INTERNAL INFORMATION SYSTEM

AND WHISTLEBLOWER PROTECTION POLICY

I. INTRODUCTION, DEFINITIONS AND OBJECTIVES

This Policy on the general principles governing the Internal Information System and Whistleblower Protection (hereinafter, the "Policy") sets forth in writing the general principles applicable to the Internal Information System and whistleblower protection within the CUSA business group (hereinafter, "CUSA" or the "Organization").

This Policy complies with the provisions of Law 2/2023, of 20 February, on the protection of persons who report regulatory infringements and on the fight against corruption.

For clarification purposes, the following definitions are established to determine the scope of this Policy:

(i) CUSA: this term refers to the group of companies comprising:

Cromogenia Units, S.A.

Alcover Química, S.L.

Quimipiel, S.L.

Marlet Química, S.L.

Arteixo Química, S.L.

BM Polymers, S.L.

(ii) Persons associated with the Organization: natural or legal persons who maintain an ongoing relationship with CUSA.
By way of illustration, but not limitation, this includes employees of the aforementioned entities, as well as entrepreneurs (individual or corporate) with whom they maintain business relationships of any kind.

(iii) Crime Prevention and Response Policy: the set of provisions currently in force and implemented in each of the CUSA group companies.

(iv) Criminal Compliance Policy: the document that develops the necessary monitoring and control concepts regarding the various criminal offenses attributable to legal entities under Article 31 bis of the current Spanish Criminal Code.

(v) Criminal Prevention Model: the documents forming the essential basis of the measures adopted by CUSA to prevent criminal offenses within the Organization.

II. DEFINITION AND CHARACTERISTICS OF THE POLICY

This Policy constitutes the internal regulation of CUSA through which a framework is established to define **the general principles governing the Internal Information System and whistleblower protection**.

The purpose of this document is to ensure the proper interpretation of the procedure for managing information within the internal system, as well as the response procedures applicable where data or indications may suggest the commission of a criminal offense.

Taken together, the aforementioned documents comply with a regulatory framework that coherently organizes the Internal Information System within CUSA, including procedures for its ongoing development and updating.

This Policy has the following characteristics, which must be considered for its proper interpretation:

(i) It is a **continuous and dynamic** document. Its content must be adapted to circumstances arising from the evolution of CUSA or from legal, case law, or doctrinal developments.

(ii) The principles established herein shall be led and managed by the System Officer.

III. SCOPE OF APPLICATION

This Policy applies exclusively to CUSA, as defined in Section I above.

However, there are or may be other persons linked to CUSA through shareholding or commercial relationships, beyond those defined in Section I, who may adhere to this Policy. These include:

Self-employed collaborators working with the companies

Shareholders, partners, and members of administrative, management, or supervisory bodies of other companies, including non-executive members

Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers

The Policy establishes the basic principles governing the Internal Information System and whistleblower protection. The system applies to natural persons who submit information through any of the procedures provided herein. Such information shall be deemed a report and shall be analyzed and processed through the information management procedure.

This includes:

a. Any acts or omissions that may constitute breaches of European Union law, provided that they:

Fall within the scope of the EU acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, irrespective of their classification under national law;

Affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or

Affect the internal market as referred to in Article 26(2) TFEU, including breaches of EU competition and State aid rules, as well as breaches relating to the internal market in connection with corporate tax rules or practices aimed at obtaining a tax advantage that defeats the object or purpose of applicable corporate tax legislation.

b. Acts or omissions that may constitute serious or very serious criminal or administrative offenses.

In any case, this includes serious or very serious criminal or administrative offenses involving financial loss to the Public Treasury or the Social Security system.

This protection does not exclude the application of criminal procedural rules, including investigative proceedings.

Protection also applies to workers who report breaches of labor law relating to occupational health and safety, without prejudice to protection established under specific applicable legislation.

However, this Policy does not apply to information affecting classified information. Nor does it affect obligations arising from professional secrecy in the medical and legal professions, confidentiality duties of law enforcement authorities in the course of their actions, or the confidentiality of judicial deliberations.

The provisions of this Policy shall not apply to information relating to breaches in public procurement procedures containing classified information, declared secret

or confidential, requiring special security measures under applicable legislation, or involving essential State security interests.

Where information or public disclosure concerns infringements referred to in Part II of the Annex to Directive (EU) 2019/1937, the specific regulatory framework governing communication of such infringements shall apply.

IV. MANDATORY COMPLIANCE

The principles set forth in this Policy are mandatory for all natural and legal persons to whom the Internal Information System and whistleblower protection framework applies.

They hold the highest rank within CUSA's internal regulations, as they reflect the explicit opposition of CUSA's governing bodies (including senior management and middle management) to obtaining any direct or indirect benefit through unlawful conduct.

CUSA's Management shall ensure the application of this Policy, providing the relevant bodies and persons with sufficient authority and resources, including adequate financial resources, to perform their duties effectively.

