



POLICY OF USE AND OPERATION OF THE INTERNAL INFORMATION CHANNEL SOUTH SUMMIT

PREPARED BY		
Grupo Adaptalia	Consultant and external advisor	July 2023
REVISADO POR		
Compliance Committee		July 2023
APROBADO POR		
Sole Administrator		July 2023
VERSIÓN		
		V. 01

INDEX

1.	DEFINITIONS.....	
2.	INTRODUCTION.....	
3.	SCOPE OF APLICATION.....	
4.	MEDIA.....	
5.	CONTENTS AND IDENTIFICATION DATA OF COMMUNICATIONS.....	
6.	CONFIDENTIALITY.....	
7.	DATA PROTECTION.....	
8.	PROTECTION OF THE CALLER.....	
9.	PROCESSING AND MANAGEMENT OF COMMUNICATIONS.....	
1.	Reception, classification and management of communications.....	9
2.	Investigation of the file.....	10
3.	Precautionary measures.....	11
4.	Communication to the investigated subject and hearing/defense process.....	11
5.	Final Report.....	12
6.	Resolution and closure of the file.....	12
7.	Hearing Procedura.....	13
8.	Penalties.....	13
9.	Information and closure of the file.....	13
10.	Advertising.....	13
10.	CONSERVATION, CUSTODY AND ARCHIVING OF INFORMATION.....	
11.	TRAINING, AWARENESS AND SENSITIZATION.....	
12.	DUE DILIGENCE FOR NEW PROFESSIONALS.....	
13.	APPROVAL.....	
14.	COMMUNICATION AND DISSEMINATION.....	
15.	ENTRY INTO FORCE AND VALIDITY.....	
16.	VERSION CONTROL.....	

1. DEFINITIONS

Communicator / Informant: person victim of illicit or irregular conduct or who has indications or has the suspicion that any of these behaviors is being committed within the Organization, who interposes a communication in this regard through the Internal Information Channel.

Compliance Committee: collegiate body responsible for the supervision and monitoring of the Compliance Management System in the Organization.

Internal Information Channel: channel through which both the Professionals of the organization and other third parties that are related to it, may communicate suspicions of contrary conduct, irregular, non-aligned or that imply a violation, infraction or breach of current legislation, the Ethical Code or the internal regulations of the organization.

Organization: SPAIN STARTUP AND INVESTORS SERVICES S.L. (SOUTH SUMMIT)

Professionals: are all the members of the organization, from the Management and the Administrative Body, to the workers, through the middle managers and the management bodies.

Subject investigated: person against whom the communicator interposes the communication through the Internal Information Channel for having indications or the well-founded suspicion that he is the author of an illicit or irregular conduct within the organization.

Stakeholders: Also known as "interested parties", *stakeholders* are all those people or organizations that constitute the public of interest to the organization, that is, that relate to the activities and decisions of the same, such as employees, managers, owners, shareholders, customers, suppliers, creditors, competitors, banks and financial institutions, media, Government, organizations and Administrations Public, NGOs, unions, collaborators, *partners*, business partners, etc. Following the terminology of the UNE/EN/ISO Standards, are the people or organizations, external or internal, that may affect, be affected or be perceived as affected by a decision or activity of the organization.

2. INTRODUCTION

The Organization has institutionalized the general principles of action and ethical values, which must be complied with by all personnel (administrators, managers, employees) and all those natural or legal persons whose activity is expressly subject to the Organization's Ethical Code. Likewise, it has in its organizational structure the figure of the Compliance Committee whose function, among others, is to coherently solve ethical conflicts that may arise in the future of the corporate life of the entity.

The collaboration of the Organization's staff, as well as its collaborators, suppliers or third parties related to it, is of the utmost importance for the

detection and prevention of irregular or illicit conduct that may jeopardize the prestige and good name of the Organization and its professionals.

The purpose of this document is to regulate and inform its recipients of the operation of the Internal Information Channel. The reception and management of communications will be carried out by an independent external advisor (GRUPO ADAPTALIA LEGAL - FORMATIVO, S.L., hereinafter GRUPO ADAPTALIA), while the subsequent investigation will correspond to an investigating body or responsible for the investigation (being able to be internal or external personnel to the organization) of the Organization appointed by the Compliance Committee, all in order to guarantee a process with the maximum guarantees of transparency and impartiality. Both bodies will ensure that the confidentiality and/or anonymity of the communicator is preserved, as well as the absence of retaliation and other negative consequences for professionals or any other person in their environment due to the communication made.

