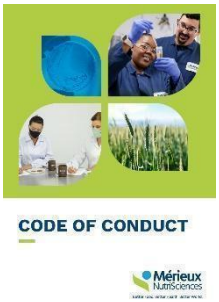

MÉRIEUX NUTRISCIENCES

COMPLIANCE POLICY

THIRD PARTY CONTROL POLICY

(January 2025 V.2)

1. INTRODUCTION

Mérieux NutriSciences is committed to the highest standards of business ethics and integrity. One of its most valuable assets is its reputation as a global leader committed to honest, legal, and ethical practices, as well as conducting business with integrity and trustworthiness.

Dealing with third parties naturally exposes the Group to certain financial, reputational and regulatory risks, including risks of corruption, money laundering or breach to human and environmental laws.

As such, Mérieux NutriSciences is aware that it could be held legally and financially liable and would as well suffer substantial reputational damages in case of fraudulent acts or significant breaches of ethics and compliance principles committed by any of its employees, directors or officers in their business relationships with third parties.

Engagement and control procedures for third parties are a key requirement of many international and national anti-corruption legislation such as the French Sapin 2 law and the US Foreign Corrupt Practices Act (FCPA), which are applicable to all Mérieux NutriSciences entities considering the US-based holding entity of the group (Mérieux NutriSciences Corporation) and its French controlling shareholder (Institut Mérieux).

This Compliance Policy sets out the minimum required declaration and control procedures to assess, validate, refuse or authorise under certain conditions any and all third parties before entering into business relationships with any Mérieux NutriSciences legal entities, to ensure Mérieux NutriSciences does business with third parties respecting ethics and compliance principles.

2. DECLARATION OF THIRD PARTIES

2.1 Third Parties to be declared

Any third party engaged in a business or financial relationship in whatever form and purposes with any entity of the Mérieux NutriSciences group, including but not limited to:

- suppliers of products or services, including business intermediaries (brokers, sales agents, etc.);
- customers;
- M&A and JV partners;
- accreditation bodies;
- recipients of any gifts, charitable donations or sponsorships

must be declared to the third party control system described in this policy (the "Third Party Control System") unless the same Third Party and the same business relationship have been already declared and cleared in the last 24 months preceding the date when the contract for the contemplated business relationship is signed.

2.2 Employee in charge of the Third Party declaration

The responsibility for declaring third parties to the Third Party Control System typically falls upon employees who are directly involved in the procurement or engagement process with those third parties.

This may include individuals in procurement departments, vendor management teams, legal departments, or any other relevant departments within the organisation.

2.3 Access to the Third Party Control System

The Third Party Control System has been designed and configured by the Group Internal Control and Risk Management department.

The Third Party Control System is or will be made available to all employees through the intranet page of each Mérieux NutriSciences country.

2.4 Information to be provided

The following information on the Third Party and the contemplated business relationship shall be provided by the relevant employee in charge of the transaction:

Information on the Third Party

- **Identity of the Third Party :** name, address and email of the Third Party's contact person;

- **Type of the Third Party**: customer or supplier, public or privately-owned entity, individual or legal entity, global or small company; and

- **Country of the Third Party** country where the Third Party is registered.

Information on the related business relationship

- **Involvement of Public Officers** in the proposed transaction (other than mandatory reporting of positive results imposed by health authorities in certain jurisdictions);

- **Selection process (for suppliers only)**: renewal of existing contracts without tender or tendering process involving several suppliers; and

- **Transaction scheme (for suppliers only)**: unusual remuneration model or methods, such as payment made to a bank account in a different country or to another third party.

3. SUPPLIER COMPLIANCE DECLARATION

The MXNS Code of Conduct and Compliance Declaration should be communicated and signed to all suppliers. The system is designed to automatically send this document to suppliers for digital signature.

4. THIRD PARTY RISK ASSESSMENT

4.1 First-level risk assessment by the Third Party Control System

The Third Party Control System will provide a first-level risk assessment, based on an automatic and objective review of the information provided by the declaring employee on the Third Party and the related business arrangement.

The risk assessment for each declared Third Party and related transaction will be determined on a scale between 0% (no ethical risk at all) and 100% (third party or transaction fully exposed to ethical risks):

- For a risk rating below 33% and unless specific features of the Third Party require a more advanced due diligence (see below), the risk will be considered low and the Third Party and the related business transaction shall be automatically **cleared** (see below); and

- In all other cases the declared Third Party and the related business transaction shall be subject to more advanced due diligence, as explained below.

4.2 Second-level risk assessment and decision by the Compliance Officer

The Compliance Officer in charge of the relevant Country (you may consult the list of compliance officers for each country in the intranet page dedicated to Compliance) shall then conduct a more detailed review of the risks involved.

