Better Every Day

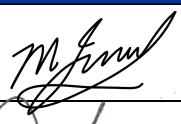
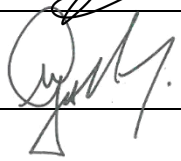
# INFORMATION TECHNOLOGY POLICIES

Montego
Pet Nutrition

## Policy Prepared by:

| NAME | DESIGNATION | SIGNATURE | DATE |
|---|---|---|---|
| Adelai van Heerden | HR Administrator<br>(Policies & Procedures) |  | 16/02/2023 |

## Policy Approved by:

| NAME | DESIGNATION | SIGNATURE | DATE |
|---|---|---|---|
| Morné Van Jaarsveld | Corporate Services Director |  | 03/04/2023 |
| Henry Galloway | HR Manager (Labour Relations) |  | 03/04/2023 |

## Document Change History

| VERSION | CHANGE DATE | DESCRIPTION |
|---|---|---|
| Version 2 | | |
| | | |
| | | |
| | | |
| | | |

## Contents

## INTRODUCTION

Information Technology (IT) is an integral and critical component of Montego Pet Nutrition (PTY) Ltd.'s (Montego Pet Nutrition) daily business. This Policy seeks to ensure that Montego Pet Nutrition's IT resources efficiently serve the primary business functions of Montego Pet Nutrition, provide security for Montego Pet Nutrition and members' electronic data, and comply with national and other regulations.

IT resources include:

- Hardware (computers, servers, peripherals)
- Software (licensed applications, operating systems)
- Network equipment (routers, *firewalls,* wiring)
- Data (both digital and hard copies)
- IT personnel

The integrity of all IT resources is extremely important to the successful operation of Montego Pet Nutrition's business.

All computer equipment, peripherals, software, and data are the property of Montego Pet Nutrition and are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of Montego Pet Nutrition computers will result in corrective action up to and including termination.

Employees should also be aware that any work completed on Montego Pet Nutrition computers is subject to monitoring and review, and they should not expect their communications to be private.

This Policy supersedes any previous IT Policies of Montego Pet Nutrition.

## POLICY STATEMENT

It is the policy of Montego Pet Nutrition to use IT resources in a cost-effective manner that safeguards member data and promotes accuracy, safety, reliability, and efficiency. The overriding goal of this Policy is to comply with all national and other regulations and to protect the integrity of the private and confidential member and business data that resides within Montego Pet Nutrition's technology infrastructure.

## DISCIPLINARY ACTION

Violation of any of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to loss of Montego Pet Nutrition Information Systems access privileges and may be subject to civil and criminal prosecution.

## REVIEW AND ACCEPTANCE

The Directors, Management and IT personnel shall review this Policy at least annually, making such revisions and amendments as deemed appropriate and indicating approval and the revision date thereof in the Document Change History.

All Montego Pet Nutrition employees are responsible for the review and acceptance of this Policy annually. Appropriate communications by way of reminder will be sent periodically through the official communication platforms along with instructions for acceptance.

This document will be made digitally available for employees to review when needed.

**The following Policies should be signed before allowing access to Montego Pet Nutrition information systems: Policies: 2, 3, 4, 5, 6, 8, 13, 15, 18, 21, 29 & 31.**

**Additionally, employees working remotely will need to review the following Policies: 1, 16 & 23.**

**The IT Department will inform you if any additional Policies may apply to your function.**

**A signed *User Acceptance Form* (Annexure A) will be received and retained by the Human Resources Department.**

## USER ACCEPTANCE FORM
## IT POLICIES

I, _____ with ID or Passport Number: _____

Confirm that I have read and understood the IT Policies applicable to my position and work requirements and accept the following sections *(please tick and initial)*.

| √ | Section – Policy Detail | Initial |
|---|---|---|
| | Policy 1 - Movement of IT Assets | |
| | Policy 2 – Acceptable Use of Information Systems | |
| | Policy 3 – Account Management | |
| | Policy 4 – Anti-Virus | |
| | Policy 5 – MPN Owned Mobile Device Acceptable Use and Security | |
| | Policy 6 – Clean Desk | |
| | Policy 7 – E-Commerce | |
| | Policy 8 – E-mail | |
| | Policy 9 – Firewall | |
| | Policy 10 – Hardware and Electronic Media Disposal | |
| | Policy 11 – Security Incident Management | |
| | Policy 13 – Internet | |
| | Policy 14 – Log Management | |
| | Policy 15 – Safeguarding Member Information | |
| | Policy 16 – Network Security and VPN Acceptable Use | |
| | Policy 17 – Personal Device Acceptable Use and Security (BYOD) | |
| | Policy 18 – Password | |
| | Policy 19 – Patch Management | |
| | Policy 20 – Physical Access Control | |
| | Policy 21 – Cloud Computing Adoption | |
| | Policy 22 – Server Security | |
| | Policy 23 – Social Media Acceptable Use | |

| | | |
|---|---|---|
| | Policy 24 – Systems Monitoring and Auditing | |
| | Policy 25 – Vulnerability Assessment | |
| | Policy 26 – Website Operation | |
| | Policy 27 – Workstation Configuration Security | |
| | Policy 28 – Server Virtualisation | |
| | Policy 29 – Telecommuting | |
| | Policy 30 – Internet of Things | |
| | Policy 31 – Wireless (Wi-Fi) Connectivity | |

I understand that I am bound to the rules and guidelines laid out in this document.
I acknowledge that I fully understand this document and that any queries that I had about its contents have been resolved before I signed this form.