The Organization considers it necessary to have a policy for the handling of possible ethical, criminal, financial, administrative, etc. irregularities. In this sense, this Policy has been designed so that users of the Canal know how it works and the guarantees of confidentiality, privacy rights, presumption of innocence and self-defense of the persons investigated that are included in it.

3. SCOPE OF APLICATION

This Policy is applicable and, therefore, covers communications submitted by all professionals or collaborators of the Organization, as well as by suppliers or third parties with a legitimate commercial or professional interest with it.

Communications may refer to any type of action, conduct or behavior that is considered contrary to current legislation and the internal policies of the Organization.

Communications referring to doubts, queries or complaints, about a labor situation that does not involve an irregularity or possible violation of the Ethical Code, are not subject to the Channel and will be archived without procedure. In this case, it is procedural that the query may be made personally to the person in charge, as well as through the customer service contact of the Organization:

- Email: info@southsummit.io
- Online consultation form: <https://www.southsummit.io/es/contact-us/>

4. MEDIA

In order to guarantee the greatest confidentiality of the communicator, as well as the information and / or documentation provided with the communications, these will be interposed in the Internal Information Channel enabled for this purpose, which can be accessed through the website of the Organization (<https://www.southsummit.io/es/>), as well as through the following link:

<http://centinela.lefebvre.es/public/concept/1797402?access=y%2bulcK6AHyyGBOKr05mTclUiDRygOjw2N97sWf5Uswl%3d>

This channel allows the presentation of communications confidentially, allowing communications to be anonymous or not and has extreme security measures that guarantee the total confidentiality of the information and data provided through this channel.

5. CONTENTS AND IDENTIFICATION DATA OF COMMUNICATIONS

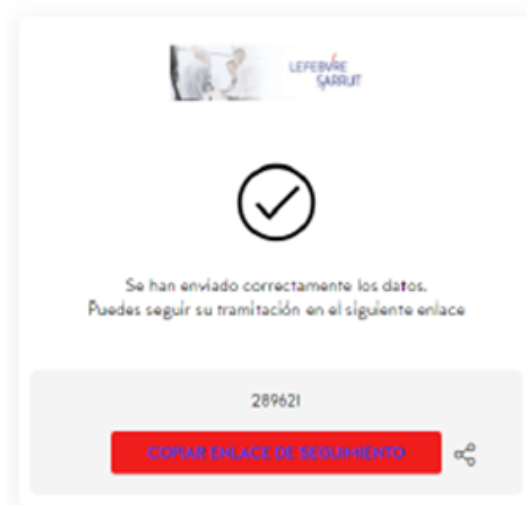
The communicator, once he accesses the form, completes a series of predefined fields through which he communicates the incident, deciding if his communication is going to be anonymous or not.

However, in order to be able to collect the necessary information for its management and for an exhaustive analysis of the problem, the informant is recommended to identify himself or, at least, provide contact information to be able to contact him if necessary.

Whether the caller decides to identify himself at the time of submission of the communication or not, he must necessarily provide the following information:

- i. **Relationship** with the organization: if the informant has an internal relationship with the company (worker, manager, etc.) or if he is external to it (supplier, collaborator, etc.).
- ii. **Typology of the conduct to be communicated**: selecting the type of behavior that best suits the situation that the informant wants to communicate.
- iii. **Detailed and exhaustive account of the facts** that are communicated (date, time, place, affected persons and any other concurrent circumstance that serves to clarify the facts).
- iv. **Date of the incident**.
- v. **Documentation accrediting** the facts communicated, if any.

If the user informs the communication anonymously and does not include any identifying data, once completed and sent the form, he will receive a unique code and a URL through which he can follow the evolution of his communication (this URL is also provided in the case of identified communications).



In the event that the caller decides to identify himself, in addition to the information detailed in the previous paragraph, he must provide the following identification data:

(i) Name and surname.

(ii) Contact details (email, telephone number or any other way to contact him). In the case of email, it will be the only required field.

In this case, the user knows the resolution of his communication through his email or also through the tracking link.

