



Regulation of the Internal Information System

Version Control

Version	Description of the actions taken	Date
1.0	Original document	01/06/2026

CONFIDENTIAL

Table of Content

1	Purpose and Scope of Application	5
1.1	Purpose	5
1.2	Subject Matter	5
1.3	Scope of Application of the Complaints Channel	6
2	Internal Information System	8
2.1	Basic Principles of the Internal Information System	8
2.2	Responsible of the Internal Information System	9
3	Implementation of the Complaint Channel.....	11
4	Communications management process.....	12
4.1	Start Process.....	12
4.2	Complaint evaluation.....	12
4.3	Investigator process.....	13
5	Information Reserve and Confidentiality	17
6	Control and Supervision.....	18
7	Protection of Personal Data	19
7.1	Responsible of the treatment, data processing and rights	19
7.2	Purpose, legal basis, and retention periods.....	19
7.3	Confidentiality.....	20
7.4	Communication of Personal Information	20
8	Applicable disciplinary System	22
8.1.	General Principles.....	22
8.2.	Scope of Application	22
8.3.	Disciplinary Authority	22

8.4. Directors and Employees Duties	23
9 Internal Information System approval.....	24

CONFIDENTIAL

1 Purpose and Scope of Application

1.1 Purpose

The purpose of these Regulations is to establish the internal operating rules for the Internal Information System of Nemergent Solutions, S.L., with Tax ID Number B95869293 and registered office in Erandio, 6 Ribera de Axpe Avenue, 2nd Floor, Offices 5-6, in accordance with the provisions of Law 2/2023 of February 20, which regulates the protection of individuals who report regulatory violations and combats corruption.

The Internal Reporting System is established as the preferred channel for people or organizations affected by its scope of application, to report—including anonymously—potential regulatory violations, conduct contrary to internal policies, or incidents falling within the scope defined in these Regulations.

The present law regulates, in particular, the substantive and subjective scope of application of the Internal Information System, the principles governing its operation; the appointment and duties of the Internal Reporting System Officer and the Alternate Internal Reporting System Officer, the procedure for handling reports received, safeguards regarding confidentiality and protection against retaliation; the processing of personal data; and the system's monitoring and updating procedures.

The Internal Reporting System shall be interpreted and applied in accordance with Law 2/2023, respecting the labor, administrative, criminal and personal data protection laws, or any other applicable legal provisions depending on the facts reported.

Activities carried out under the Internal Reporting System may be subject to internal or external review or audit, as necessary, and must be properly documented to demonstrate Nemergent's diligence in handling the communications received.

1.2 Subject Matter

Nemergent's Internal Reporting System has been made for reporting information regarding incidents that may fall under any of the following categories:

1. Any acts or omissions that may constitute violations of European Union law, provided that:
 - a. Fall within the scope of the European Union acts listed in the annex to Directive (EU) 2019/1937 of the European Parliament and Council, of October 23, 2019, on the protection of people who report breaches of Union law, regardless of how such acts are classified under national law.
 - b. Affect the financial interests of the European Union, as is stated in Article 325 of the Treaty on the operation of the European Union (TFUE)
 - c. Have an impact on the internal market, as it is in the Article 26(2) of the TFEU, including the violations of European Union rules on competition

and State aid, as well as violations to the internal market in connection with acts that breach corporate tax rules or practices intended to obtain a tax advantage that undermines the object or purpose of the legislation applicable to corporate tax.

2. Acts or omissions that may constitute a criminal offense or a serious or very serious administrative violation, particularly those that cause financial harm to the Treasury or Social Security, without being limited exclusively to these cases.
3. Violations of labor law relating to occupational safety and health that may constitute a criminal offense or a serious or very serious administrative violation.
4. Matters that the Head of the Internal Reporting System or, when is required, the substitute Head of the Internal Reporting System, considers it necessary to address by this channel because of their seriousness, social impact, or significant implications for the company.

