INTERNAL INFORMATION SYSTEM
PROTECTION OF INFORMANTS AND RELATED INDIVIDUALS

Policy Owner:	Dominic Crabb
Policy Author(s):	Carmen Artigas, Lucy Duncan
Application:	All staff, directors and third parties
Version:	V1
Effective From:	December 2023
Approved by:	The Board of Directors on 23 November 2023

CONTENTS

01 PURPOSE

The Internal Information System (hereinafter referred to as 'IIS') aims to protect the individuals who would file internal communications of breaches and to protect other individuals cooperating during the process or affected by the communication, from suffering any reprisals or negative consequences and to embed a culture of transparency and communication with LONDON AND CAPITAL WEALTH MANGEMENT EUROPE, A.V. S.A. (hereinafter, referred to as 'LCE') which is part of the LONDON AND CAPITAL GROUP LIMITED's group of companies (L&C).

LCE Board of Directors is responsible for approving the IIS policy and procedure according to Art. 5.2 h) of the Law 2/2023, of 20th February to set up its principles.

02 SCOPE

This policy is applicable to any informant working at LCE. In addition, is applicable to any third party interacting with LCE (services providers, creditors, contractors, etc.) including the employees of those third parties. All the above mentioned shall be referred to as 'Informants'.

The above mentioned individuals when acting as Informants may communicate any breaches of any applicable law.

The L&C Whistleblowing Policy and Procedure includes a complete list of all the individuals who could act as Informants and details what breaches or wrongdoings should be reported.

03 INTERNAL INFORMATION SYSTEM'S PRINCIPLES

L&C shall ensure that the IIS is effective for the purpose of facilitating the internal communication of infractions according to the applicable regulation, and therefore, it is implemented complying with the following principles:

- Accessibility: allowing all the relevant individuals to communicate breaches, including third parties, both verbally and in writing.
- Security and confidentiality of the information related to both the informant and other involved parties, even third parties and of the actions in connection with the communication.
- Gathering all the communication channels to ensure that all are governed by the same principles.
- Independent from other entities' channels.
- Protection of the Informants and related individuals who may be affected by reprisals.

04 RESPONSIBILITY FOR THE INTERNAL INFORMATION SYSTEM

LCE shall appoint an individual responsible for the IIS who shall perform its functions independently and with autonomy from other governing bodies, would not receive any instructions and shall have adequate human and material resources to implement its obligations. The Board of Directors is responsible for the appointment. LCE Board of Directors has appointed the Whistleblowing Champion as responsible for the IIS.

London and Capital Wealth Management Europe A.V., S.A. registered with the Commercial Registry of Barcelona at Volume 48048, Sheet 215, Page B-570650 and with Tax Identification Number (NIF) A16860488, authorised and supervised by the Comisión Nacional del Mercado de Valores (“CNMV”), and registered at CNMV’s register under number 307.

LCE must communicate the appointment to the Informant Protection Independent Authority within the term of ten (10) days https://www.antifrau.cat/sites/default/files/Documents/Quefem/formulario-comunicacion-registro-responsable-sistema-interno-informacion.pdf (AAI according to Spanish initials) or to the relevant regional authority at any time in Catalonia.

05 INTERNAL AND EXTERNAL COMMUNICATION CHANNELS

LCE Compliance Manual has in place the required channels to allow the Informants to file any communications of infractions complying with all the applicable regulatory requirements. In addition, LCE provides a form to be fulfilled by the Informants and that includes all the information that would be convenient to complete the investigation, nevertheless, completing the form is not compulsory to complete such form if the Informants feel more comfortable raising their concerns orally (in which case it will be either recorded with the previous consent of the Informant or transcribed).

Besides, Informants have the option to report their communications through external channel. For LCE, the competent authority is up to be enacted a Catalonian law for protection of the informants, to the Catalonia's Antifraud Office which is the Informant Protection Independent Authority (AAI according to Spanish initials).

The full information about both the internal and external channels and the form are disclosed withinthe Whistleblowing Channel Policy & Procedure.

06 INTERNAL INFORMATION SYSTEM's PROCEDURE

The IIS procedure shall comply with the following principles:

- LCE makes available to Informants the required internal channels enabling them to file any concerns orally, in writing, keeping them as confidential and anonymously, if applicable.

