APPENDIX D: MANAGEMENT OF COMMUNICATIONS RECEIVED THROUGH THE ETHICS CHANNEL

This Appendix D is based on the Elecnor Group's Internal Reporting System Procedure on Integrity and Regulatory Compliance, adapted to Deimos, the purpose of which is to develop the system for managing the communications received through the Deimos Ethics Channel.

The main relevant aspects regarding the management implemented for communications received through the Deimos Ethics Channel, with the corresponding adaptations, are set out below:

1. Functions

The **Management Body** of Deimos is responsible for the implementation of the internal Integrity and Regulatory Compliance Information System and its adaptations based on the Elecnor Group's Policy and Procedure for the Internal Integrity and Regulatory Compliance Information System, and **Deimos Management** is responsible for its effective implementation and the monitoring and supervision of its proper operation at Deimos.

The person in charge of D**eimos' internal Integrity and Regulatory Compliance Information System** (hereinafter, the System Manager) is responsible for the diligent management of the System, in accordance with the provisions of this Appendix. The appointment, dismissal or removal of the Deimos System Officer is the responsibility of the Board of Directors, which shall ensure, through the Deimos Management, that he/she has the necessary resources and the due independence and autonomy to ensure the correct operation of the System and the proper management and processing of the files that may be initiated as a result of the communications received.

The person in charge of the Deimos System may rely on the persons determined in each case to duly attend to his or her responsibilities, always guaranteeing due confidentiality and protection of the personal data included in the communications received through the System.

2. Receipt, registration of communications and analysis and decision on their admissibility

2.1. Communications received through the Ethics Channel of Deimos:

Upon receipt of a communication through the Ethics Channel, Deimos System Manager, with the support, where appropriate, of such persons as it may deem appropriate, shall carry out the following activities:

- Review the content of the communication and determine whether the communication concerns potential misconduct. If the communication is intended to raise concerns or improvements to existing internal control systems or relates to issues not related to integrity or compliance, the System Officer shall respond or consider them as appropriate and they shall not be recorded in the "Ethics Channel Communications Register".
- Where the System Officer determines that the communication does relate to potential misconduct, the System Officer shall record the communication in the "**Register of Ethics Channel Communications**".
- Shall be send, through the same reception channel, the **acknowledgement of receipt** of the communication to the person who made the communication within a maximum period of **seven calendar days** from its receipt.

2.2. The Register of Ethics Channel Communications

The Register of Ethics Channel Communications (hereinafter, the **Register of Communications**) is the file in which the System Manager shall **record all communications received** through the Ethics Channel.

The Register of Communications shall be managed exclusively by the System Manager, who shall guarantee the due **confidentiality** of the information included therein, especially with regard to the identity of the persons who have made the communications (hereinafter, informants) and of those to whom the communicated facts refer (hereinafter, affected persons) as well as to the facts described

therein. Access thereto shall be restricted to authorised persons and the personal data included therein shall only be kept for the period deemed necessary and proportionate for the purposes of being able to accredit the conclusions reached following the investigations that may have been carried out, guarantee the protection of the informants for the time deemed necessary or leave evidence of the correct functioning of the System.

The Register of Communications shall include the following information in respect of each communication:

- Communication identification code (C_BB_XYZ, where "C" stands for "Communication"; "BB" for the last two digits of the year; and "XYZ" for the sequential number of the communication in the current year).
- Date of receipt of the communication.
- Internal channel through which the report was received.
- Identification of the reporter (if applicable).
- Identification of the person(s) affected.
- Brief description of the facts that are the subject of the communication.
- Result/conclusion of the preliminary analysis/assessment ("Admitted"/"Redirected" to other department/s /"Rejected").
- Status ("Open"/"Closed").
- Date of closure of the file/investigation.
- Outcome/conclusion after investigation.
- Actions taken, conclusions reached, measures adopted and other observations.
- Resolution period (from the date of receipt of the communication to the date of closure of the file/investigation).