For the purposes of this regulation, any communication or information will be considered as a communication when it is done in good faith, by anyone falling within the scope of application, through the means provided for that purpose, regarding facts that may fall under any of the above categories.

The following cases are excluded from the scope of the Internal Information System: simple differences of opinion, professional views on the day-to-day management of the center, general inquiries, questions regarding interpretation, suggestions for improvements, routine administrative issues, general academic complaints, everyday conflicts among staff and students, or matters for which a specific procedure exists within Nemergent—unless the reported facts may reveal a significant regulatory violation, serious misconduct, or a risk to individuals or the organization.

Communications that refer exclusively to routine problems with services, support for families, academic matters, or administrative issues will be handled through the usual internal channels, without prejudice to the possibility of processing them through the Internal Reporting System if the facts described indicate the possible existence of any of the violations described in this section.

The use of the Internal Reporting System is compatible with the option of reporting directly to the competent authorities, in particular through the external reporting channel of the Independent Whistleblower Protection Authority (A.A.I.), through any channels that may be established by the competent regional authorities or agencies, and, where applicable, through the institutions, bodies, or agencies of the European Union.

1.3 Scope of Application of the Complaints Channel

The Internal Reporting System may be used by individuals who have obtained information about violations in a work or professional context related to Nemergent. Specifically, they may submit reports through the Internal Reporting System:

- a. Nemergent employees, including those whose employment has ended
- b. Volunteers, interns, employees undergoing training, and candidates who are participating or have participated in recruitment processes or pre-employment negotiations
- c. Legal representatives of employees, in the course of their duties to advise and support the informant.
- d. Self-employed individuals affiliated with Nemergent.
- e. People involved in the administration, management, or oversight of Nemergent.
- f. Any person who works for or under the supervision and direction of Nemergent's contractors, subcontractors, or suppliers.

The protection provided for in this Regulation shall extend, under the terms set forth in Law 2/2023, to individuals who assist the informant in the process, to people related to the informant who may be subject to retaliation—such as coworkers or family members—and to legal persons for whom the informant works, with whom the informant has any other type of relationship in a work context, or in which the informant holds a significant interest.

Todas las personas incluidas en el ámbito de aplicación del presente Reglamento deberán utilizar el Sistema Interno de Información de buena fe y con respeto a los principios de confidencialidad, veracidad razonable, prohibición de represalias y protección de los derechos de las personas afectadas.

All persons covered by this Regulation must use the Internal Reporting System in good faith and in accordance with the principles of confidentiality, reasonable authenticity, prohibition of retaliation and protection of the rights of the individuals concerned.

2 Internal Information System

2.1 Basic Principles of the Internal Information System

Nemergent's Internal Information System is based on the following principles:

- a. **principle of good faith and promise of non-retaliation:** Individuals who use the Internal Reporting System must do so in good faith and with reasonable grounds to believe that the information reported is accurate at the time of reporting. Nemergent will not tolerate any form of reprisal, threat of retaliation or attempt at retaliation against those who report, in good faith, facts falling within the scope of the system. The deliberate reporting of false, misrepresented, or bad-faith allegations may result in appropriate measures in accordance with applicable regulations.
- b. **Principle of Independence, Objectivity, and Impartiality:** The handling of communications shall be based on independence, objectivity, and impartiality, avoiding undue interference and ensuring that decisions are based on the facts reported, the available evidence, and applicable regulations. Individuals involved in accepting, analyzing, investigating, or resolving communications must abstain from such activities whenever any circumstance that could compromise their impartiality arises.
- c. **Security, confidentiality, compliance with personal data protection regulations, and efficiency in handling communications, including anonymous ones:** Nemergent will take appropriate technical and organizational steps to protect the identity of the informant, the affected individual, and any third part mentioned in the report, as well as to guarantee the confidentiality, integrity, and security of the information processed. The Internal Reporting System will allow for the submission and processing of anonymous reports.
- d. **The Right to reputation, the presumption of innocence, and the Right to a defense:** Communications management shall always respect the presumption of innocence, the right to defense, the right to honor and the other rights of the individuals affected by the communication. These individuals shall have the right to be informed of the facts attributed to them and to be heard under the terms set forth in these regulations, without revealing the identity of the informant.
- e. **Diligence and Traceability:** Communications received must be handled diligently, within the time limits established in these Regulations, and sufficient records must be kept of the actions taken, the decisions made, and the measures implemented in each case.
- f. **Access limitations and the need to know.** Access to communications, files, and documentation related to the Internal Reporting System will be limited to strictly authorized individuals and only when necessary for the proper processing, investigation, or resolution of the report.