Signed on the _____ day of _____ 20 _____ at _____

_____ _____

SIGNATURE: EMPLOYEE SIGNATURE: HR REPRESENTATIVE

## Policy 1 - MOVEMENT OF IT ASSETS

### Definitions

| TERM | DEFINITION |
|---|---|
| **IT Asset:** | An IT Asset is defined in this document to be any piece of hardware that provides significant service to the end-user function, irrespective of the financial value. |
| **Asset Tag:** | A barcoded sticker clearly showing the asset number of the hardware. |

### Overview

As explained in the New User Orientation process; IT assets are assigned to the end user's digital identity, and care and accountability remain the responsibility of the end user. Assets are monitored digitally and recorded by their unique serial numbers.

These assets are meant to be office-bound unless specifically designed to be mobile, such as laptops and tablets. Special rules, as laid out in this document, apply to the removal of no moveable assets from any Montego Pet Nutrition premises.

### Purpose

The purpose of this Policy is to outline the acceptable use of computer equipment outside of the premises of Montego Pet Nutrition. These rules are in place to protect the authorised user and Montego Pet Nutrition. Inappropriate use exposes Montego Pet Nutrition to damage and loss of IT assets.

### Scope

This Policy applies to the use of electronic and computing devices to conduct Montego Pet Nutrition business outside of official business premises.

All employees, volunteers, directors, contractors, consultants, temporaries, and other workers at Montego Pet Nutrition, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding the appropriate use of these electronic devices under Montego Pet Nutrition policies and standards, local laws, and regulations.

## Policy Detail

### Ownership of Electronic Equipment

All electronic equipment purchased or leased by Montego Pet Nutrition or otherwise under the custody and control of Montego Pet Nutrition are the property of Montego Pet Nutrition until disposed of in terms of the *Hardware and Electronic Media Disposal Policy*.

### Movement of IT Assets and Equipment

- IT assets may not be removed from the premises unless authorised by the IT Manager or his designated representative. This authorisation will be in the form of a *Montego IT Helpdesk Request*.
- Removed assets must be marked with an Asset Tag. Untagged assets may not be removed.
- The removal can only be requested through a *Helpdesk Ticket* and assets must be returned on the next business day after the loan period, unless the item has been sent away for repairs, in which case it should be returned as soon as possible.
- Users must submit written approval from their line Manager permitting them to remove assets.
- By removing the asset from the premises, the user acknowledges the increased risk of theft, loss, or damage. Thus, the user must take all possible steps to protect the equipment at all times.
- Any loss or damage of the asset is to be reported in writing to the *Helpdesk* as soon as possible.
- Removal of assets is subject to availability.

### Review and Acceptance

Montego Pet Nutrition employees who required loan equipment are responsible for the review and acceptance of *IT Policy 1 - Movement of IT Assets* upon approval to remove IT assets.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 2 – ACCEPTABLE USE OF INFORMATION SYSTEMS

### Definitions

| TERM | DEFINITION |
|---|---|
| **Information Systems:** | All electronic means used to create, store, access, transmit and use data, information, or communications in the conduct of administrative, instructional, research, or service activities. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information. |
| **Authorised User:** | An individual or automated application or process that is authorised access to the resource by the system owner, following the system owner's procedures and rules. |
| **Extranet:** | An *intranet* that is partially accessible to authorised persons outside of a company or organisation. |

### Overview

Data, electronic file content, information systems, and computer systems at Montego Pet Nutrition must be managed as valuable organisational resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to Montego Pet Nutrition's established culture of openness, trust, and integrity. IT is committed to protecting Montego Pet Nutrition's authorised users, partners, and the company from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/*Intranet*/*Extranet*-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web (www) browsing, and File Transfer Protocol (FTP) are the property of Montego Pet Nutrition. These systems are to be used for business purposes in serving the interests of Montego Pet Nutrition and its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every Montego Pet Nutrition employee, consultant, contractor, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct activities accordingly.

## Policy Detail

### Ownership of Electronic Files

All electronic files created, sent, received, or stored on Montego Pet Nutrition owned, leased, or administered equipment or otherwise under the custody and control of Montego Pet Nutrition are the property of Montego Pet Nutrition.

### Privacy

Electronic files created, sent, received, or stored on Montego Pet Nutrition owned, leased, or administered equipment, or otherwise under the custody and control of Montego Pet Nutrition are not private and may be accessed by Montego Pet Nutrition IT employees at any time without the knowledge of the user, sender, recipient, or owner. Electronic file content may also be accessed by appropriate personnel following directives from Human Resources or the Directors.

### General Use and Ownership

- Access requests must be authorised and submitted by Supervisors for employees to gain access to computer systems.
- Authorised users are accountable for all activity that takes place under their username.
- Authorised users should be aware that the data and files they create on the corporate systems immediately become the property of Montego Pet Nutrition. Because of the need to protect Montego Pet Nutrition's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to Montego Pet Nutrition.
- For security and network maintenance purposes, authorised individuals within Montego Pet Nutrition IT Department, or designee, may monitor equipment, systems, and network traffic at any time.
- Montego Pet Nutrition's IT Department, or designee, reserves the right to audit networks and systems periodically to ensure compliance with this Policy.
- Montego Pet Nutrition's IT Department, or designee, reserves the right to remove any non-business-related software or files from any system. Examples of non-business-related software or files include, but are not limited to, games, instant messengers, private email accounts, music files, image files, freeware, and shareware.

### Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this Policy and the following Policies:

- Policy 3 - Account Management
- Policy 4 - Anti-Virus
- Policy 5 - Montego Pet Nutrition Owned Mobile Device Acceptable Use and Security

- Policy 8 - E-mail
- Policy 13 - Internet
- Policy 15 - Safeguarding Member Information
- Policy 17 - Personal Device Acceptable Use and Security
- Policy 18 - Password
- Policy 21 - Cloud Computing Adoption
- Policy 29 - Telecommuting
- Policy 31 - Wireless (Wi-Fi) Connectivity

System-level and user-level passwords must comply with the *Password Policy*.

Authorised users must not share their Montego Pet Nutrition login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), or similar information or devices used for identification and authentication purposes. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Under special circumstances, users may need to share such details with their manager or IT employees for the maintenance of their IT equipment. Should the user refuse or be unavailable, IT will reset these details. It is recommended that the user change their password, where possible, after such interactions to retain their security integrity. Remote sessions should always be supervised, and access codes reset afterwards.

Authorised users may access, use, or share Montego Pet Nutrition proprietary information only to the extent it is authorised and necessary to fulfil the users' assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at ten (10) minutes or less.

All users must lock down their PCs, laptops, and workstations by locking when the host will be unattended for any amount of time.

Montego Pet Nutrition proprietary information stored on electronic and computing devices, whether owned or leased by Montego Pet Nutrition, the employee or a third party, remains the sole property of Montego Pet Nutrition. All proprietary information must be protected through legal and technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorised disclosure of Montego Pet Nutrition proprietary information to their immediate Supervisor and/or the IT Department, or designee.

All users must report any weaknesses in Montego Pet Nutrition computer security and any incidents of possible misuse or violation of this agreement to their immediate Supervisor and/or the IT Department, or designee.

Authorised users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or *Trojan Horse* codes.

Users must not intentionally access, create, store, or transmit material that Montego Pet Nutrition may deem to be offensive, indecent, obscene, or in any way tarnish the reputation of Montego Pet Nutrition.

Under no circumstances is an employee, Director, contractor, consultant, or temporary employee of Montego Pet Nutrition authorised to engage in any activity that is illegal under local, national, or international law while utilising Montego Pet Nutrition-owned resources.

### Unacceptable Use

The following activities are prohibited by users, with no exceptions:

Violations of the rights of any person or company protected by Copyright, Trade Secret, Patent, or other Intellectual Property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Montego Pet Nutrition.

- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Montego Pet Nutrition or the end-user does not have an active license are prohibited. Users must report unlicensed copies of installed software to IT.
- Introduction of malicious programs into the network or server (e.g., viruses, *worms*, *Trojan Horses*, e-mail bombs, etc.).
- Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
- Using a Montego Pet Nutrition computing asset to actively engage in procuring or transmitting material that violates Sexual Harassment or Hostile Workplace Laws and Policies.
- Attempting to access any data, electronic content, or programs contained on Montego Pet Nutrition systems for which they do not have authorisation, explicit consent, or implicit need for their job duties.
- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of Montego Pet Nutrition IT.
- Installing or using non-standard shareware or freeware software without Montego Pet Nutrition IT approval.
- Installing, disconnecting, or moving any Montego Pet Nutrition-owned computer equipment and peripheral devices without the prior consent of Montego Pet Nutrition's IT Department, or designee.

- Purchasing software or hardware, for Montego Pet Nutrition use, without prior IT compatibility review.
- All licensing information is to be made available to the IT department and kept in a secure register.
- Purposely engaging in activities that may:
  - degrade the performance of information systems.
  - deprive an authorised Montego Pet Nutrition user of valid access to a Montego Pet Nutrition resource.
  - obtain extra resources beyond those allocated, or
  - circumvent Montego Pet Nutrition computer security measures.
- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, Montego Pet Nutrition users must not run *spyware, adware, password cracking programs, packet sniffers, port scanners,* or any other non-approved programs on Montego Pet Nutrition information systems. Montego Pet Nutrition IT Department, or designee, is the only department authorised to perform these actions with the approval of Senior Management.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's session, via any means, locally or via the Internet/*Intranet*/*Extranet*.
- Access to the Internet at home, from a Montego Pet Nutrition-owned computer, must adhere to all the same policies that apply to use from within Montego Pet Nutrition facilities. Authorised users must not allow family members or other non-authorised users to access Montego Pet Nutrition computer systems.

Montego Pet Nutrition information systems must not be used for personal benefit.

### Incidental Use

As a convenience to Montego Pet Nutrition employees, incidental use of information systems is permitted. The following restrictions apply:

- Authorised users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate Supervisors are responsible for supervising their employees regarding excessive use.
- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to Montego Pet Nutrition-approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Montego Pet Nutrition without prior approval of Management.
- Incidental use must not interfere with the normal performance of an employee's work duties.

