MÉRIEUX NUTRISCIENCES

COMPLIANCE POLICY

CONFIDENTIALITY

(October 2020 – V.1)

1. OBJECTIVES

Keeping information confidential is critical to our business and for our customers and suppliers. Unauthorized disclosure of confidential information may be very detrimental to the Company, its employees, customers, suppliers and stakeholders.

There may be however legitimate business reasons to share confidential information with a third party.

In this context, this Confidentiality Policy provides rules to ensure confidentiality of sensitive information and to protect the Company from the risk of unauthorized disclosure.

This Confidentiality Policy applies to all employees, directors and officers of the Company. It is the responsibility of managers to share these guidelines and recommendations with all employees of the Company.

2. CONFIDENTIAL INFORMATION

Confidential information are non-public proprietary information, whether in visual, oral, paper, or electronic form, trade secrets, know-how, materials and/or data related either to the Company or to a third party in business relationship with the Company (customers, suppliers, joint-venture partners and owners of potential target companies for acquisition).

Confidential information includes, but is not limited to:

- customer lists, pricing, call lists, contracts, and other confidential customer data;
- memoranda, summaries, notes, records, reports, analyses, and other confidential technical data;
- sketches, product specifications, plans (including strategic plans and marketing plans), drawings, software codes, and other confidential research and development data;
- know-how, methods, standard operating procedures, test traceability documents, test results as well as results of scientific research & development projects;
- standard operating procedures, processes and practices;
- lab and floor plans and work space and equipment configurations;
- information technology processes, practices, security standards and designs, and security protocols, administrator identities, and passwords;

- employee records, lists, contact information, and other confidential employee data (including payroll and personnel records);
- personal data of all our external contacts, including those of the volunteers participating to clinical or sensory studies;
- suppliers, pricing, costs, business processes and practices, and distribution methods;
- audit reports, financial data, accounting and financial practices, and technology;
- any information regarding the content of the agreements with the Company's lenders and insurers;
- confidential information regarding companies of the Institut Mérieux group, especially those who are publicly listed;
- any information regarding the Company's shareholders; and
- any other information that is not public knowledge and other material derived in whole or in part from confidential information.

If you want to know more about the confidentiality and privacy rules applicable to personal data, please refer to the Privacy Notice (available on MXNSConnect /Legal Affairs & Compliance / Personal Data Protection).

3. BASIC CONFIDENTIALITY RULES

Unlike trademarks, patents or domain names that are legally protected by an official registration, confidential information and know-how cannot be registered. Such rights are only protected as long as they are kept confidential.

For that reason, it is reminded to all employees of the Company the following basic principles:

- **When you do not know, assume information is confidential!**

Consult the Legal Affairs & Compliance Department if you are not sure and prior to using any sensitive information (compliance@mxns.com).

- **Do not use Confidential Information and logos of our clients and suppliers**

Information provided by our clients and suppliers in the frame of a specific business relationship cannot be used for any other purposes, unless you obtain first their prior written consent.

The same rule shall apply before any use of our clients and suppliers' trademarks and logos in any marketing communication.

- **Be careful with informal conversations!**

Lot of confidential Information are actually shared during internal meetings that take place in the premises of the Company (meeting rooms, employee's offices) or in shared or public space (open space, restaurant, train, flight, street, etc.). Discussing confidential information in shared or public spaces is inadvisable. Discuss stakeholders issues in private and only with employees authorized to receive such information.

Be also careful with discussions with friends and family members about work topics.

- **Be careful with documents you leave, print or send!**

When leaving a meeting room (private or public), no record including confidential information shall be left (from the paperboard to the bin). Do not leave unattended any confidential information visible on your desk, printer or work station and lock your computer when away from your desk. Be mindful when bringing files or papers to conference rooms or when printing documents.

As stated in the Data Security Policy, transfer of confidential information by digital means must be done only through the Company tools such as Company email, Company Drive.
Use of publicly available platforms such as Dropbox, Wetransfer or local equivalents are strictly prohibited. Backups of Company files are automatic through Google system. Backups on personal cloud based systems, external hard drives, thumb drives or equivalent are then not allowed.