2.2 Responsible of the Internal Information System

The competent administrative or governing body of Nemergent shall designate the individual or collegiate body that will act as the Head of the Internal Reporting System, in accordance with the provisions of Article 8 of Law 2/2023.

The Head of the Internal Reporting System shall be the person or body responsible for ensuring the proper management of the system and the diligence in processing the reports received. If a collegiate body is appointed, its members must be identified, and the authority to manage the system and handle investigation files must be delegated to one of them.

The Head of the Internal Reporting System shall perform their duties with independence, autonomy, confidentiality, and diligence, without receiving instructions that could unduly affect the acceptance, analysis, investigation, or resolution of specific reports.

In particular, the Head of the Internal Reporting System shall be responsible for receiving or accessing reports submitted through the established channels, conducting an initial assessment, initiating the appropriate investigative actions, documenting relevant decisions, coordinating with the necessary internal departments or external professionals, and submitting the corresponding conclusions or proposals to the competent body.

The Internal Reporting System Officer shall not carry out functions that fall under the remit of Nemergent's administrative or governing body, the center's management, the human resources department, the Data Protection Officer, or other competent bodies. In particular, the Head of the Internal Reporting System is not authorized to impose disciplinary sanctions, make employment decisions, approve the Internal Reporting System Regulations, or represent Nemergent before public authorities unless he or she has sufficient authorization to do so.

If the Head of the Internal Reporting System finds themselves in a situation that could constitute a conflict of interest with regard to the report or investigation under review — whether due to a personal, professional, hierarchical, functional, or any other type of relationship with the individuals involved— they must immediately bring this to the attention of the competent administrative or governing body of Nemergent.

The competent body will assess the existence and scope of the potential conflict of interest and, if it is necessary, order the recusal or temporary removal of the responsible official from the specific case, designating another person or seeking external support to ensure the objectivity, impartiality, confidentiality, and continuity of the proceedings.

For the duration of their recusal or temporary removal, the affected Officer shall not participate in deliberations, decisions, or actions related to the case in question, nor shall they access, directly or indirectly, any information related to said report, except to the extent strictly necessary to document the conflict of interest or to activate the corresponding replacement mechanism.

In addition, Nemergent will appoint an individual or a collegiate body as the Alternate Head of the Internal Reporting System, who will act as the Head of the Internal Reporting System in the event that the Head is unable to perform those duties due to absence from the workplace. The appointment of the Alternate Head of the Internal Reporting System shall be carried out in accordance with the appointment procedure for the Head of the Internal Reporting System, and the Alternate Head must perform their duties in the same manner as the Head of the Internal Reporting System, in compliance with the obligations set forth in Law 2/2023.

CONFIDENTIAL

3 Implementation of the Complaint Channel

Nemergent provides individuals included in the scope of application of this Regulation with a specific, visible, and accessible section on its corporate website, which provides information on the operation of the Internal Reporting System, the applicable safeguards, and the channels available for submitting reports.

The Internal Reporting System will allow users to submit written reports via a web form, accessible at the following link: <https://legal.nemergent-solutions.com/>

The channel provided allows for the submission of both identified and anonymous reports, ensuring in all cases the confidentiality of the identity of the reporter, the person concerned, and any third party mentioned in the report, as well as the security of the information transmitted. When using a specific email address, please be aware that sending the report from an identifiable account may reveal your identity or technical data associated with the transmission.