- The Informants may as well file their concern with the relevant external competent authority, for LCE the Catalonia's Antifraud Office.

- The maximum period to complete and conclude the investigation would be three (3) months from the date of receipt of the investigation or, if the acknowledgement of receipt was not sent to the Informant, three (3) months as from the date after seven (7) days from the date of the communication. Nevertheless, for complex cases it may be extended for three (3) additional months.

- It will exist the possibility to keep the contact with the Informant, asking for additional information if required.
- The affected individual would have the right to be informed about the communication and to defend itself, as required and considered adequate for the investigation.

- It will be guaranteed that even those communications received by different channels will be kept as confidential, training as necessary the personnel and warning of the very serious breach of the Spanish Law 2/2023 if the confidentiality is not kept and the consequences.

- It will be ensured the benefit from the presumption of innocence and honour of the affected individuals.

- The protection of personal data will be guaranteed according to the Whistleblowing Channel Policy & Procedure.

- In the event of communications that would present indications of criminal offenses, the information would be immediately reported to the General Office Attorney and to the EU General Attorney Office if they affect to the financial interests of the EU.

The IIS channels, internal channel procedure and all the rights and obligations of the Informants and of the individuals affected by the communication are detailed in the Whistleblowing Channel Policy & Procedure. For any additional information please contact the Compliance team.

07 COMMUNICATION PROCESS

Once the communication has been received through the internal channel the Informant shall receive an acknowledgement of receipt within seven (7) days.

The Whistleblowing Officer (or the Whistleblowing Champion or Stephen Murphy, if applicable) shall receive the communication and perform an initial analysis. After this initial analysis it would be confirmed if the communication is admitted or not (when: (i) it is not realistic, (ii) it does not represent a breach, (iii) there is not enough information, or it relates to a previous communication and (iv) does not provide new information). If it is not admitted the Informant will be informed within the term of five (5) days.

If the communication is admitted, it will be performed a complete investigation to confirm its authenticity. It may be requested the assistance of other departments to assist in the investigation provided that they act independently, being all the information subject to strict confidentiality.

As part of the investigation, LCE will arrange a meeting with the Informant as soon as possible to discuss their concerns, unless that it would have been communicated anonymously. They may bring a colleague, trade union representative or an official employed by a trade union to any meetings under this policy. This companion must respect the confidentiality of the disclosure and any subsequent investigation.

The facts communicated shall always be investigated in a manner that would not jeopardise the confidentiality of the Informant's identity, clarifying and/or corroborating what happened without disclosing information that could disclose who is the Informant.

Finally, the investigation shall be concluded, and the parties would be informed of the outcome of the investigation, being taken the necessary measures, disciplinary, if applicable
The communication shall be recorded at the communications log. Besides, the analysis and conclusion shall be properly documented.

The maximum period to complete the investigation would be three (3) months. However, in the event of cases of special complexity the period could be extended by three (3) additional months.

08 DATA PROTECTION

Overall, it is applicable GDPR, Title VI of Personal Data Protection of the Spanish Law 2/2023 and Organic Law 3/2018, of 5th December, of Data Protection and guarantee of digital rights apply, regulating the protection of the individuals reporting regulatory breaches' personal data.

When the information would be received directly from the interested individuals, they will be informed about their rights in connection with the protection of their data according to article 13 of EU GDPR. The informants additionally will be informed of their right to keep their information confidential, in no event the affected Individuals would be informed about the identity of the informants.

The access to the data within the Internal Information System would be limited as stated by the applicable regulation expressly to those individuals to which the concerns is reported, those involved in the investigation and the application of sanctions, and similar disciplinary measures. The informant's identity would not be revealed to third parties. The Internal Information System would feature with the required technical and organisational measures to ensure that the informants' identity remains confidential.

The identity of the informant could exclusively be disclosed to the judicial authority, the General Attorney's Office, or the relevant competent authority within the framework of a criminal, disciplinary investigation or an investigation that would entail a sanction or other penalties.

The access to the data for the investigation shall be restricted and kept for a maximum period of three (3) months except for especially complex cases for which it may be extended for another three (3) months in which case the total period shall be of maximum six (6) months.

CONTROL / DOCUMENT MAINTENANCE

Created	October 2023
Next Review	November 2024
Reviewed by	Carmen Artigas
Questions / Queries to	Compliance Team