Both at the time of identification and at a later time, national and Community regulations on the protection of personal data will apply, in particular, Regulation (EU) 679/2016 on the protection of personal data of *April 27, 2016 (hereinafter, RGPD)* and Organic Law 3/2018 , of *December 5, Protection of Personal Data and Guarantee of Digital Rights (hereinafter, LOPDGDD)*, so that the information transmitted by the communicator is "inviolable", and cannot be modified at any time by the person responsible for the channel or any other user of the platform, thus complying with the current regulations mentioned above.

It is important to mention that the Internal Information Channel form includes the following elements, beyond the descriptive fields of the incident:

- **Upload of documents:** the user can include in his communication documents that he considers important to prove his declaration (images, PDF, Word, Excel documents, etc.).
- **Internal Information Channel:** the communicator and the investigated subject can communicate through this functionality.
- **Information:** the heading of the form includes the following introduction, with information of interest to the communicator:

"The internal information system allows you to report a violation according to L 2/2023. If you wish, you can make your report anonymously. In that case, you will receive a unique code and URL once you complete the form. Please save this access to be able to consult at all times the status and resolution of your complaint.

Any person who carries out an action that involves an effective limitation of the rights and guarantees provided for in this law, introduced through contracts or agreements at the individual or collective level and in general any attempt or effective action to hinder the presentation of communications or to prevent, frustrate or slow down their follow-up, including the provision of false information or documentation by those required to do so, shall be subject to the corresponding disciplinary procedures and sanctions in accordance with the labour legislation in force at any given time and the applicable collective agreement."

6. CONFIDENTIALITY

Access to the data of the communicator or any other information related to the communication will be limited exclusively to the independent external advisor, GRUPO ADAPTALIA, as Channel Manager in charge of the reception and management of communications that will act as an intermediary between the Compliance Committee facilitating the content of the communication but not the personal data of the communicator and the investigating body or responsible for the investigation (internal or external to the organization) appointed by the Compliance Committee of the Organization that will carry out the investigation of the facts communicated.

However, it will be lawful for other persons to access it, or even to communicate it to third parties, when it is necessary to:

- The adoption of disciplinary measures, in cases of false communication.
- If there is a requirement for identification by the Security Forces and Bodies, Public Administrations with competence over the actions communicated and Courts of Justice or other jurisdictional bodies.
- Be essential for communication research.

The maximum confidentiality and confidentiality about the identity of the caller and the documents or any other evidence that is provided throughout the process will be kept.

In order to comply with the provisions of the previous sections, it will be the obligation of the Compliance Committee to adopt the necessary technical and organizational measures to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected by the information provided, especially that of the person who had brought the facts to the attention of the entity, if identified.

7. DATA PROTECTION

The data of the participants in the procedure will be managed in accordance with the provisions of the RGPD and the LOPDGDD and will be incorporated into the Register of Treatment Activities of the Organization as Responsible for Treatment, with address at Monte Esquinza 28, 4ºD. 280100, Madrid (Madrid), Spain, in order to manage, investigate and resolve communications in relation to the alleged commission of irregularities.

The communicators may freely exercise their rights of access, rectification, deletion, opposition, limitation and portability, accompanying the necessary information by any of the following means:

1. Letter addressed to: GRUPO ADAPTALIA LEGAL-FORMATIVO, S.L., CL. JULIÁN CAMARILLO 26, 4ª PLANTA / 28037 - MADRID (MADRID).
2. By email to the address: legal@grupoadaptalia.es

Required information:

- Name and surname of the interested party.
- Photocopy of the DNI, passport or other valid document that identifies you, or of the person who represents you, if applicable.
- Request in which the request is specified.
- Address for notification purposes, date and signature of the applicant.
- Documents accrediting the request made, if applicable.

If the recipient of this policy wishes to obtain additional and detailed documentation on the privacy policy, you can consult it on the left margin of the Channel, by clicking on the following link (<http://centinela.lefebvre.es/public/concept/1797402?access=y%2bulcK6AHyyGBOKr05mTclUiDRygOjw2N97sWf5Uswl%3d>), or by sending an email to legal@grupoadaptalia.es.

8. PROTECTION OF THE CALLER

All bona fide communicators are guaranteed that the Organization may not, before, during, or after receipt of the communication, take any measure that harms their professional career or that involves the cessation of the employment or professional relationship with the company or any other

negative consequence for the professional or the people around him. In any case, the protection of the communicator will not exempt him from the responsibilities that he could have incurred for facts other than those that constitute the object of the communication.