Nemergent guarantees that access to received reports is limited to the Head of the Internal Reporting System (or the Deputy Head of the Internal Reporting System) and, where applicable, to those individuals strictly authorized to participate in their management, analysis, or investigation in accordance with these Regulations.

4 Communications management process

4.1 Start Process

The management procedure will be started by the receipt of a report through any of the channels provided within the Internal Reporting System. Likewise, the Head of the Internal Reporting System may initiate proceedings when he or she becomes aware, through other means, of facts that could objectively fall within the scope of these Regulations.

Reports may be submitted either with or without the reporter's identity disclosed. When a report is submitted with the reporter's identity disclosed, Nemergent will ensure the confidentiality of the reporter's identity and restrict access to the reporter's information to only those individuals who are strictly authorized to view it.

The report should include, as far as possible, a description of the facts, the approximate date or period during which they occurred, the individuals, areas, or activities affected, and any documents or evidence that may facilitate its analysis. The absence of any of these elements will not, in and of itself, result in the report being rejected, provided that there is sufficient information to allow for its evaluation.

Within seven calendar days of receiving the report, the Head of the Internal Reporting System shall send a confirmation of receipt to the reporter, unless the report is anonymous and no contact information has been provided, or unless sending the confirmation of receipt could put the confidentiality of the report at risk.

The person in charge of the Internal Reporting System must record the report received and, when appropriate, open the corresponding case file, stating the date of receipt, the method of submission, a summary of the facts reported, the initial actions taken, and any other information necessary to ensure the traceability of the procedure.

When a report is sent through different channels from those established or is received by a person who is not responsible for handling it, the receptor must immediately forward it to the Head of the Internal Reporting System via email at legal@nemergent-solutions.com, without disclosing its content to third parties and maintaining strict confidentiality regarding the identity of the reporter, the identity of the person involved, and the facts reported.

A violation of this duty of confidentiality may result in disciplinary action and, where applicable, constitute a very serious violation under Law 2/2023.

4.2 Complaint evaluation

After receiving the report, the person in charge of the Internal Reporting System will conduct an initial assessment to determine whether the reported facts fall within the scope of these Regulations and whether there is sufficient information to support their

analysis. Following this initial assessment, the person in charge may take one of the following actions:

- a. Not admitting the report when the facts reported are manifestly unfounded, are implausible, fall outside the scope of the Internal Reporting System, or do not contain enough information to allow for an analysis.
- b. Forward the report to the appropriate internal channel when the reported incidents do not fall within the scope of the Internal Reporting System but can be addressed through other internal Nemergent procedures, such as academic, administrative, labor, community relations, family support, or routine incident management channels.
- c. Accept the report for processing when the facts reported may fall within the scope of the Internal Reporting System and there is sufficient evidence to start analysis or an investigation.

The decision to reject, refer to another channel, or accept the complaint for processing must be documented in the case file. When the complainant has provided contact information, he or she will be informed of the decision within a reasonable time and, in any case, within the maximum response time provided for in these Regulations, unless such notification can compromise confidentiality, the investigation, or the rights of the individuals involved.

Each communication accepted for processing must be the subject of an internal file, which must be properly identified, documented, and kept confidential with restricted access.

At this stage, it must also be evaluated if there is any conflict of interest that could affect the Head of the Internal Reporting System or any person involved in the handling or investigation of the report. In the event of the conflict, the mechanism for recusal, replacement, or external support provided for in these Regulations will be activated.

4.3 Investigator process

4.3.1 Beginning:

The investigation process will begin when the Head of the Internal Reporting System accepts a report for processing and determines that further action is necessary to clarify the facts reported.

