropriate measures to prevent the Inside Information from being misused or abused; and

e. 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 Governance and Sustainability 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

1. Persons Responsible for Inside Information must:
   a. Classify as Inside Information the information received or generated in financial or legal operations or transactions, whether in the study or negotiation phase or of which they become aware at any other time or in any other situation, in which case they must cause the issuance of the relevant notice to the CNMV upon the terms and according to the procedure set forth in Article 3 of the *Internal Regulations for Conduct.*
   b. Evaluate whether there are legitimate reasons for delaying dissemination of Inside Information upon the terms of Article 4 of the *Internal Regulations for Conduct*, and if so make said decision or propose that the competent body so resolve for the approval of the operation or transaction in question.
   c. Once a decision has been made to delay the dissemination of Inside Information:
      i. endeavour to ensure that the processing and transmission of said information conforms to the provisions of these *Rules*;
      ii. implement appropriate measures to protect the confidentiality thereof;
      iii. comply with the other provisions of the *Internal Regulations for Conduct* (particularly Articles 3, 4, 5 and 8) and the legal provisions on market abuse that are applicable to the decision made.
   d. Prepare the Communication of Inside Information, when appropriate, pursuant to the *Internal Regulations for Conduct* and in accordance with the provisions of Article 11.
2. Without prejudice to the foregoing, the Unit may at any time request additional information regarding a particular operation, transaction, internal process, project, activity or event and regarding the classification of the information and any decision to delay dissemination thereof.

Article 8. Custody of Inside Information and Access Authorisation

1. The Person Responsible for Inside Information may delegate custody of Inside Information and of Confidential Documents to those persons entrusted with coordination of the work, operation, transaction, internal process, project, activity or event to which the Inside Information refers.
2. The Person Responsible for Inside Information 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, profession or duties.

Article 9. Management of Confidential Documents

In addition to the provisions of the *Internal Regulations for Conduct* and any additional measures that might be established by the Unit regarding the processing and transmission of Confidential Documents, the following guidelines must be observed:

1. Code name: the responsible area shall assign code names to each operation or transaction, internal process, project, activity or event, and the parts thereof, in which Inside Information is evidenced, received or generated. Such names shall be used in all communications relating to the operation or transaction, internal process, project, activity or event, such that neither the parties involved therein nor the characteristics thereof can be identified.
2. Marking or labelling: Confidential Documents must be marked "CONFIDENTIAL" on the cover page, or in the subject line in the case of an e-mail, and must also include the date of issuance thereof. To the extent possible, it is also recommended that "CONFIDENTIAL" be repeated on each page and that reference be made that the use thereof is restricted.
3. Use, access control and filing:
   a. General principle:

      Access to Confidential Documents, regardless of the format, media and storage location thereof, must be restricted to Authorised Persons and shall require the approval of the Person Responsible for Inside Information responsible for the custody thereof.

      They shall be kept in places set aside for such purposes, and designated cabinets or electronic media shall be determined for local filing purposes, which shall be fitted or equipped with special protective measures.

      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 can be gained during the provision of the service.

b. Specific measures for documents in electronic format:

Confidential Documents in electronic format shall have security mechanisms ensuring that only Authorised Persons can access the contents thereof.

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 or similar devices be used to store or transmit Inside Information.

In addition, Authorised Persons shall take the utmost care to prevent unauthorised persons from seeing Confidential Documents on the screen 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 Confidential Information is 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 Confidential Information is stored, the equipment may only be removed with the express authorisation of the Person Responsible for Inside Information. Whenever possible, any Inside Information contained in the memory of the equipment must be deleted prior to the removal (see section 5 below).

c. Specific measures for 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 without supervision, 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 a leak of 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, aeroplanes, 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. Reproduction, distribution and transmission:

a. General rules:

The making of copies of Confidential Documents is prohibited, unless the Person Responsible for Inside Information grants prior express authorisation for the delivery of such copies to an Authorised Person. Recipients of reproductions or copies must be advised of the prohibition against making second copies and using the information for purposes other than those for which it was disclosed to them. 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 Person Responsible for Inside Information.

The area in charge of coordinating the work or transaction to which Inside Information refers shall 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 making 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.

i. Specific measures for documents in electronic format:

If Inside Information is distributed in electronic format, it must be ensured that only Authorised Persons can access the content thereof.

Confidential Documents sent in electronic format must be password-protected or encrypted by any other means. In this regard, a document can be deemed encrypted if the media or location in which it is contained is encrypted.