2.3. Analysis and decision on the admissibility of communications

Deimos System Manager, with the support of such persons as it may deem appropriate, once the communication has been received and registered, where appropriate, shall carry out an initial analysis or assessment of the communication in order to determine whether it should be admitted:

- Admitted, in which case the corresponding investigation process will be initiated.
- Redirected to other department(s), when it is considered, in view of the nature of the facts reported and other particular circumstances, that their investigation and decision on the possible measures to be adopted do not fall within the scope of the System, without prejudice to the due monitoring of this process by the person responsible for the same. In this process, the due confidentiality and protection of the personal data included in the communications shall be respected.
- Rejected, when it is considered, based on the nature of the facts reported or their lack of plausibility, that it is not appropriate to initiate an investigation process.

When the communication presents indications that may make its admission or redirection to other departments for handling feasible, but its content is insufficient, incomplete or does not provide the necessary detail to be able to complete this preliminary analysis or assessment, the System Officer may request the informant to provide additional information deemed relevant.

The result of this analysis or assessment shall be recorded in the Register of Communications.

When, after this initial analysis or assessment, the System Manager determines that the whistle-blower is entitled to due protection against reprisals simply because of his or her status as such, he or she shall assess the advisability of informing the organisation's Human Resources Manager and the members of management identified of this fact so that the appropriate measures may be adopted to prevent and avoid possible reprisals, guaranteeing maximum confidentiality in all cases.

Likewise, the System Manager shall assess the advisability of informing the heads of the areas or departments it considers appropriate of the possibility of adopting certain measures as a matter of urgency in order to prevent and avoid the continuation or repetition of the events reported during the period of the investigation process. Likewise, maximum confidentiality shall be guaranteed in this process.

2.4. Receipt of communications through other internal communication channels

When the communication is received through any internal communication channel, whether formal or informal, other than the Ethics Channel of Deimos, the person who received the communication shall immediately **contact the System Manager** to determine how to proceed.

When, in view of the nature of the reported facts, the System Officer determines that the report should be handled in accordance with this Appendix, it shall inform the person who first received the report to

report it through the Ethics Channel. Likewise, the System Manager shall inform such person of the obligations and commitments regarding confidentiality, protection of personal data and guarantee of the rights of the informant and of the persons affected that must be respected both during the processing of the file and after its closure, if applicable.

From that moment onwards, these communications shall be managed in accordance with the provisions of this Appendix.

3. Investigation

When the communication has been admitted, the System Manager shall initiate the **investigation process**, which shall include all those actions aimed at verifying the veracity of the facts communicated.

3.1. Investigation team

The investigation may be carried out by the System Manager himself or by such persons as he may determine, taking into account the nature of the facts reported and the profile of both the informant and the persons affected, so that the investigating team may carry out its actions with due independence and absence of any conflict of interest, with sufficient authority and with the best capabilities to ensure the proper completion of the process. Likewise, the investigating team shall guarantee the utmost confidentiality regarding the content of the communication and, in particular, the identity of the informant and the persons affected.

3.2. Investigation process

There is no fixed pattern for the development of the investigation, as it will be conditioned by the nature of the facts reported and by the specific circumstances accompanying the process. The investigation process will therefore be defined in each case by virtue of these particular circumstances.

In any case, the research team will take into consideration and develop the following **actions**:

- Assess the need and/or advisability of maintaining communication with the informant during the investigation process for the purpose of requesting additional information or evidence from the informant in relation to the facts reported.
- It may request the documentation and information it deems necessary from other divisions, areas or departments of the organisation and hold the appropriate interviews with the persons it determines for the purpose of verifying the veracity of the facts reported.
- The right of the persons affected to be informed of the facts attributed to them and to have the opportunity to be heard and to exercise their right to defence shall be duly attended to. In no case shall the persons affected be provided with the identity of the informant or with access to the communication received. Such communication with the persons affected shall take place, where appropriate, at such time and in such manner as is considered adequate to ensure the proper conduct of the investigation.

The investigation process shall be carried out with the utmost **confidentiality** of the facts investigated and the identity of the informant and the persons affected.

All Deimos Group employees shall **cooperate fully** with the investigative team throughout the investigation process.

3.3. Investigation report and conclusions

Once the investigation has been completed, the investigative team shall prepare an **Investigation Report**, which shall be submitted to the System Manager for review, discussion and approval. This report will contain at least the following information:

- Identification code of the communication in the Register of Communications and date of registration.
- A statement of the facts reported.
- The actions carried out in order to verify the veracity of the facts reported.
- The conclusions reached.