When the reporter has provided a contact method, the responsible of the Internal Reporting System may communicate with the reporter and request additional information, not compromising confidentiality, the security of the procedure, or the rights of the individuals concerned.

The person affected by the report shall have the right to be informed of the actions or omissions attributed to him or her and to be heard at any stage of the proceedings, in the way and at the time appropriate to ensure the successful completion of the investigation. Under no circumstances shall the identity of the reporter be disclosed to the person affected, except in cases provided under the law.

4.3.2 Investigation:

The purpose of the investigation will be to take the necessary steps to clarify the reported facts. To that end, interviews, document reviews, internal audits, requests for information, and any other actions that are proportionate and appropriate to the nature of the facts may be carried out.

The Head of the Internal Reporting System may request the assistance of the relevant internal departments or specialized external professionals when the nature, complexity, or sensitivity of the report so requires. All individuals involved in the investigation must maintain strict confidentiality regarding the information to which they have access.

A record of the actions taken will be included in the case file, including communications, interviews, reviewed documentation, evidence obtained, decisions made, and any other relevant information to demonstrate the diligence of the investigation.

The maximum time limit for to answer the investigation may not exceed three months from the date of receipt of the notice or, if an acknowledgment of receipt was sent to the whistleblower, from the date of that acknowledgment. In particularly complex cases that require an extension of the time limit, it may be extended for a maximum of an additional three months, provided that a written and reasoned record of such extension is kept.

The guiding principles of the procedure are the following ones, and all individuals involved must adhere to them:

- a. Actions must be taken quickly and efficiently, avoiding unjustified delays.
- b. The information handled during the investigation will be kept confidential and may only be disclosed to those individuals whose access is strictly necessary for its proper processing.
- c. The identity of the reporter, the affected person, and any third parties mentioned in the report must be protected throughout the proceedings, without prejudice to any communication that may be legally required.
- d. The affected person shall always retain the right to the benefit of the presumption of innocence, to honor, to a defense, and to be heard under the terms set forth in these Regulations.
- e. Decisions made during the investigation must be based on the facts reported, the available evidence, and applicable regulations, while avoiding any undue interference or non-objective judgment.

- f. Good-faith reporting shall not give rise to retaliation, threats of retaliation, or attempts at retaliation against the whistleblower or against people protected under Law 2/2023.
- g. The deliberate communication of false, distorted, or malicious statements may result in appropriate measures being taken in accordance with applicable regulations.

The maximum time limit for responding to investigative proceedings may not exceed three months from the date of receipt of the notice or, if an acknowledgment of receipt was sent to the whistleblower, from the date of that acknowledgment. In particularly complex cases requiring an extension of the time limit, it may be extended for a maximum of an additional three months, provided that a written and reasoned record of such extension is maintained.

4.3.3. Process of getting the evidence:

The collection of evidence will be conducted in full compliance with applicable law, the principle of proportionality, the confidentiality of information, the protection of personal data, and the rights of whistleblowers, affected individuals, and third parties mentioned in the report.

Investigative actions shall be limited to those that are necessary and appropriate to clarify the reported facts. They may consist of reviewing internal documentation, analyzing information provided by the reporter, interviewing individuals who may provide relevant information, requesting explanations, reviewing records, or any other action appropriate to the nature of the facts.

The evidence obtained must be incorporated into the case file in an organized and safe way, documenting its origin, date of collection, the individuals involved, and its relevance to the analysis of the reported facts.

When interviews or statements are conducted, a written record shall be made of the fact that they took place, the individuals involved, and the main points made, without prejudice to taking the necessary precautions to preserve the confidentiality of the proceedings and the rights of the individuals concerned.

When first taken evidence is not conclusive, additional steps that are considered necessary may be taken to determine the plausibility of the reported facts.

In no case may evidence be obtained through means that violate fundamental rights, are disproportionate, or involve unjustified access to personal or confidential information unrelated to the facts under investigation.