To the extent possible, all Inside Information sent in e-mails shall be sent as attachments protected in the manner set forth in the preceding paragraph.

Authorised Persons shall attempt to 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.

ii. Specific measures for paper documents:

Printed versions of Confidential Documents should preferably be delivered by hand. If this is not possible, protective measures must be maximised, and the persons in charge of keeping custody of the Confidential Documents shall be responsible for any such distribution. Distribution shall be effected 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 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, Confidential Documents must be stored in places that satisfy the access control and filing requirements described in section 3 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.

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 Advisors must be restricted to those instances in which such transmission is essential in the opinion of the Person Responsible for Inside Information, and it shall particularly comply with the provisions of this section:

i. Inside Information shall be transmitted to External Advisors as late as possible given the nature of the operation or transaction in question.

ii. Prior to the transmission of any Inside Information, the External Advisors must sign a confidentiality undertaking with the Company in which they state that they are aware of or agree to: the confidential nature of the information transmitted; the obligations stemming from the legal provisions applicable to the Inside Information; the consequences of violating such legal provisions; and that they have the means required to ensure the confidential nature of the Inside Information. The foregoing shall not apply if the External Adviser is subject to a duty of secrecy under their professional rules. They shall also be informed of their obligation to create and keep up-to-date their own list of insiders in accordance with the provisions of the MAR, which shall include the persons of their organisation who have access to Inside Information. They shall also be required to state that they are aware of all of the foregoing.

The signing of such confidentiality undertaking shall also be required of those External Advisors (unless they are subject to a duty of secrecy under their professional rules) with whom contact is made at a preliminary phase and to whom the general outline of an operation or transaction is presented in order to request financing offers or advice, even if they do not ultimately participate in such transaction.

iii. In the event that Inside Information is transmitted to one or more External Advisors belonging to the same firm or entity, the confidentiality undertaking required in the preceding paragraph 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 this case, the prior express authorisation of the Person Responsible for Inside Information 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 instance contemplated in the preceding paragraph, the internal processing of the Inside Information shall be subject to the provisions established for such purpose by the organisations to which the External Advisors belong.

iv. The content and implications of the confidentiality undertaking must be explained orally in a clear and concise manner in the case of External Advisors that may not be acquainted with the applicable legal provisions.

v. In any case, the transmission of Inside Information by one External Adviser to another External Advisor within a different firm or entity shall require the prior express authorisation of the Person Responsible for Inside Information and that such other External Adviser has itself signed a confidentiality undertaking equivalent to the one described in paragraph (ii) above, either with the Group or with the other External Adviser (unless it is subject to a duty of secrecy under its professional rules).

vi. The Unit or the Person Responsible for Inside Information may subject a transfer in electronic format of Inside Information to the External Advisors to encryption or protection of the Confidential Documents through any computerised procedure that restricts access to the Inside Information.

5. Disposal:

   Authorised Persons who have had access to Inside Information must destroy any media containing copies of such information at the time they cease to be useful, unless there is a legal or business requirement that justifies the retention thereof. Specifically, there shall be maintained and there will be no obligation to destroy the original or master documents containing the Inside Information for at least the legal or internally established period.

   Any disposal required pursuant to the provisions of this article must be handled in such a way as to ensure the complete destruction of the 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 is removed or discontinued from use or the internal memory or any other data storage device (which contains or contained Inside Information) 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. Agents from outside the Company who provide these services professionally (for instance, specialised companies in the case of the destruction of large volumes of documentation) can participate in the documentation destruction process provided that the service contracts that are signed with them include clauses protecting the confidentiality of the Inside Information to which such external agents may have 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 10. 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. Face-to-face 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. Any telephone conversation in which Inside Information is discussed must be held by using digital or mobile telephones at both ends, which in no event shall have the speakerphone activated.
4. 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; and
   b. never leave voice messages containing or relating to Inside Information.
5. In video-conferences or audio-conferences in which Inside Information is discussed, only the equipment provided for such purpose by the Company or a company of the Group or by trustworthy External Advisors shall be used and protective measures intended to avoid intrusion by unauthorised persons shall be established.

Article 11. Preparation of the Notification of Inside Information

When it is appropriate to submit a Notification of Inside Information to the CNMV in accordance with the *Internal Regulations for Conduct*, the Person Responsible for Inside Information must prepare the draft of the Disclosure of Inside Information (II) and its corresponding translation into English, and must ensure the due preservation of the support for the information to be disclosed.

These drafts shall be sent immediately to the Office of the Secretary of the Board of Directors to validate the text thereof and to arrange for publication in accordance with Articles 3 and 4 of the *Internal Regulations for Conduct*.