- No files or documents may be sent or received that may cause legal action against, or embarrassment to, Montego Pet Nutrition.
- Storage of personal email messages, voice messages, files, and documents within Montego Pet Nutrition's information systems must be nominal.
- All messages, files, and documents – including personal messages, files, and documents – located on Montego Pet Nutrition information systems are owned by Montego Pet Nutrition, may be subject to open records requests, and may be accessed following this Policy.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 2 - Acceptable Use of Information Systems* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 3 – ACCOUNT MANAGEMENT

### Definitions

| TERM | DEFINITION |
|---|---|
| **Account:** | Any combination of a User ID (sometimes referred to as a username) and a password that grants an authorised user access to a computer, an application, the network, or any other information or technology resource. |
| **Security Administrator:** | The person charged with monitoring and implementing security controls and procedures for a system. Whereas Montego Pet Nutrition may have one Information Security Officer, Technical Management may designate several Security Administrators. |
| **System Administrator:** | The person responsible for the effective operation and maintenance of information systems, including the implementation of standard procedures and controls to enforce an organisation's Security Policy. |

### Overview

Computer accounts are the means used to grant access to Montego Pet Nutrition's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for Montego Pet Nutrition usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

### Purpose

The purpose of this Policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at Montego Pet Nutrition.

### Audience

This Policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at Montego Pet Nutrition, including all personnel affiliated with third parties with authorised access to any Montego Pet Nutrition information system.

## Policy Detail

### Accounts

- All accounts created must have an associated written request and Management approval that is appropriate for the Montego Pet Nutrition system or service.
- All accounts must be uniquely identified using the assigned username.
- Shared accounts on Montego Pet Nutrition information systems are not permitted.
- Reference the *Employee Access During Leave of Absence Agreement* for removing an employee's access while on a leave of absence or vacation.
- All default passwords for accounts must be constructed per Montego Pet Nutrition *Password Policy*.
- All accounts must have a password expiration that complies with Montego Pet Nutrition *Password Policy*.
- Concurrent connections may be limited for technical or security reasons.
- **All accounts must be disabled immediately upon notification of any employee's termination or suspension.**

### Account Management

The following items apply to System Administrators or other designated employees:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual's account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorise, perform, review, and audit a single transaction on sensitive systems.
- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.
- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.
- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third-party account is found to be inactive for thirty (30) days, the owners (of the account) and their manager will be notified of pending disablement.
- A list of accounts, for the systems they administer, must be provided when requested by authorised Montego Pet Nutrition management.
- An independent audit review may be performed to ensure the accounts are properly managed.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 3 - Account Management* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

# EMPLOYEE ACCESS DURING LEAVE OF ABSENCE AGREEMENT

This *Employee Access During Leave of Absence Agreement* is entered into between the Users of Montego Pet Nutrition (Pty) Ltd. (Montego Pet Nutrition). The effective date of this agreement is kept on record for Montego Pet Nutrition's Information Technology (IT) Department for audit purposes.

The parties agree as follows:

**Eligibility**

- That user information is shared only between the parties of this agreement, for the duration of this agreement.
- That user information only is shared as a necessity, stemming from a license, time, equipment, or data constraints, and not out of convenience.
- That the temporary (or secondary) user is a permanent employee of Montego Pet Nutrition.
- That the temporary (or secondary) user is subject to the same rules and policies as the primary user.

**Security Considerations and Acceptable Use**

- The Primary User must reset their password upon return in compliance with the *Password Policy*.
- Wherever possible, this form is to be completed before the leave of absence occurs.
- In the case of emergency or unexpected absences, this form is to be completed immediately upon the primary User's return to service.
- The Human Resources Manager, or their designee, may in special circumstances, sign *in absentia* for either party.
- The signed form is to be kept by the Human Resources Department on the employee's permanent record for audit purposes.

**Support**

- The Human Resources Manager, or their designee, may ask IT to reset the primary User's password before first access through a *HelpDesk Ticket*.

**Agreement:**

I, _____ (Primary User) with Employee Number: _____

hereby confirm access to my account has been given in my absence to

_____ (Secondary User) with Employee Number: _____

From (Date and Time): _____

To (Date and Time): _____

_____ _____

SIGNATURE: PRIMARY USER DATE

_____ _____

SIGNATURE: SECONDARY USER DATE

_____ _____

SIGNATURE: HR REPRESENTATIVE DATE

## Policy 4 – ANTI-VIRUS

### Definitions

| TERM | DEFINITION |
|---|---|
| **Virus:** | A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros. |
| **Trojan Horse:** | Destructive programs, usually viruses or *worms*, which are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a *Trojan Horse* program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a website or download site. |
| **Worm:** | A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some *worms* use security threats over networks to spread themselves against the wishes of the system owners and disrupt networks by overloading them. A *worm* is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all. |
| **Spyware:** | Programs that install and gather information from a computer without permission and report the information to the creator of the software or one or more third parties. |
| **Malware:** | Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, *worm*, or *Trojan Horse*. |
| **Adware:** | Programs that are downloaded and installed without the user's consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exceptions after installation. |
| **Keyloggers:** | A computer program that captures the keystrokes of a computer user and stores them. Modern *keyloggers* can store additional information, such as images of the user's screen. Most malicious *keyloggers* send this data to a third party remotely (such as via email). |

| | |
|---|---|
| **Ransomware:** | A type of *malware* that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid. |
| **Server:** | A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running another client (and server) program. |
| **Security Incident:** | In information operations, a security incident is an assessed event of attempted entry, unauthorised entry, or an information attack on an automated information system. It includes unauthorised probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent. |
| **e-mail:** | Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application. |
| **Anti-virus:** | A program that scans, blocks, and neutralises any and more of the threats defined above. |

## Overview

*Malware* threats must be managed to minimize the amount of downtime realised by Montego Pet Nutrition's systems and prevent risk to critical systems and member data.