4.3.4. Conclusion:

Once the necessary steps to clarify the reported facts have been completed, the Head of the Internal Reporting System will issue a final report that must include, at a minimum,

a description of the reported facts, the date of the report was received, the actions taken, the evidence analyzed, the individuals or departments involved, the conclusions reached, and, where applicable, the proposed measures or the competent body or department to which the matter should be referred.

- a. The case shall be closed when there is insufficient evidence of a violation, when the reported facts have not been proven, or when it is not possible to continue the investigation due to a lack of sufficient evidence.
- b. Referral to the appropriate internal department or body when the circumstances may require labor, disciplinary, organizational, educational, workplace relations, data protection, or other measures.
- c. The implementation of corrective or improvement measures when defects are identified in Nemergent's protocols, procedures, internal controls, or organizational measures.
- d. Immediate notification to the Public Prosecutor's Office when the facts may, on the face of it, constitute a crime, or to the European Public Prosecutor's Office when the facts affect the financial interests of the European Union.
- e. Notification to the competent administrative or judicial authority when required by law or appropriate given the nature of the facts.
- f. The adoption of measures to protect against retaliation when risks are identified for the reporter or for any of the people protected under Law 2/2023.

The final report and the decisions adopted must be documented in the case file. When the report proposes measures that fall under the jurisdiction of another body or department within Nemergent, the Head of the Internal Information System shall forward its conclusions to the appropriate authority, limiting the information provided to what is strictly necessary to evaluate and adopt the corresponding measures.

When the reporter has provided a means of contact, they will be notified of the actions taken in accordance with the law, without disclosing any information that could infringe on the rights of third parties, compromise confidentiality, interfere with internal, administrative, or judicial proceedings, or affect the protection of personal data.

The affected person will be informed and given the opportunity to be heard in accordance with these Regulations; under no circumstances will the identity of the whistleblower be disclosed, except in cases provided for by law.

The closing of the case must be documented on the case file, including the decision taken, the date of closing, the proposed or adopted actions, and when it could be necessary, any information transferred to internal bodies, competent authorities, or external professionals.

5 Information Reserve and Confidentiality

All people who have knowledge of communications, files, proceedings, or documentation related to the Internal Reporting System are required to maintain strict confidentiality regarding the information to which they have access.

The identity of the reporter, the person concerned, and any third part mentioned in the report shall not be revealed to unauthorized people. In particular, the identity of the reporter shall not be disclosed to the person concerned or to third parties, except in cases provided for by law or when required by a competent authority in the context of a criminal, disciplinary, or sanctioning investigation.

Access to information received through the Internal Reporting System shall be limited to the Head of the Internal Reporting System and, where applicable, to those individuals strictly authorized to participate in the management, analysis, investigation, or resolution of the report, always in accordance with the principles of necessity, proportionality, and confidentiality.

When a report is received by someone other than is not part of the Internal Reporting System Manager or through an unauthorized channel, the recipient must immediately forward it to the Manager through the channel provided by Nemergent, without disclosing its content to third parties and maintaining strict confidentiality regarding the identity of the whistleblower, the identity of the person involved, and the facts reported.

A violation of the duty of confidentiality may result in disciplinary action in accordance with the collective agreement, applicable labor laws, statutory provisions, or internal policies, without prejudice to any other legal liabilities that may arise.

Nemergent will not tolerate retaliation, threats of retaliation, or attempts at retaliation against anyone who, in good faith, reports incidents falling within the scope of the Internal Reporting System, nor against people protected by Law 2/2023.

6 Control and Supervision

The Internal Information System Manager will periodically monitor the system's operation in order to identify potential issues, weaknesses, the need for updates, or areas for improvement.

This monitoring may include reviewing the operation of the channels established for submitting communications, compliance with processing deadlines, proper documentation of case files, access restrictions, the secure storage of information, the effectiveness of confidentiality measures, and the need to update the information made available to individuals authorized to use the system.