Those communicators in bad faith who present false communications or communications whose sole purpose is to undermine the reputation of the company or any of its professionals, will be subject to the corresponding disciplinary procedures and sanctions in accordance with the labor legislation in force at any time and the collective agreement that is applicable.

9. PROCESSING AND MANAGEMENT OF COMMUNICATIONS

1. Reception, classification and management of communications

The communication will be received by the Channel Manager (ADAPTALIA GROUP), constituted by an external and independent advisor to the organization who will proceed to its classification, processing and assignment of a unique code (in case of having submitted it anonymously) and a URL through which the communicator can identify the communication presented and request information about its course. The Channel Manager must acknowledge receipt of the communication within a maximum period of **7 days**¹ from the date of its receipt and, if necessary, will request additional information from the communicator to clarify aspects of the communication that are key to determining if it is likely to continue with the subsequent investigation. If within 15 calendar days the caller does not provide such information and corrects the defects indicated, it will be archived without investigation.

In the event that the Channel Manager considers that there are no indications to continue with the course of the communication, it will be **archived**. Likewise, if the communicator does not provide the information indicated in the previous paragraph and it is not possible to obtain it by other means, it will also be filed. In the event that in the future the required data, new indications or additional information are obtained, the opening of a new file will be necessary.

In other cases, the Channel Manager, after the preliminary analysis of the communication, may:

1. **File without investigation procedure and finalize the file**, in the event that:
 - The communication does not meet the minimum formal requirements for processing.
 - The conduct does not present prima facie evidence of an infringement.

¹ The periods expressed in days throughout this document should always be understood as referring to "natural" days, not working days.

- The communication refers to a doubt, query or complaint (e.g. about an employment situation, characteristics of a product, etc.), without involving an infringement.
- The content of the communication is manifestly irrelevant.

2. Admit to investigation procedure.

The Channel Manager will send to the Organization, through the liaison contact, all the information and documentation collected from the communication, with the exception of the personal data of the communicator. Specifically, the name, surname, email and contact telephone number of the caller will not be communicated to the company.

The status of both cases may be consulted by the communicator through the URL generated once the communication form has been completed and sent.

2. Investigation of the file

Once the communication has been admitted for investigation, the Channel Manager will transfer its content to the Compliance Committee, which must designate, within a maximum period of **10 calendar days**, a person responsible for the investigation or investigating body that will be the person in charge of carrying out the proceedings and actions necessary for the clarification of the facts that occurred. as well as the identification of those responsible.

In the case of opting for an external instructor body to the Organization, their choice will be made according to criteria of suitability in terms of knowledge, training and area of *expertise, as well as* their communicative and empathic skills that provide the communicator and / or subject investigated with an adequate and friendly environment, as well as favorable conditions in which they can express themselves with total freedom and confidence.

The investigating body may use all the means of proof and sources of information at its disposal to try to clarify the facts, always taking into account the principle of proportionality. In this sense and by way of example, but not limited to, you can conduct personal interviews, review reports or performance evaluations, records, visits, etc.

Depending on the scope, scope and persons allegedly involved in the irregularity reported, the investigating body will assess the investigation strategy to be developed in each specific case, having the following options:

- That the investigation file is fully designed, led and managed by the investigating body, without prejudice to the consultations or support that may be required from other departments for its complete substantiation (designation of a work team).
- That the investigation file is designed, led and managed by the investigating body and that, in response to the needs of the case, it delegates all or part of the investigation process to a specific internal body or department of the Organization when this is advisable due to its

specialty, specific knowledge, access to information or geographical scope of the irregularity to be investigated.

- That the investigation file is designed, led and managed by the investigating body and that according to the needs of the case, all or part of the investigation process is outsourced, in an external collaborating company.
- That according to the circumstances of each case it is a member of the Compliance Committee itself who directly assumes the role of investigating body.

Any collaboration in the investigation of an irregularity is subject to the duty of confidentiality with respect to the information that may become known in its actions. Likewise, any person who is going to collaborate has the obligation to refrain from being part of the investigation team if there could be a conflict of interest or just cause on it, expressly communicating said incompatibility to the investigating body.

The Compliance Committee may supervise the investigation carried out, leaving evidence together with the investigating body of the corresponding records.