This Policy is established to:

- Create prudent and acceptable practices regarding anti-virus management
- Define key terms regarding *malware* and anti-virus protection
- Educate individuals, who utilise Montego Pet Nutrition system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and *malware*, as well as anti-virus and anti-*malware*, may be used interchangeably.

## Purpose

This Policy was established to help prevent infection of Montego Pet Nutrition computers, networks, and technology systems from *malware* and other malicious code. This Policy is intended to help prevent damage to user applications, data, files, and hardware.

## Audience

This Policy applies to all computers connecting to the Montego Pet Nutrition network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC-based equipment connecting to the Montego Pet Nutrition network.

## Policy Detail

- All computer devices connected to the Montego Pet Nutrition network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.
- The virus protection software must not be disabled or bypassed without IT approval.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each file server, attached to the Montego Pet Nutrition network, must utilise Montego Pet Nutrition IT-approved virus protection software, and be set up to detect and clean viruses that may infect Montego Pet Nutrition resources.
- Each e-mail gateway must utilise Montego Pet Nutrition IT-approved e-mail virus protection software.
- All files on computer devices will be scanned periodically for *malware*.
- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the *Helpdesk*.
- If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the Montego Pet Nutrition network until the infection has been removed.

## Users should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.
- Delete spam, chain, or other junk mail without opening or forwarding the item.
- Never download files from unknown or suspicious sources.
- Always scan removable media from an unknown or non-Montego Pet Nutrition source (such as a CD or USB from a vendor) for viruses before using it.
- Back up critical data regularly and store the data in a safe place. Critical Montego Pet Nutrition data must be saved to provided cloud-based sources and are backed up periodically. Contact Montego Pet Nutrition IT Department, or designee, for details.

- Because new viruses are discovered every day, users should periodically check the *Anti-Virus Policy* for updates. Montego Pet Nutrition IT Department, or designee, should be contacted for updated recommendations.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *Policy 4 - Anti-Virus Policy* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 5 – MONTEGO PET NUTRITION OWNED MOBILE DEVICE ACCEPTABLE USE AND SECURITY

### Definitions

| TERM | DEFINITION |
|---|---|
| **Clear text:** | Unencrypted data. |
| **Full disk encryption:** | Technique that encrypts an entire hard drive, including the operating system and data. |
| **Key:** | Phrase used to encrypt or decrypt data. |

### Overview

Acceptable use of Montego Pet Nutrition-owned mobile devices must be managed to ensure that employees, management, and related constituents who use mobile devices to access Montego Pet Nutrition's resources for business do so safely and securely. This Policy is designed to maximise the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

### Purpose

This Policy defines the standards, procedures, and restrictions for end-users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of Montego Pet Nutrition's direct control. This Mobile Device Policy applies to but is not limed to, any mobile device issued by Montego Pet Nutrition that contains stored data owned by Montego Pet Nutrition and all devices and accompanying media that fit the following device classifications:

- Laptops, Notebooks, and Hybrid devices
- Tablets
- Mobile/cellular phones including Smartphones
- Any Montego Pet Nutrition-owned mobile device capable of storing corporate data and connecting to an unmanaged network

This policy addresses a range of threats to, or related to, the use of Montego Pet Nutrition data:

| Threat | Description |
|---|---|
| **Loss:** | Devices used to transfer, or transport work files could be lost or stolen. |
| **Theft:** | Sensitive corporate data is deliberately stolen and sold by an employee. |

| | |
|---|---|
| **Copyright:** | Software copied onto a mobile device could violate licensing. |
| **Malware:** | Virus, *Trojan Horse*, *Worms*, *Spyware*, and other threats could be introduced via a mobile device. |
| **Compliance:** | Loss or theft of financial and/or personal and confidential data could expose Montego Pet Nutrition to the risk of non-compliance with various identity theft and privacy laws. |

The addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden. This Policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Montego Pet Nutrition network.

## Audience

This Policy applies to all Montego Pet Nutrition employees, including full and part-time staff, and managers who utilise company-owned mobile devices to access, store, back up, relocate or access any organisation or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Montego Pet Nutrition has built with its members, suppliers, and other constituents. Consequently, employment at Montego Pet Nutrition does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

## Policy Detail

This Policy applies to any corporate-owned hardware and related software that could be used to access corporate resources. The overriding goal of this Policy is to protect the integrity of the private and confidential member and business data that resides within Montego Pet Nutrition's technology infrastructure.

This Policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to Montego Pet Nutrition's public image. Therefore, all users employing a Montego Pet Nutrition-owned mobile device, connected to an unmanaged network outside of Montego Pet Nutrition's direct control, to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

## Affected Technology

Connectivity of all mobile devices will be centrally managed by Montego Pet Nutrition's IT Department, or designee, and will utilise authentication and strong encryption measures. To protect Montego Pet Nutrition's infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

## Responsibilities

It is the responsibility of any employee of Montego Pet Nutrition, who uses a Montego Pet Nutrition-owned mobile device to access corporate resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any Montego Pet Nutrition-owned mobile device that is used to conduct Montego Pet Nutrition business be utilised appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.