- **Be careful with your computers and smart phones!**

Secure devices with security filters shall be used in public space. Your local IT support team can provide you with one. Renew your password on a regular basis. Consult the Data Security Policy for more information regarding the use of IT devices.
Recording meetings by video or microphone are not allowed unless previously agreed with participants.

- **Be careful during lab visits with videos and pictures!**

We shall always be mindful about what is shared on a public basis or can be caught by our clients and suppliers during any laboratory visit. In principle, pictures or videos shall be prohibited during laboratory visits. In addition, visits to laboratory parts where specific methods are performed shall always be first authorized by the country Managing Director and after a Non-Disclosure Agreement has been signed. Also, any external visitor shall be first registered on the visitors' register book before any visit.

- **Your confidentiality obligations will survive your stay in the Company!**

Employees are subject to a confidential undertaking with respect to any confidential information they have had access to in the course of their employment and this obligation survives the termination of employment.

4. GUIDELINES FOR DISCLOSURE OF CONFIDENTIAL INFORMATION

Disclosure of confidential information to external parties may be necessary in responses to requests for proposals, presentations to clients or suppliers, sales calls and other business exchanges.

It is reminded that it is strictly prohibited to share confidential information with any competitor of the Company.

- **Limit the disclosure to those who really need to know**

Access to, possession of, or other use of confidential information must be limited to only those individuals who have a reasonable need for such information in order to perform their job duties.

- **Check existing agreements signed with this business partner**

Before any disclosure of confidential information, check if the Company has already entered into any agreement with the third party that would include protective provisions on confidential information.

- **Sign a Non-Disclosure Agreement (NDA)**

When it is necessary to disclose confidential information, ensure that a NDA has been validly signed by both parties before sharing any information.

NDAs however do not relieve employees of the responsibility to use care in deciding what information to disclose.

NDA template is available on MXNS Connect/Legal Affairs and Compliance together with a NDA checklist providing guidelines. Please do not hesitate to use it on your own. If you still have questions on how to fulfill it, please contact the Legal Affairs & Compliance Department.

- **Contact Communication Department before any exchange with media**

No verbal or written exchange with the press shall be done without prior specific authorization from the Communication Department.

Disclosure of information to media representatives, specifically during any potential or already existing crisis situation has to be managed with the highest care. Please consult the Crisis Management Policy for more information about the Company guidelines to manage crisis and the recommended do's and don'ts.

- **Contact Legal Affairs and Compliance Department when disclosure is required by public authorities**

The Company may be requested or compelled to disclose certain confidential information by public authorities and the Company's failure to comply could be punishable by law. This can happen in case of subpoena, police investigations, audits and controls conducted by accreditation bodies or other government agencies.

When the Company receives a request for information, either its own or a client's, we must assess what is truly being asked so we do not run the risk of over or under disclosing. Many requests for documents from government agencies or regulators may seem like demands, but in fact, the Company may have the right to refuse to disclose the information. When in doubt, please consult Legal Affairs and Compliance Department (compliance@mxns.com).

Even when compelled by law, the Company still owes a duty of confidentiality to its employees, clients, etc. In each instance, we should confirm first whether or not the Company has a duty to notify a client prior to disclosure of its confidential information. We should also ensure that confidential treatment is given to the documents that are disclosed to the government agencies.

- **Contact Legal Affairs and Compliance Department in case of unauthorized disclosure of confidential obligations**

A confidential information breach shall never be underestimated. Unauthorized disclosure of confidential information could indeed lead to reputational and legal risks.

Thus, without fear of retaliation, employees are encouraged to report any confidential information breach to:

- the IT department, in case the breach is linked to the loss of electronic data or IT materials
- the Data Protection Officer of the Company (dpo@mxns.com) in case of breach of personal data
- the Legal Affairs & Compliance Department in all cases

5. 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.

6. 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.

7. 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 your manager and/or from your Legal Affairs and Compliance Department.

You may contact the Legal Affairs & Compliance Department by email at compliance@mxns.com. Your questions or concerns will remain confidential to fullest possible extent and will receive quick and appropriate follow-up.

* *
*