He/she may involve the Local Ethics Committee and the Group Ethics Committee when relevant. He/She shall report his/her banned decision to the local Ethics & Compliance Committee.

Upon completion of the risk assessment, the Third Party and the related business transaction will fall within one of the following categories:

- **Cleared**, which means that no specific ethical or compliance risk has been detected, in which case the contractual arrangements negotiated with the Third Party can be finalised and signed;
- Under **Watch**, which means that some ethical or compliance risks have been detected and shall be managed with attention. Certain conditions may be imposed by the relevant Compliance Officer such as the inclusion of certain protective provisions in the agreement, or the necessity to redo the Third Party risk assessment regularly to monitor the evolution of the situation; or

- Under **Ban**, which means that some substantial ethical or compliance risks have been detected and that no business transaction with the Third Party can be completed. The decision to ban a Third Party must be approved by the Chief Compliance Officer.

5. IMPLEMENTATION AND MANAGEMENT OF THE THIRD PARTY CONTROL SYSTEM

Local management teams shall be responsible for implementing the Third Party Control System in their respective Mérieux NutriSciences legal entities, with the assistance and under the supervision of the Group Risk Manager and with the assistance of the Legal & Compliance team.

To ease its adoption by local teams, the Third Party Control System should be preferably integrated into the routine sales and procurement processes.

Each subsidiary may choose to adopt additional policies or procedures relating to the third party controls, as long as they do not conflict with this Policy and approval is obtained from the Chief Compliance Officer. Copies of any such policies and procedures should be sent to the Legal & Compliance Department.

The Third Party Control System is placed under the supervision of the local Managing Director assisted by the **local Ethics & Compliance Committee**, which shall be responsible for :

- the communication of this Compliance Policy to all concerned employees;
- the adaptation of the processes involving interactions with third parties (procure-to-pay, order-to-cash…);
- assigning roles and responsibilities to local teams; and,
- implementing independent and year-end controls to ensure that third parties are managed according to the policy.

The **Compliance Officer** (at Country or Region level) shall be in charge of the following duties:

- to timely conduct the second-level risk assessment on Third Party dossiers escalated to his/her review;
- to define the conditions imposed on Third Parties and related Transactions under **Watch** to the Local Ethics Committee; and

- to immediately inform the Chief Compliance Officer of any decision to **Ban** a Third Party.

6. PERSONAL DATA PROTECTION

In the context of the Third Party Control System, the Company may collect and process the following personal information:

- identity, functions and contact details of the employee who has made the Third Party declaration;
- identity, functions and contact details of the declared Third Party;
- facts reported as long as they allow a direct or indirect identification of the Third Party;
- elements collected as part of the additional integrity checks of the Third Party as long as they allow a direct or indirect identification of an individual;
- report describing the outcomes if the integrity checks as long as they allow a direct or indirect identification of an individual;
- actions taken to mitigate or monitor the identified Third Party risks as long as they allow a direct or indirect identification of an individual.

The Company undertakes to process and retain personal data in full compliance with applicable laws and regulations, including the EU General Data Protection Regulation.

The data are kept in the Third Party Control System in a secured folder, access to which is limited to the members of the local Ethics & Compliance Committee, and the Regional and Group Compliance Officers.

The following retention rules shall apply to data related to the Third Parties which are submitted to the system:

- Information on the Third Parties and the related business transaction shall remain available in the system to all users for a period of 2 years, provided however that personal data relating to such Third Parties shall only be accessible by the Risk Manager and the Compliance Officers;

- After 2 years, access to all data relating to Third Parties shall be restricted to the sole Director of internal Control & Risks in his capacity as super-administrator of the system; and

- All data relating to the Third Parties shall be destroyed 5 years after their submission to the system.

7. LOCAL REGULATIONS PROVIDING RULES DIFFERENT FROM THIS POLICY

This Policy is intended to provide a minimum standard by which to follow. To the extent any applicable law provides a higher or additional standard, such standards must be followed in addition to this Policy.

However, if complying with this Policy would conflict with any applicable law, you must follow the law and notify the Legal Affairs and Compliance Department of the conflict.

8. SANCTION STATEMENT

Failure to comply with the requirements of this Policy or its procedures will result in disciplinary action up to and including termination of employment.

9. RAISING QUESTIONS OR REPORTING IDENTIFIED RISKS

This Policy does not address every situation you may encounter at work. If there is a situation that you think may pose a risk and you are unsure about how to handle it, you should seek guidance. Support is available to you from the Risk Manager and your Compliance Officer.

* *
*