Based on this, the following rules must be observed:

## Access control

- IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to Montego Pet Nutrition and Montego Pet Nutrition-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts Montego Pet Nutrition's systems, data, users, and members at risk.
- Before initial use on the Montego Pet Nutrition network or related infrastructure, **all mobile devices must be registered with IT**. Montego Pet Nutrition will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored in the *IT Document Storage* location. Devices that are not on this list may not be connected to Montego Pet Nutrition infrastructure. To find out if a preferred device is on this list, an individual should contact Montego Pet Nutrition IT Department, or designee, through the *Helpdesk*. Although IT currently allows only listed devices to be connected to Montego Pet Nutrition infrastructure, it reserves the right to update this list in the future **(Annexure B)**.
- **End users** who wish to connect such devices to non-corporate network infrastructure to gain access to Montego Pet Nutrition data **must employ**, for their devices and related infrastructure, **a company-approved personal anti-virus program, firewall** and any other security measure deemed necessary by the IT Department, or designee. Montego Pet Nutrition data is not to be accessed on any hardware that fails to meet Montego Pet Nutrition's established enterprise IT Security Standards.
- All mobile devices attempting to connect to the Montego Pet Nutrition network through an unmanaged network (i.e., the Internet) will be inspected using technology centrally managed by Montego Pet Nutrition's IT Department, or designee. Devices that are not corporate issued are not in compliance with IT's *Security Policies* and

will not be allowed to connect except by a provision of the *Personal Device Acceptable Use and Security Policy*. Montego Pet Nutrition-owned laptop computers may only access the corporate network and cloud data using a *Secure Socket Layer* (SSL) or *Internet Protocol Security* (IPsec) protocol.

- **Employees** using mobile devices and related software for network and data access **will**, without exception, **use secure Data Management Procedures**. All mobile devices containing stored data owned by Montego Pet Nutrition **must use an approved method of encryption** to protect data. Laptops must employ full drive encryption with an approved software encryption package. No Montego Pet Nutrition data may exist on a laptop in *cleartext*. All mobile devices must be protected by a **strong password.** Refer to Montego Pet Nutrition's *Password Policy* for additional information. **Employees agree to never disclose their passwords to anyone**, particularly to family members, if business work is conducted from home. In some instances, IT Support may request login information. These are the exception, and sharing these details is entirely at the user's discretion and subject to the guideline listed in the *Password Policy*.
- All keys used for encryption and decryption must meet the complexity requirements described in Montego Pet Nutrition's *Password Policy*.
- All users of corporate-owned mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain Montego Pet Nutrition data. Users with devices that are not issued by Montego Pet Nutrition must adhere to the *Personal Device Acceptable Use and Security Policy.*
- Passwords and confidential data should not be stored on unapproved or unauthorised non-Montego Pet Nutrition devices.
- Any corporate-owned mobile device that is being used to store Montego Pet Nutrition data must adhere to the authentication requirements of Montego Pet Nutrition's IT Department or designee. In addition, all hardware security configurations must be preapproved by Montego Pet Nutrition's IT Department, or designee, before any enterprise data-carrying device can be connected to it.
- IT will manage *Security Policies*, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with by Montego Pet Nutrition's overarching *Security Policy*.
- Employees, Partners, and temporary staff will follow all Enterprise-sanctioned Data Removal Procedures to permanently erase company-specific data from such devices once their use is no longer required. For assistance with detailed Data Wipe Procedures for mobile devices, an individual should contact Montego Pet Nutrition IT Department, or designee, through the *Helpdesk*. This information is found in the *IT Document* Storage location.
- In the event of a lost or stolen mobile device, it is incumbent on the user to report this to IT immediately. Montego Pet Nutrition shall employ remote wipe technology to remotely disable and delete any data stored on a Montego Pet Nutrition PDA or

cell phone that is reported lost or stolen. If the device is recovered, it can be submitted to IT for re-provisioning.

- IT maintains the process for patching and updating mobile devices. A device's *firmware* operating system **must** be up to date to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the user for computing platforms (i.e., laptops). Users can contact the *Helpdesk* if they need assistance.
- IT maintains the process for security audits on mobile devices. Since handheld devices are not completely under the control of Montego Pet Nutrition, a periodic audit will be performed to ensure the devices are not a potential threat to Montego Pet Nutrition.

## Help and Support

- Montego Pet Nutrition's IT Department, or designee will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department, or designee.
- Employees, Management, and temporary staff will not make modifications of any kind to Montego Pet Nutrition owned and installed hardware or software without the express approval of Montego Pet Nutrition's IT Department, or designee. This includes, but is not limited to, any reconfiguration of the mobile device.
- IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the Montego Pet Nutrition network.

## Organisational Protocol

- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. To identify unusual usage patterns or other suspicious activity, the end-user agrees to and accepts that his or her access and/or connection to Montego Pet Nutrition's Networks may be monitored to record dates, times, duration of access, etc. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Montego Pet Nutrition's highest priority.
- The **end-user agrees to immediately report**, to his/her manager and Montego Pet Nutrition's IT Department, or designee, **any incident or suspected incidents of unauthorised data access,** data loss, and/or disclosure of Montego Pet Nutrition resources, databases, networks, etc.
- Montego Pet Nutrition will not reimburse employees if they choose to purchase their own mobile devices except under the *Personal Device Acceptable Use and Security Policy*. Users will not be allowed to expense mobile network usage costs.
- Montego Pet Nutrition prohibits the unsafe and unlawful use of mobile devices, including but not limited to, texting, emailing, or any distracting activity while driving,

and requires this audience to comply with all laws in which one is currently operating, regarding same, hands-free requirements, etc.

