MÉRIEUX NUTRISCIENCES

COMPLIANCE POLICY

DATA SECURITY

(October 2020 – V.1)

1. OBJECTIVES

This policy aims at specifying the Users' obligations and responsibilities to ensure appropriate use of IT Resources and protection of Business and Personal Data within each of the Company entities.

This policy applies to the use of IT Resources to conduct the Company business or interact with internal networks and business systems, whether owned or leased by the Company, the User, or a third party.

This Data Security 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. DEFINITIONS

Personal Data means any information identifying, directly or indirectly, a natural person.

Business Data means any confidential information processed on behalf of the Company or one of its partners or customers.

Legislation on Data Protection means the European Regulation (EU) 2016/679 on the protection of Personal Data and any other national legislation relating to the protection of Personal Data applicable to this policy.

IT Resources include all:

- Computer hardware that provides or provides access to it : servers, computers, printers, tablets, smartphones, networks, channels and other computer equipment;
- Software stored on the User's computer or remotely accessible on the Company servers (Intranet) or external servers (Internet).

User means any person, whatever his status, using the Company IT Resources.

3. GENERAL PRINCIPLE

All IT Resources belong to the Company and are provided to Users for the sole purpose of being used for legitimate business purposes and in accordance with the Company policies, procedures, guidelines and instructions.

Personal use of IT Resources, including access to networks (Internet or local), is allowed as long as it remains appropriate, limited, legal, does not disrupt the operation of the Company and does not harm its reputation.

4. CONFIDENTIALITY AND PROTECTION

Information Protection

It is the responsibility of each User to properly manage, maintain and protect the security of the Company IT Resources and Business Data to which it has access or control in accordance with the Company' global information security guidelines available on MXNS Connect.

The information and processes used to transmit, store and access the Company IT Resources and Business Data may be confidential, commercially sensitive or subject to intellectual property rights.

Each User must also protect information belonging to third parties, such as customers, partners and suppliers, against unauthorized disclosure or other damages.

Access Settings

Accounts, logins, passwords, licenses or any other personal computer key device issued to the User are personal information.

Passwords are associated with a User-specific login and, when used correctly, prevent unauthorized access. Passwords must be kept strictly confidential and must never be disclosed, including to the manager or IT Support. Passwords should not be obvious and must contain letters, numbers and/or punctuation.

To ensure good security, the Company highly recommends each User to change his/her passwords every 120 days.

The User modifies or requests the renewal of his authentication means as soon as he suspects their disclosure.

The User must use his access rights only to access information or services necessary for the performance of the tasks entrusted to him and for which he is authorized.

The User must ensure the confidentiality of his computer station by locking his display during his absence. He also commits to ensure its proper function and in particular to restart his computer at least once a week attached to the internal network to allow the installation of enterprise security updates. Regular reboot is also required for tablets and phones.

The User must take care of the Company's portable equipment and ensure its protection whether within the Company or outside of it. If, outside the working hours, the User leaves the

portable device onsite, he undertakes to store it in a box or furniture locked. If the User takes the portable device with him, he commits not to leave it in an unattended place.

5. ACTIVITIES CONTROL

Automated Controls

All actions performed from the Company IT Resources may be subject to supervision. Each User is considered responsible for the actions performed under his computer identity.

Manual Control Procedure

In the event of a malfunction noted by the IT Department, a manual check and a verification of any operation performed by one or more Users may be carried out.

If an IT Resource has anomalies, the User must immediately inform the IT department via ssp.mxns.com.

6. E-MAIL

Electronic mail (nominative or not) is made available to the User for Business purposes and under User own responsibility.

Personal Use of E-mail

The User has the right to use occasionally his email for personal purposes. However, such messages should be clearly identified as private and personal messages (by adding the word "PERSONAL" or "PRIVATE" in the subject line or creating a specific directory dedicated to this content). All messages not identified as personal are presumed to be Business messages.

The Company Rights

While the Company is committed to always protect employees data, the Company shall nevertheless have the right to consult any User's emails in specific and critical circumstances and for legitimate purposes such as ensuring business continuity, securing the IT Resources or in case of police or administrative investigations.