3. Precautionary measures

At the same time as the investigation begins and before communicating the facts to the subjects under investigation, the investigating body may request the Organization's management to adopt precautionary measures as a matter of urgency when:

- There is a risk of loss or manipulation of information or evidence.
- The extreme gravity of the facts reported so advises.

The communication of these measures to the subjects investigated will be carried out by the investigating body, always taking into account the principle of presumption of innocence.

These measures may be delayed as long as the risk exists, taking into account that, except in extraordinary cases to be justified by the investigating body, the validity of any precautionary measure may not exceed **three months** from the communication of the Canal Manager to the Compliance Committee.

4. Communication to the investigated subject and hearing/defense process

In the course of the investigation, the investigating body - whenever possible and there are no reasonable grounds to the contrary - will contact the subject under investigation, identifying itself to him as the person in charge of the investigation of the alleged irregularity and briefly informing him of the facts imputed to him, of the possible classification of the same and the possible consequences.

In the event that several persons are responsible for the alleged irregularity, the interviews will be carried out separately, but simultaneously to avoid

communication between them. In this case, if the investigating body deems it appropriate, it may opt for confrontation between the persons investigated or between them and the admitted witnesses.

The person under investigation shall be notified within a maximum period of **15 days** from the initiation of the investigation or from the moment his identity is known, if this occurs at a time after the initiation. This notification may be delayed when it entails a risk of destruction or tampering with evidence. If so, the instructor will document in his investigation report the basis for this decision. In any case, such notification may not be delayed to the extent that it may render the person under investigation defenceless.

From the notification to the person investigated, he has a period of **20 days** to exercise his defense, arguing in writing what he deems appropriate for his defense and provide those documents that he considers of interest. The subject investigated may be assisted by the professional of his confidence or person who advises him to make such allegations without more requirement than his mere designation in writing. After the deadline, no allegations will be admitted and the procedure will continue, unless the Compliance Committee considers, in its prudent discretion, that the deadline should be extended for just cause.

During the interview, the investigating body will ask the person under investigation the questions it deems appropriate to clarify the facts investigated. The person under investigation, if he so wishes, shall not be obliged to reply and his refusal to reply shall not be regarded as tacit acceptance of the facts.

The investigating body shall draw up a record of the interview conducted and it shall be signed by it, the person under investigation and the witnesses questioned, if any.

The research process is developed within a maximum period of **60 days from the receipt of the research proposal, extendable for a maximum of 30 days, if the person involved has not been identified by the caller, if all the necessary evidence has not been obtained to conclude the investigation or for other reasons that duly justify it.**

5. Final Report

Once all the investigative measures have been completed, the investigating body shall prepare as quickly as possible a final report addressed to the Compliance Committee for its information, opinion and control, which shall contain details of the alleged irregularities, the work carried out, the opinion of the investigating body regarding the facts that occurred and, if applicable, proposals for actions or controls to be carried out by the Organization to prevent such irregularity from occurring again.

6. Resolution and closure of the file

Upon completion of the investigation, the investigating body shall forward the report to the Compliance Committee, which shall be the competent body to resolve the investigation file of any irregularity committed in relation to the Organization.

The Compliance Committee may adopt any of the following decisions, recording the reasons and conclusions that support them:

- a) **Request the practice of additional investigative actions** to the investigating body in the event that its final report has not been sufficiently conclusive. In this case, the file will be sent back to the investigating body to comply with the mandate of the Compliance Committee.
- b) **Discard the communication**, declaring the non-commission of an irregularity, considering that the facts provided (i) do not constitute non-compliance; (ii) the information provided is insufficient to proceed with any further action; (iii) does not meet the requirements of truthfulness, completeness and clarity.
- c) **Declare the commission of an irregularity**, being able to adopt the following measures:
 - Apply the Disciplinary Regime in coordination with the HR Department.
 - Transfer to the business unit / department in which the irregularity has been committed the adoption of corrective measures to prevent the commission of new irregularities.
- d) **Make available to the competent administration of justice the irregularities detected.**

7. Hearing Procedura

Once the investigation is over, the Compliance Committee will inform the investigated subjects of the proposed resolution, who may, if they consider it necessary, expressly allege whatever they deem appropriate for their discharge and provide the documentation they deem appropriate.

The Compliance Committee may invite any person it considers appropriate in view of its specific expertise to participate in this procedure.