- Before being granted a device and access to Montego Pet Nutrition resources, a mobile device user must understand and accept the terms and conditions of this policy.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 5 - Montego Pet Nutrition Owned Mobile Device Acceptable Use and Security* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

# MONTEGO PET NUTRITION OWNED MOBILE DEVICE AGREEMENT

This *Montego Pet Nutrition Owned Mobile Device Agreement* is entered into between the User and Montego Pet Nutrition (Pty) Ltd. (Montego Pet Nutrition), after the effective date this agreement is executed by Montego Pet Nutrition's Information Technology (IT) Department.

The parties agree as follows:

**Eligibility**

- The use of a Montego Pet Nutrition-supported mobile device by the User for Montego Pet Nutrition business is a privilege granted to the User, by management approval, per the *Montego Pet Nutrition Owned Mobile Device Acceptable Use and Security Policy.* If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to Montego Pet Nutrition and ensure the data remains secure.
- In the event of a security breach or threat, Montego Pet Nutrition reserves the right, without prior notice to the User, to disable or disconnect some or all Montego Pet Nutrition services related to the connection of a Montego Pet Nutrition-owned mobile device to the Montego Pet Nutrition network.

**Security Considerations and Acceptable Use**

- Compliance by the User with the following Montego Pet Nutrition Policies, published elsewhere and made available, is mandatory:
  - Acceptable Use of Information Systems
  - Montego Pet Nutrition Owned Mobile Device Acceptable Use and Security
  - and other related policies including, but not limited to, Anti-Virus, e-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.
- The User of the Montego Pet Nutrition-owned mobile device shall not remove sensitive information from the Montego Pet Nutrition Network, attack Montego Pet Nutrition assets, or violate any of the *Security Policies* related to the subject matter of this Agreement.

**Support**

Montego Pet Nutrition will offer the following support for the Montego Pet Nutrition-owned mobile device:

- Connectivity to Montego Pet Nutrition servers, including email and calendar
- Security services, including policy management, password management

- Decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), and carrier network or system outages that result in a failure of connectivity to the Montego Pet Nutrition Network.
  The User assumes full liability including, but not limited to, an outage or crash of any or all of the Montego Pet Nutrition network, programming and other errors, *bugs*, viruses, and other software or hardware failures resulting in the partial or complete loss of data, or which render the mobile device inoperable.

**Device Description**:

| | |
|---|---|
| **Device Make:** | |
| **Device Model:** | |
| **Device Serial Number:** | |
| **Device IMEI Number:** | |

SIGNATURE: USER _____ DATE _____

SIGNATURE: IT DEPARTMENT MANAGEMENT _____ DATE _____

## Policy 6 – CLEAN DESK

### Overview

Montego Pet Nutrition is committed to protecting the privacy of its employees and members and shall protect the confidentiality of non-public information consistent with laws. Montego Pet Nutrition should ensure the security and confidentiality of its member and client records and protect these records against unauthorised access that could result in any type of loss or inconvenience for its members.

### Purpose

The purpose and principle of a *Clean Desk Policy* are to ensure that confidential data is not exposed to individuals who may pass through the area such as members, service personnel, and thieves. It encourages methodical management of one's workspace. Because of the risk of being compromised, confidential information should always be treated with care.

### Policy Detail

To maintain the security and privacy of clients', employees' and members' personal information, Montego Pet Nutrition employees should observe the "clean desk" rule. All employees should take appropriate actions to prevent unauthorised persons from having access to member information, applications, or data. Employees are also required to make a conscientious check of their surrounding work environment to ensure that there will be no loss of confidentiality to data media or documents.

The clean desk policy applies to:

- Day Planners and *Rolodexes* that may contain non-public information.
- File cabinets, storage cabinets, and briefcases containing sensitive or confidential information.
- Any confidential or sensitive data, including reports, lists, or statements. Sensitive data refers to personal information and restricted data. Personal information includes, but is not limited to:
  - An individual's name
  - ID number
  - Driver's license number or identification card number
  - Account number, credit or debit card number, security code, access code, or password that could permit access to an individual's financial account
- Restricted data is divided into two (2) categories:
  - Personal data refers to any combination of information that identifies and describes an individual.
  - Limited data, refers to electronic information whose unauthorised access, modification, or loss could seriously or adversely affect Montego Pet Nutrition, its members, and non-members.
- Electronic devices, including cellphones and *PDAs*.

- Keys used to access sensitive information.
- Printouts containing sensitive information.
- Data on printers, copy machines, and/or fax machines.
- Computer workstations and passwords.
- Portable media, such as CDs, disks, or flash drives.
- Desks or work areas, including whiteboards and bookshelves.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 6 – Clean Desk* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 7 – E-COMMERCE

### Definitions

| TERM | DEFINITION |
|---|---|
| **Electronic commerce:** | Electronic financial services are delivered via electronic means including, but not limited to, the Internet or other electronic delivery vehicles.<br><br>**Specific examples of e-commerce activities include:**<br><br>• Internet/World Wide Web (www) services<br>• e-mail inquiries and responses<br>• Publishing of general information on the Montego Pet Nutrition Website<br>• Data entry or verification by staff on a vendor's data processing system<br>• File transfers of member information for direct mail projects or statement generation<br>• Web account access<br>• Viewing share or loan transaction history and balances<br>• Transferring funds between shares and loans, transfers to other financial, or *Person to Person Transfers* (PTP)<br>• Requesting a cheque withdrawal from a share or loan<br>• Applying for Montego Pet Nutrition services through applications or forms<br>• e-mail Statements<br>• Electronic retrieval of cheque copies<br>• e-Alerts<br>• ONLINE BILL-PAYING SERVICES<br>• AUDIO RESPONSE/PHONE-BASED<br>• WIRELESS SERVICES<br>• MOBILE BANKING |
| **Encryption:** | This is the conversion of data into a form, called a *cypher* text, which cannot be easily understood by unauthorised people. |
| **Authentication:** | This is the process of determining whether someone or something is who or what it is declared to be. Depending on the transactions, a more stringent authentication process may be required. |
| **Firewall:** | Any hardware and/or software designed to examine network traffic using Policy Statements (ruleset) to block unauthorised access while permitting authorised communications to or from a network or electronic equipment. |