The Data Protection Officer may submit to Nemergent's competent administrative or governing body any proposals for improvements, updates, or corrections that he or she considers necessary to ensure the proper functioning of the Internal Information System.

These Regulations shall be reviewed when regulatory, organizational, technical, or procedural changes arise that may affect the operation of the Internal Information System, as well as when experience gained from its use suggests that improvements should be made.

Any significant revisions, updates, or amendments to the Regulations must be approved by Nemergent's competent administrative or governing body and properly documented.

7 Protection of Personal Data

7.1 Responsible of the treatment, data processing and rights

In accordance with the provisions of Regulation (EU) 2016/679, the General Data Protection Regulation, and Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights, Nemergent, with Tax ID Number B95869293 and registered office in Erandio, 6 Ribera de Axpe Avenue, 2nd Floor, Offices 5-6, Erandio, will act as the data controller for the personal data processed within the framework of the Internal Information System.

The Internal Reporting System may be used without providing the reporter's identifying information. However, the reporter may voluntarily provide personal information, including first and last name, phone number, email address, relationship to Nemergent, or any other information deemed necessary for reporting or following up on the matter.

The communications received may include personal data regarding the person affected by the reported events, third parties mentioned in the communication, or other individuals involved in the proceedings.

Interested individuals may exercise, to the extent applicable, their rights of access, rectification, removal, and limitation of processing by submitting a request to Nemergent's Data Protection Officer via info@nemergent-solutions.com or by mail to the address indicated in this section.

The exercise of these rights may be restricted when necessary to preserve the confidentiality of the whistleblower's identity, ensure the successful completion of the investigation, protect the rights of third parties, or comply with applicable regulations.

In addition, interested people may file a complaint with the Spanish Data Protection Agency through its website.

7.2 Purpose, legal basis, and retention periods

Personal data processed through the Internal Information System will be used for the purpose of receiving, managing, analyzing, and processing the reports submitted; investigating the reported incidents when appropriate; taking the necessary measures; and complying with the obligations set forth in Law 2/2023.

The legal ground for the processing is compliance with a legal obligation applicable to Nemergent, in accordance with Article 6.1.c) of the General Data Protection Regulation, in reference to Law 2/2023. When it is necessary to process special categories of data, such processing will be carried out when necessary for reasons of substantial public interest, in accordance with applicable regulations.

Personal data included in the reports received will be kept in the Internal Information System for as long as necessary to determine whether to initiate an investigation and, in any case, for a maximum period of three months from the date of receipt of the report, unless retaining the data for a longer period is necessary to provide evidence of the system's operation.

When it is appropriate to start an investigation, the data may continue to be processed outside the Internal Information System for as long as necessary to process the case, take the appropriate action and address any potential legal liabilities that may arise from the reported facts.

Nemergent will maintain a record of the information received and the internal investigations resulting therefrom, ensuring compliance with the confidentiality requirements set forth in Law 2/2023. This record will not be public and may only be made available to the competent judicial authority by court order and within the framework of judicial proceedings.

7.3 Confidentiality

Nemergent will ensure the confidentiality of the identity of the whistleblower, the affected person, and any third party mentioned in the report, as well as of the actions taken within the framework of the Internal Reporting System.

The person concerned shall have the right to be informed of the allegations against them and to be heard during the proceedings, in accordance with the provisions of these Regulations. However, such information shall be provided without revealing the identity of the whistleblower or any details that would allow that identity to be deduced, except in cases provided for by law.

Access to personal data processed within the scope of the Internal Information System shall be limited to the Head of the Internal Information System, or, where applicable, the substitute Head of the Internal Information System, and to those persons strictly authorized in accordance with Law 2/2023 and these Regulations.

7.4 Communication of Personal Information

Personal data processed within the scope of the Internal Information System may be accessed by the Head of the Internal Information System, or—when strictly necessary—by the Deputy Head of the Internal Information System, and by individuals who must be involved in the management, analysis, investigation, or resolution of the communications received, always within the limits set forth in Law 2/2023 and these Regulations.