V. GOVERNING PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM AND WHISTLEBLOWER PROTECTION

1. UNITY OF CHANNEL

The following reporting channels, previously managed independently, are integrated into the Internal Information System Information Management Procedure:

The reporting channel established under the Crime Prevention and Response Policy, Criminal Compliance Policy, and Criminal Prevention Model

The harassment reporting channel established under the applicable Collective Bargaining Agreement

The infringement reporting channel established under the Code of Ethics

2. IMPARTIALITY

CUSA avoids any form of discrimination based on age, gender, sexual orientation, health status, nationality, political opinions, or religious beliefs in all decisions

affecting stakeholders, including customer selection, shareholder relations, personnel management, work organization, supplier management, and community relations.

3. HONESTY

Within the framework of this Policy, CUSA collaborators must strictly comply with applicable laws, the Code of Ethics, the Crime Prevention and Response Policy, the Criminal Compliance Policy, and the Criminal Prevention Model.

Under no circumstances may the pursuit of CUSA's interests justify dishonest conduct.

4. SYSTEM OFFICER

The governing bodies of each CUSA company have appointed Carlos Cabestany Ferre as the Internal Information System Officer (the "System Officer").

5. PUBLICITY

This Policy and the Information Management Procedure shall be published on the website of each CUSA company.

The Independent Whistleblower Protection Authority (A.A.I.) shall publish the external information management procedure.

The external procedure shall be reviewed every three years and, where appropriate, amended based on experience and that of other competent authorities. Any amendment shall be published accordingly.

6. CONFIDENTIALITY

CUSA guarantees the confidentiality of the information it holds, complies with data protection legislation, and refrains from seeking confidential data unless expressly authorized and in accordance with applicable legal provisions.

Collaborators shall not use confidential information for purposes unrelated to their professional duties, including insider trading or market manipulation.

7. GUARANTEES

CUSA expressly guarantees that no retaliation shall result from reports submitted through the Internal Information System, including threats or attempts of retaliation.

Retaliation is understood as any act or omission prohibited by law, or any direct or indirect unfavorable treatment placing the reporting person at a particular disadvantage in the workplace or professional context solely because of their status as a whistleblower or due to public disclosure.

(Examples of retaliation include dismissal, disciplinary measures, reputational damage, blacklisting, denial of training, discrimination, among others, as defined in the original text.)

Protection may exceptionally be extended beyond two years by the competent authority where duly justified.

8. ANONYMITY

CUSA's Internal Information System allows anonymous reporting and includes appropriate technical and organizational measures to preserve identity and ensure confidentiality.

If not anonymous, the whistleblower's identity may only be disclosed to judicial authorities, the Public Prosecutor's Office, or competent administrative authorities within the framework of criminal, disciplinary, or sanctioning proceedings, subject to applicable safeguards.

9. CONDITIONS FOR PROTECTION

Protection applies provided that:

a) The reporting person had reasonable grounds to believe the information was true at the time of reporting and falls within the scope of the law; and
b) The report or disclosure complies with the requirements of Law 2/2023.

Anonymous reporters later identified who meet these conditions shall also be entitled to protection.

10. EXCLUSIONS FROM PROTECTION

Protection does not apply to:

Communications declared inadmissible due to implausible facts, lack of legal infringement, manifestly unfounded content, unlawfully obtained information, or absence of new relevant information;

Interpersonal conflicts affecting only the reporting person and the individuals concerned;

Information already publicly available or mere rumors.

11. INDEPENDENCE

The System Officer shall perform duties independently and autonomously, without receiving instructions from other bodies, and shall be provided with sufficient human and material resources.

12. TRANSPARENCY AND INTEGRITY OF INFORMATION

CUSA collaborators must provide complete, transparent, clear, and accurate information, enabling informed and autonomous decision-making.

13. INFORMATION PROCESSING

CUSA processes information in full compliance with confidentiality and privacy principles.

Appropriate policies and procedures are continuously updated to ensure:

Proper organizational separation of roles and responsibilities;

Information classification and appropriate safeguards at each stage;

Confidentiality agreements for personnel handling information.

Personal data not clearly relevant shall not be collected, or if collected inadvertently, shall be promptly deleted.

VI. RIGHTS AND GUARANTEES OF THE WHISTLEBLOWER

Persons submitting reports in accordance with Section III shall have the following rights:

To report anonymously or non-anonymously, with guaranteed confidentiality of identity.

To submit reports verbally or in writing.

To designate a secure address or email for communications.

To waive receiving communications.

To appear before the System Officer or A.A.I., assisted by legal counsel if desired.

To request secure videoconference appearances.

To exercise data protection rights.

To be informed of the status and outcome of the investigation.

If you would like, I can also prepare a formatted, publication-ready version in Word layout style suitable for corporate website upload or board approval.