GROUPE NUTRI

CYBERSECURITY POLICY

JANUARY 2024

TABLE OF CONTENTS

I. INTRODUCTION 3

II. OBJECTIVES 3

III. SCOPE OF APPLICATION 3

IV. DEFINITIONS 3

- *"confidential data* 3
- *"confidentiality incident* 4

V. EQUIPMENT SAFETY 4

VI. E-MAIL SECURITY 4

VII. DATA TRANSFER 5

VIII. DISCIPLINARY MEASURES 5

IX. POLICY ADMINISTRATION 5

The use of the masculine gender includes the feminine, and the singular includes the plural and vice versa. This presentation is intended to make the text easier to read.

I. INTRODUCTION

The risk of data theft, fraud and security breaches can have a negative impact on a company's systems, technological infrastructure and reputation. Therefore, Groupe Nutri Inc. and its business units, hereinafter referred to as **Groupe Nutri**, adopt this policy to help describe the security measures in place to ensure that information remains secure and protected.

II. OBJECTIVES

The aim of this policy is to :

- Protect Groupe Nutri's confidential data and technological infrastructure;
- Describe the protocols and guidelines governing cybersecurity measures;
- Define rules for professional and personal use of IT tools, and;
- Recall the disciplinary process for policy violations.

III. SCOPE OF APPLICATION

This policy applies to all members of the Board of Directors, permanent and part-time employees, subcontractors, volunteers, suppliers, trainees and any person having access to Groupe Nutri's electronic systems, information, software or computer tools.

IV. DEFINITIONS

For the purposes of this policy, the following expressions mean :

– *"confidential data*

  - Personal information;
  - Unpublished financial information;
  - Information on customers, suppliers and shareholders;
  - Potential customers and sales data;
  - Patents, business processes and new technologies;
  - Employee passwords, assignments and personal information;
  - Company contracts and legal documents.

– *"confidentiality incident*

- Unauthorized access to confidential data;
- Unauthorized use of confidential data;
- Unauthorized communication of confidential data;
- Loss of confidential data or any other breach in the protection of such information.

V. EQUIPMENT SAFETY

To ensure the security of all devices and information provided by the company, Groupe Nutri employees are required to :

- Keep all company-supplied devices, including tablets, computers and mobile devices, password-protected (at least 8 characters);
- Secure all supplied equipment before leaving the office;
- Obtain authorization from management or their immediate superior before removing equipment from company premises;
- Refrain from sharing private passwords with colleagues, personal acquaintances or anyone else;
- Regularly update the security of the software you use;
- Comply with IT department guidelines.

VI. E-MAIL SECURITY

Protecting email systems is a high priority, as emails can lead to data theft, fraud and the introduction of malware. Consequently, Groupe Nutri requires that all employees :

- Check the legitimacy of each e-mail before opening it, including the e-mail address and sender's name;
- Avoid opening suspicious e-mails and attachments, and clicking on links they contain;
- Check emails for significant grammatical errors;
- Contact the IT department in the event of suspicious e-mails.

VII. DATA TRANSFER

Groupe Nutri recognizes the security risks associated with the transfer of confidential data, both internally and externally. To minimize the risk of data theft, all employees must:

- Obtain the necessary authorization from management or their immediate superior before transferring confidential data;
- Refrain from transferring confidential data to employees and third parties who do not have access to it in the course of their duties;
- Only transfer confidential data to networks approved by Groupe Nutri;
- Verify the authorized recipient of confidential data, and ensure that appropriate security measures are in place;
- Immediately alert the IT department of any suspicious activity, including confidentiality incidents.

VIII. DISCIPLINARY MEASURES

Violation of this policy may result in disciplinary action up to and including termination of employment. Sanctions will be based on the seriousness of the violation. Unintentional violations may warrant a verbal warning, frequent violations of a similar nature may lead to a written warning, and intentional violations may result in suspension or dismissal, depending on the circumstances.

IX. POLICY ADMINISTRATION

Responsible body :	Board of Directors
Responsible for policy application :	Vice President, Human Resources
Approval date :	January 2024
Revision date :	n/a
Effective date of policy :	January 2024
Frequency of policy updates :	This policy is revised at the request of the Vice President, Human Resources or as needed.