By virtue of the result of the investigation and the conclusions reached, the System Manager shall inform the heads of the areas or departments that it deems appropriate of the possibility of adopting certain measures as a matter of urgency in order to prevent and avoid the continuation or repetition of the verified events, guaranteeing in all cases the utmost confidentiality.

Deimos System Manager shall inform Deimos Management of the outcome and conclusions of the investigation, which shall in turn be forwarded by the latter to the Governance Body whenever it deems appropriate. Likewise, by virtue of the nature of the facts investigated and of this result, and whenever deemed necessary for the proper completion of the process, the System Manager shall inform the areas and departments it deems appropriate of its conclusions, safeguarding the due confidentiality of all information relating to the file and the protection of personal data.

When the investigation or actions carried out for the purpose of understanding and verifying the veracity of the facts reported have not required special verifications or enquiries, the investigating team, at the request of the System Manager, may be exempted from drawing up the corresponding Investigation Report under the terms established in this section. In any case, the System Manager shall duly record the actions carried out and the conclusions reached in the Communications Register.

3.4. Term

The maximum time limit for completing the investigation process shall be **three (3) months** from the receipt of the communication, except in cases where the investigation is particularly complex or difficult or where other situations justify an extension of the time limit, in which case the time limit may be extended by up to a maximum of three additional months.

4. Resolution, closure of the file and adoption of disciplinary or contractual measures

Deimos System Manager is responsible for resolving and closing the file, informing in a timely manner to the Deimos Management and the **competent internal instance, body or function** in each case for the establishment and adoption of the **decisions and disciplinary measures** (in the labour sphere) **or contractual measures** (in commercial relations with third parties) deemed appropriate by virtue of his knowledge of the facts reported and investigated and, in particular, based on the conclusions set out in the Investigation Report duly approved by the System Manager.

The disciplinary measures adopted shall not only apply to the persons who have committed the irregularity, but also to those who have not followed the procedures established by Deimos Group for its prevention and due response, a circumstance that is in itself considered a breach of the ethical values and principles to which Deimos Group is committed.

Disciplinary measures of a labour nature must be respectful of the applicable regulations, without losing forcefulness or proportionality with the seriousness of the facts that give rise to them, informing, where appropriate, the Legal Representatives of the Employees.

The information relating to the decisions and disciplinary measures adopted, if any, shall be included in the file, thus proceeding to its final closure and conclusion.

On the other hand, and in the event that after the process of analysis and investigation of the communication and the facts reported, it is determined that the same has been made in **bad faith**, Deimos Group shall assess the possibility of adopting the **appropriate disciplinary measures** against the corresponding informants. For these purposes, and as established in *the Internal Information System on Integrity and Compliance of Deimos Group*, a communication in bad faith shall be understood to be one that is not based on facts or evidence from which irregular conduct may reasonably be inferred, one made even when the informant is aware of the falsity of the facts and/or fraudulently exaggerates or misrepresents them, or one made for the sole purpose of revenge, harassment or defamation or to seek personal or professional harm to the persons affected.

5. Measures for the protection of the informant and the persons affected

5.1. Whistleblower protection

As established in the Section III of this Guideline, the Deimos Group does **not tolerate retaliation**, including threats or attempts at retaliation, against persons who report in **good faith** through the internal channels provided for this purpose any irregular conduct or conduct contrary to the principles and values of Deimos Group or to the legislation in force (whistleblowers). Deimos System Manager, with the support of the persons determined in each case, shall make every effort to ensure that whistleblowers are duly protected against reprisals.

For the purposes of this Procedure, retaliation is understood to be any **acts or omissions that harm the whistleblower** or that, directly or indirectly, involve unfavourable treatment that places the persons who suffer them at a particular disadvantage with respect to another in the employment or professional context, solely because of their status as a whistleblower.

Protection against any kind of retaliation shall also extend to natural persons assisting the whistleblower in the process, to natural persons who are related to the whistleblower and who may suffer retaliation, such as co-workers or family members, to legal persons for whom the whistleblower works or with whom it has any other relationship in an employment context or in which it has a significant shareholding, and to legal representatives of employees in the exercise of their functions of advising and supporting the whistleblower.