The text of the Notification of Inside Information must comply with the provisions of Article 3 of the *Internal Regulations for Conduct*.

In addition, if the Notification of Inside Information refers to an operation, transaction or project that is quantified in foreign currency, the disclosure must contain the approximate equivalent thereof in euros, based on the most recent euro exchange rate published by the European Central Bank.

Article 12. Dissemination of the Notification of Inside Information

Disclosures of Inside Information (II) must be reported to the CNMV by the secretary of the Board of Directors or, in the absence thereof, by one of the deputy secretaries of the Board of Directors, through the use of the CIFRADOC/CNMV system or of any other means that the CNMV provides for such purpose.

Notifications of Inside Information (II), once submitted to the CNMV, shall be published on the corporate website (Shareholders and Investors - Notifications Sent to the CNMV -Inside Information).

Information contained in the Notification of Inside Information (II) may not be disseminated by any other means without prior publication thereof on the website of the CNMV. Furthermore, the content of the Inside Information disclosed to the market by any information or communication channel other than the CNMV must be consistent with that corresponding to the Notification of Inside Information (II).

TITLE II. LEAK OR UNLAWFUL USE OF INSIDE INFORMATION

Article 13. Action Protocol in the Event of Detection of a Leak or Unlawful Use of Inside Information

In the event that any person subject to the *Internal Regulations for Conduct* and/or to these *Rules* detects a possible Leak or an instance of unlawful use of Inside Information, action shall be taken as provided below:

a. The person 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 of Compliance or the secretary of the Unit[1].

   After receiving this notice, or if the Unit in any other way becomes aware of the possibility that a Leak or unlawful use of Inside Information has occurred, the Unit shall follow the procedure set out in the *Guide*, with the particular indications set out in this Article 13.

b. The Unit may request such additional data and information from the Finance, Control and Corporate Development Division of the Company as it deems necessary in relation to the procedure set out in the *Guide*. If there is a suspicion that the Leak or unlawful use of Inside Information comes from or has been made by External Advisors or by any other person or entity unrelated to the Group, the provisions of paragraph f) below shall apply.

c. Upon granting the corresponding investigation file leave to proceed, the Unit, after consulting with the Legal Services Division and, if appropriate, with the secretary (or in the absence thereof, with any of the deputy secretaries) of the Board of Directors, shall inform the CNMV of the opening of the investigation when legally required as well as if it so believes appropriate even if not required, provided that this does not include personal information of the person being investigated that allows for the identification thereof.

d. In addition to the provisions of the *Guide*, the Unit may ask the person under investigation:

   i. to provide the Company with any receipts for the transactions under investigation, as well as all information in the possession thereof relating to said transactions; and

   ii. to expressly consent in writing for the Company to contact the financial intermediaries with which the transactions under investigation may have been performed or other third parties when appropriate.

   If the person under investigation states that he or she is willing to give the consent referred to in paragraph (ii) above, he or she will be asked to send a communication to each of the third parties that the Company intends to contact within the scope of the investigation, authorising them to provide the Company with the information required for the purposes indicated. The communication shall contain the provisions on personal data protection required by applicable law.

   Alternatively, if the financial intermediary or third party from whom the person under investigation has requested the information demands security or indemnification from the Company for damages that may occur due to disclosure of the information requested that the Unit does not believe appropriate to provide, or if for any other reason it is not considered appropriate to obtain the information directly from third parties, the person under investigation shall be asked to personally request the relevant information from the financial intermediary or third party in question for such information to be sent to the Company in a sealed envelope to be subsequently opened in the presence of the person under investigation.

e. The Unit, after consulting with the Legal Services Division and, if appropriate, with the secretary (or in the absence thereof, with any of the deputy secretaries) of the Board of Directors, shall notify the CNMV of the disposition of the investigation when legally required, and may do so if it so believes appropriate even if not required, provided that this does not include personal information of the person being investigated that allows for the identification thereof.

f. Once the procedure set out in the Guide is completed, if it is verified that the Leak or unlawful use of Inside Information is attributable to an External Adviser or to any other person or entity unrelated to the Group, the Unit shall give notice thereof to the Legal Services 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.

TITLE III. MANAGEMENT OF NEWS AND RUMOURS

Article 14. Ongoing Monitoring and Tracking of News and Rumours and of the Listing Price and Trading Volumes of Affected Securities

1. It is the responsibility of the Company's Finance, Control and Corporate Development Division to perform ongoing monitoring and tracking of the market performance of listing prices and trading volumes of Affected Securities, Rumours that may be disseminated to the market, and News of which the Company should reasonably be aware.