In addition, the data may be processed by external providers or professionals who assist Nemergent in the management or investigation of communications, provided that the corresponding confidentiality agreements have been formalized and, where applicable, a data processor agreement or other applicable legal instrument has been entered into.

Personal data may be disclosed to judicial authorities, the Public Prosecutor's Office, the European Public Prosecutor's Office, law enforcement agencies, competent administrative authorities, or other third parties when necessary or required under applicable regulations.

CONFIDENTIAL

8 Applicable disciplinary System

8.1. General Principles

Nemergent may take appropriate disciplinary action in response to violations of internal regulations, protocols, instructions, or applicable legal provisions, in accordance with the labor, statutory, contractual, or sector-specific regulations applicable in each case.

The disciplinary response must be proportionate and take into account the nature of the facts, their severity, the surrounding circumstances, the rights of the individuals involved, and the applicable procedural safeguards.

The use of the Internal Reporting System does not alter Nemergent's disciplinary authority nor does it replace any applicable labor, statutory, educational, conduct, or administrative procedures.

8.2. Scope of Application

Personal data processed under the Internal Reporting System may be accessed by the Internal Reporting System Manager, or—when strictly necessary—by the substitute Internal Reporting System Manager, and by individuals who must be involved in the management, analysis, investigation, or resolution of the reports received, always within the limits set forth in Law 2/2023 and these Regulations.

In these cases, the data may be processed by external providers or professionals who assist Nemergent in the management or investigation of communications, provided that the corresponding confidentiality agreements have been formalized and, where applicable, a data processor agreement or other applicable legal instrument has been entered into..

The Internal Reporting System should not be used as the standard channel for handling academic complaints, administrative issues, day-to-day interpersonal conflicts, general complaints from families or students, requests for information, or matters for which there is a specific procedure within Nemergent, unless the reported facts may indicate a significant regulatory violation, serious misconduct, or a risk to individuals or the organization.

8.3. Disciplinary Authority

Disciplinary authority shall rest with Nemergent, through the body or department with jurisdiction in each case, and shall be exercised in accordance with applicable labor, collective bargaining, statutory, educational, or internal regulations.

The Head of the Internal Reporting System may document findings, submit reports, and propose that the facts be referred to the appropriate body; however, this does not

grant him or her the authority to impose disciplinary sanctions or to make employment, educational, organizational, or other decisions that fall under the purview of other bodies or departments within Nemergent.

When the reported facts may constitute a labor, disciplinary, administrative, or criminal violation, Nemergent will evaluate whether to initiate the appropriate proceedings, ensuring in all cases the rights of the individuals involved, the proportionality of the measures, and compliance with applicable regulations.

8.4. Directors and Employees Duties

Employees, managers, and other individuals covered by these Regulations must comply with Nemergent's internal rules and the instructions related to their work, and must use in good faith the channels provided to report incidents falling within the scope of the Internal Reporting System.

In addition, they must maintain confidentiality regarding any communication or information related to the Internal Reporting System to which they may have access, and cooperate diligently when requested to do so in the context of an internal investigation.

The deliberate communication of false, distorted, or malicious statements; a breach of the duty of confidentiality; retaliation; or the unjustified obstruction of an internal investigation may result in appropriate disciplinary or legal action in accordance with applicable regulations.

9 Internal Information System approval

These regulations have been approved by Nemergent's competent administrative or governing body on 26 of July of 2026.

The Regulation will take effect on the date of its adoption or on the date expressly specified in the relevant resolution, and will remain in force until it is replaced, amended, or updated by the competent body.

Significant changes in these regulations must be approved by Nemergent's competent administrative or governing body and communicated to individuals, made available to the affected individuals when necessary to ensure proper understanding of the operation of the Internal Reporting System.

CONFIDENTIAL