When Deimos System Manager determines that a whistleblower is entitled to due protection against retaliation simply because of his or her status as a whistleblower, he or she shall inform the Human Resources Manager of the organisation and the members of management identified for the purpose of adopting the appropriate measures to prevent and avoid possible retaliation, guaranteeing in all cases the utmost confidentiality.

5.2. Protection of the persons affected

The persons affected by the communications (the persons to whom the communications refer) shall have the right, during the processing of any proceedings initiated as a result thereof, to the **presumption of innocence and the right to honour, defence** and **access to the file** under the terms established in chapter 5 above, as well as to the same protection established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the proceedings.

The right to honour shall be preserved beyond the end of the investigation process.

6. Management and preservation of information and documentation and protection of personal data

Deimos System Manager shall be responsible for the **appropriate filing and safekeeping of all documentation** relating to the communications received and generated during the investigation process, including the corresponding investigation reports. The management of this documentation shall be carried out guaranteeing **maximum confidentiality** and **due protection of the corresponding personal data** and shall only **be kept for the period** considered **necessary and proportionate** for the purposes of being able to accredit the conclusions reached after the investigations that may have been carried out, guarantee the protection of informants for the time considered necessary or leave evidence of the correct functioning of the system. This period shall never exceed **ten (10) years**.

Without prejudice to this responsibility, all persons who have participated in the investigation process or who have had access to certain information related to the communications received shall **contribute to ensuring the utmost confidentiality** with regard to the same.

The **personal data** obtained as a result of the communications received and the investigation processes that may arise from them will be treated with the **strictest confidentiality**, only by **authorised personnel** and for the sole purpose of investigating the facts reported in order to verify their veracity, duly address any doubts in the area of integrity and regulatory compliance or proposals for improvement in the existing internal control systems and keep the pertinent Register of Communications duly updated. This register will not be public and only upon a reasoned request from the competent judicial authority will it be possible to access all or part of its contents.

The **legitimate basis** for the processing of this personal data lies **in compliance with the legal obligations** of Deimos Group deriving from the application of the relevant regulations and, in particular, Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, which also covers their possible communication in a confidential manner and with the appropriate security measures to other areas or departments of the organisation and to the different companies of the Group for the proper completion of the investigation process and for the due adoption, where appropriate, of the disciplinary, contractual or legal measures that may be determined in each case.

Likewise, the personal data recorded in the System may be communicated to the administrative or judicial authorities, when so requested, as a consequence of any procedure arising from the object of the communication made, as well as to the persons involved in judicial or administrative proceedings initiated as a consequence of the investigation.

In no case shall personal data that are not necessary for the knowledge and investigation of the reported facts be collected or processed and, should they be obtained accidentally, they shall be immediately deleted.

The informant or the persons affected may exercise, where appropriate, the rights of access, opposition, rectification, deletion, limitation of processing, portability and the right not to be subject to automated individual decisions by writing to the e-mail address gdpr@deimosgroup.net, through which they may contact the Data Protection Manager of Deimos Group.

7. Monitoring and supervision, development and review

Deimos Management is responsible for **monitoring and supervising** the effective application of the Procedure and the Policy it develops, and the Management Body is responsible for the implementation of the Procedure and the aforementioned Policy. The **diligent management** of the internal information system in matters of Integrity and Regulatory Compliance is the responsibility of the **System Manager of Deimos**, appointed by the Board of Directors, who shall carry out his or her functions independently and autonomously, with the personal and material resources necessary to do so.

Deimos System Manager, within the framework of his or her functions and without prejudice to the powers of monitoring and supervision of the Procedure and the Policy it develops, which correspond to **Deimos Management**, may develop and approve the rules for the development of this Appendix D that he or she deems necessary to ensure the correct operation of the System.

Deimos Management, in accordance with its function of monitoring and supervising the Procedure, shall update the Procedure whenever it deems it appropriate and shall submit the corresponding proposal to the Board of Directors.

Deimos Management shall report periodically (in principle, annually) to the Governing Body on the result of the exercise of its function of monitoring and supervising the effective operation of the System.