   To such end, the Finance, Control and Corporate Development Division shall establish the required coordination mechanisms with the Global Communications Division in order to have permanent access to such News.

2. The Finance, Control and Corporate Development Division shall report to the Unit, whenever requested thereby, regarding its ongoing monitoring and tracking of the market performance of listing prices and trading volumes of Affected Securities and of the Rumours and News disseminated to the market.

1 See Article 16.

Article 15. Action Protocol in the Event of Becoming Aware of News or Rumours

1. In the event that the Finance, Control and Corporate Development Division becomes aware of the existence of News or a Rumour relating to information not previously provided by the Company to the CNMV by means of the corresponding Notice of Information, the Finance, Control and Corporate Development Division shall analyse the significance of the disseminated information in accordance with the standards it deems appropriate in each case.

   To such end, the Finance, Control and Corporate Development Division shall, without limitation, take into account the impact that the actual materialisation of the content of the News or Rumour could have on the accounting or financial indicators of the Company or its Group and on the listing price of the Affected Securities, and changes in the listing price of the Affected Securities as a result of the News or Rumour.

   In particular, in those cases in which the News or Rumour is disseminated during a trading session, special attention shall be paid to changes in the traded volumes and the listing prices of the Affected Securities in order to assess the significance of the disseminated information.

   In addition, the Finance, Control and Corporate Development Division shall analyse the truthfulness of the News or Rumour, for which purpose it will carry out, in coordination with the Unit, all internal investigation and consultation activities that it deems appropriate for such purpose.

2. Following the required reviews of significance and truthfulness, the Finance, Control and Corporate Development Division shall proceed as follows:

   a. If it determines that the information disseminated to the market is significant and truthful, the Finance, Control and Corporate Development Division shall contact the secretary of the Board of Directors, or any of the deputy secretaries of the Board of Directors in the absence thereof, in order to evaluate the advisability of publishing a Notice of Information in order to clearly and precisely report the facts to which the disseminated News or Rumour refers.

   b. Whenever it deems the information disseminated to the market to be significant but lacking sufficient elements to determine the truthfulness thereof (for instance, because it is information stated by, or relating to, third parties not related to the Company and beyond its control), the Finance, Control and Corporate Development Division shall consider the possibility of asking the CNMV to take the necessary actions to verify and investigate the News or Rumour in order that the CNMV itself, or the appropriate person, may publicly express a clear, full and precise opinion regarding the News or Rumour.

   c. If it determines that the information disseminated to the market is insignificant or untrue, the Finance, Control and Corporate Development Division may encourage the adoption of the necessary measures to deny any untrue News and Rumours that could harm the interests of shareholders and investors.

3. The Finance, Control and Corporate Development Division shall report to the Unit on the result of the analysis of the News or Rumours, along with any measures that may have been adopted pursuant to this Article 15, in order for the Unit to be able to evaluate the advisability of taking any additional actions.

4. Without prejudice to the provisions of this Article 15, the Board of Directors may take any actions it deems appropriate to protect the corporate interest against the dissemination of Rumours that could affect the normal business operations of the Company or the Group or the listing price of the Affected Securities.

Article 16. Action Protocol in the Event of Unusual Changes in the Listing Price or the Traded Volume of Affected Securities.

1. In the event that the Finance, Control and Corporate Development Division notices unusual changes in the listing prices or traded volumes of Affected Securities, it may ask the Unit if a Register of Insiders has been opened, and if so after contacting the Person Responsible for Inside Information in order for them to report the status of the pending operation or transaction, internal process, project, activity or event, it will as soon as possible report to the chair of the Unit or, in the absence thereof, to the director or the secretary of the Unit, if it has noticed any extraordinary or irregular situation or a situation that may derive from conduct that might entail a violation of the *Internal Regulations for Conduct*, the MAR or any other legal provision governing the securities markets.

2. The Finance, Control and Corporate Development Division shall analyse whether there are rational indications that such changes are the consequence of a Leak, and shall report its conclusions to the Unit, which shall act as follows:

   a. If it establishes or suspects that there are indications of a Leak, the Unit shall take the relevant actions and measures pursuant to the provisions of these *Rules*.

   b. If it does not establish that there are indications of a Leak, the Unit may implement any initiatives it deems appropriate in light of the possible causes of the unusual changes in the listing price or the traded volumes of the Affected Securities.