The investigated subjects will have a period of 5 working days, counting from the communication of the resolution proposal by the Compliance Committee, to present the allegations it deems appropriate.

Once this period has elapsed, the decision shall be final and there is no appeal.

8. Penalties

The sanctions that may be imposed in each case will be those provided for depending on the regime of relationship with the subject investigated, taking into account the internal Disciplinary Regime in accordance with the Workers' Statute and the applicable collective agreement, namely the **Collective Agreement of offices and offices of the Community of Madrid**.

The gradation of the sanctions will be determined according to the acts committed, and circumstances such as recidivism, damage or losses caused, circumstances, etc. may be taken into consideration.

When the investigation concludes with the imposition of disciplinary actions, it will be the Chief Operations Officer of the Organization who reliably notifies the person investigated, within a maximum period of **15 days**, of the disciplinary measures taken and their causes.

9. Information and closure of the file

After the completion of the file and, where appropriate, its mandatory communication to the person investigated and its business unit / department, the closure will be informed to the communicator through the URL provided at the time of submission of the communication. Such information shall contain only mention of whether the facts reported have led to the identification of any irregularity and shall never contain details of the actions taken or the conclusions reached. In no case, the investigation file will be shared with the communicator.

10. Advertising

The communication of admission to processing made by the Canal Manager, the content of the investigation file and the resolution reached, will not be public.

Exceptions to the above:

- The periodic report on the resolutions issued that the Compliance Committee must issue for statistical purposes to the Administrative Body of the Organization.
- The communication of the irregularity to the administrative or judicial authorities, in the event that it presents characteristics of administrative offense or crime, in which case the Organization is obliged to communicate it.

10. CONSERVATION, CUSTODY AND ARCHIVING OF INFORMATION

A record will be kept with all communications received and, where appropriate, all information for the time legally allowed by current regulations at all times. The aforementioned registry will comply with the technical and organizational security measures.

Under art. 24 of the LOPDGDD the data of the person who formulates the communication, professionals and third parties will be kept in the communication system only for the time necessary to decide on the appropriateness of initiating an investigation into the facts communicated.

In any case, after **3 months** from the introduction of the data, you must proceed to cancel the communication system. This cancellation will consist of blocking the data, that is, the reservation of the same in order to prevent its treatment, with the exception of its availability to public administrations and judges and courts for the attention of possible responsibilities during the corresponding

limitation periods in accordance with the provisions of current regulations. After that, the data will be physically deleted.

However, the foregoing, after the period of **3 months**, the data may continue to be processed, by the person to whom the investigation of the facts communicated corresponds, not being kept in the internal communications information system itself. In no case may the data be kept for a period exceeding ten years.

11. TRAINING, AWARENESS AND SENSITIZATION

The principles and rules contained in this standard will be included within the contents of the training plans carried out within the Organization.

These actions will have the purpose of training, raising awareness and sensitizing Professionals, with the aim of promoting internally a culture of respect for current legislation and the internal regulations of the Organization.

Ultimately, this will have a very positive impact on the internal functioning of the Organization itself, on the correct development of processes, on the improvement of competitiveness, on the increase of transparency and, especially, on the maintenance, consolidation and strengthening of the corporate image, brand and reputation, guaranteeing the trust of Professionals, suppliers, customers and other *stakeholders*.

In addition to the aforementioned training activities, the Organization may undertake other training, awareness and sensitization actions, such as publications on the Web, on the Blog, on the intranet, issuance of internal communications, incorporation into the bulletin board, etc.

12. DUE DILIGENCE FOR NEW PROFESSIONALS

In application of this standard, the Organization assumes the commitment to inform new staff of the existence of the same, its content and the mandatory nature of its compliance.

13. APPROVAL

This standard is approved by the Organization's Administrative Body.

14. COMMUNICATION AND DISSEMINATION

Without prejudice to the foregoing for newly incorporated Professionals, this standard will be communicated and disseminated annually to the Professionals of the Organization, through its digital or physical distribution (sending by email, issuing internal communications, incorporation to the bulletin board, publication on the Intranet, etc.).

15. ENTRY INTO FORCE AND VALIDITY

This standard enters into force and is in force from the day following its communication and dissemination to the Professionals of the Organization, in accordance with the provisions of the previous section.

16. VERSION CONTROL

VERSION	DATE	CHANGE DESCRIPTION
1.0	27/07/2023	INITIAL VERSION