In such exceptional situations, access to the User’s email box will be given only to the very few managers of the Company or external experts who really need to be involved in the resolution of the critical situation. Consultation rights extended to any third party to the User’s email box will never allow the Company to otherwise use the User’s email address. The Company shall, to the best possible extent, inform the User before extending any access rights to his/her email box to any third party. If such information cannot be given beforehand for confidential or practical reasons, the User will be informed as soon as possible afterwards. By accessing the Users emails, the Company undertakes not to consult messages clearly identified as “personal” as described in the previous sub-section.

User Departure

Before leaving the Company, it is the User's responsibility to remove all of his personal messages and to set up an out of office message indicating his departure from the Company. Access to the User's mail will be terminated at the end of his employment contract.

After the User's departure, the Company will be able to access his emails for a limited period of time if it is necessary in the context of business activities. The Company will not be able to use the User's email address and will only access it for consultation. The Company undertakes not to consult messages clearly identified as personal.

7. NETWORKS AND EXCHANGES PROTECTION

Use of Networks

The User agrees not to download or use for Business purposes, software or software packages whose license fees have not been paid, from suspicious sites, or prohibited by the Company. They agree not to deliberately disrupt the proper functioning of IT Resources and networks. If the Users wish to install software or software package or any application on IT Resources available, they agree to make a request to the IT Support service via ssp.mxns.com.

It is forbidden to connect Computer Resources other than those of the Company on the wired network of the Company locations. 'Guest' Wifi connections for personal or third-party equipment should be used if necessary. The IT Support has the right to interrupt the connection in case of risk for the Company or abuse.

Network Exchanges

The User shall exercise vigilance with regard to information sent and received (disinformation, computer virus, attempted fraud, chains, phishing, ...) and the websites on which they connect. Any suspicion or information received regarding a computer security problem must be reported to the IT Support department via ssp.mxns.com. It is forbidden to send, transmit, download, import, create or display e-mail, attachments or elements found on the Internet that are inappropriate and constitute a breach or a violation of the Company political values, procedures, directives or instructions.

Information electronically exchanged with third parties may, in legal terms, form a contract under certain conditions or be used for legal evidence. The User must, therefore, be careful about the kind of information they exchange electronically as well as for traditional mail. The User is informed that email is an administrative document recognized as evidence in case of litigation.

Using Storage Space

The Company storage space is Google Drive. The Company is only committed to recovering data stored on Google Drive.

Any storage of business files on servers or other applications than Google Drive must be discussed and approved upstream by the IT Department.

Storage devices (e.g: USB key, external hard drive) of unknown origin must not be connected to the Company computers and equipment. Use of storage devices must be temporary in order to limit any risk of data loss. Files stored on these devices must be deleted after use.

File transfer between the Company Users is done through dynamic links to Google Drive whose shares must be managed with care and not as email attachments.

File storage and private information

All data is considered Business except for data clearly marked by the User as private (adding the word "PERSONAL" or "PRIVATE"). Private file and information storage is tolerated on the computer and on Google Drive as long as it remains limited. It should not occupy servers and other applications.

Control Procedure in Case of Loss or Theft

In case of loss, theft of equipment or fraudulent use, the User must immediately inform the IT Department via ssp.mxns.com and report to the Local Data Champion/DPO through the Data Breach MXNS Connect link. The Data Champion shall consider the need to report the security breach to Local Authorities.

The IT Department can remotely delete all the Company data on the device and, at any time, proceed with the deletion of the Company data in case of suspicious use of a mobile device.

8. TELEPHONY

Personal Use of Telephony for Business Trips

Personal phone use is tolerated on business trips, provided it is justified by the ordinary needs of family life and used within reasonable limits. The User is informed that the Company can have access to the employee's activity history, both on landline and mobile devices, only for a legitimate reason as stated below. This history will be used for statistical purposes, internal control and verification within the limits provided by law.

9. 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 standards, 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.

10. 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.

11. 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 IT team support, from your manager and 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.

* *
*