## Overview

Montego Pet Nutrition recognises the importance of electronic commerce (e-commerce) activities to its present-day operations. Montego Pet Nutrition is committed to using e-commerce activities in a cost-effective manner that promotes accuracy, safety, security, and efficiency. These activities bring automation and efficiencies to traditional manual tasks and allow quicker access to information resulting in improved member service.

## Purpose

This *e-commerce Policy* is to be used as both a guideline and an overview of the management of Montego Pet Nutrition's electronic services.

## Policy Detail

Montego Pet Nutrition is committed to enhancing member service through the use of many forms of e-commerce activities.
Electronic commerce activities include Montego Pet Nutrition's website, email, telephone access system, online bill payment, and home and business banking services. They also include business-to-business transactions where interaction is conducted electronically between Montego Pet Nutrition and its business partners using the Internet as the communications network.

It is the practice of Montego Pet Nutrition to safeguard member data at all times, including the processing of e-commerce transactions. The information must be protected at both the sending and receiving ends of each transaction. To accomplish this, there are several levels of protection applied to e-commerce activities.

## Encryption

Encrypting transactions provides security by ensuring that no portion of a transaction is readable except by the parties at each end of the transmission.

This ensures that data can be transmitted securely without concern that another party could intercept all or part of the transaction. Encryption also makes certain that the transaction is not tampered with as it routes from point to point and data is received exactly as it was sent.

## Authentication

- After a secure connection is established, the initiating party must prove his/her identity before conducting the transaction. This is typically handled with user IDs or account numbers, along with password or PIN combinations. Additionally, encryption certificates are also employed to validate the authenticity of both servers and users. System Administrators control system access by assigning users different levels of access to applications and data. These access levels are

determined by Senior Management and are specific to each job function. This ensures that access to applications and specific types of transactions are only granted as job functions require.

- *Multi-factor Authentication (MFA)*
- For online transactions, *MFA* offers more than one form of authentication to verify the legitimacy of a transaction. The layered defence makes it more difficult for an unauthorised person to gain access.

## Firewalls

Montego Pet Nutrition will deploy and utilise *firewalls* as necessary to protect internal systems from threats originating from the Internet, as well as those that might be present when connecting to vendors' networks. *Firewall* Operating Systems and Configurations will be reviewed periodically to ensure maximum protection. An *Audit Log* will be maintained tracking all attempts to access unconfigured (blocked) services. *Firewalls* and other access devices will be used, as needed, to limit access to sites or services that are deemed inappropriate or non-corporate. Vendor-hosted solution *firewalls* will be reviewed before implementation.

## Network Traffic Rules and Restrictions

Intra-network traffic is subject to distinct operating rules and restrictions. Through the use of *firewall* technology, outside parties are directed only to approved, internal resources. An example of this is web page services that allow certain types of traffic from the Internet (web page browsing) but have other types of traffic blocked (i.e., administrative tasks). This strategy dramatically reduces the risk of any party gaining unauthorised access to a protected server.

The internal network is also protected from virus attacks through the use of anti-virus software that is updated automatically regularly. These regular updates are loaded automatically to each PC, as they are available. This provides the most up-to-date virus protection and security available. e-mail is also scanned before delivery, reducing the potential of a virus entering the network in this manner.

## Staff Training and Review

Necessary staff receive training and review all Procedures at least annually or as major system additions or changes are implemented.

## User Password Maintenance

Staff passwords, where possible, will expire after ninety (90) days, forcing users to modify their passwords. This control, along with a strict Montego Pet Nutrition Policy prohibiting users from sharing or disclosing their passwords, is intended to prohibit unauthorised access to systems and data. After receiving a change in status from the Human Resources Department or other Management team members, IT personnel immediately removes user access codes from appropriate systems.

## Expert Assistance

Montego Pet Nutrition recognises that e-commerce security issues change daily. New threats to security, safety, and accuracy appear daily and system vendors publish updates and patches regularly to eliminate the threat. To assist in the ongoing maintenance of key components of system security, Montego Pet Nutrition will engage, at a regularly scheduled interval, in consulting, and audit oversight. This vendor may also provide technical assistance as new *e-commerce*-related features are added to the system to ensure the continued safety and security of existing systems.

## Communications Network

Montego Pet Nutrition employs the use of several types of data communication lines including private and public network connections. Data transmissions are secured, encrypted, and/or password-protected, as needed.

## Response Program

In the event Montego Pet Nutrition suspects or detects unauthorised individuals have gained access to member information systems, Montego Pet Nutrition will report such actions to appropriate regulatory and law enforcement agencies according to Montego Pet Nutrition's Information Security Response Procedures.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 7 – E-Commerce* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 8 – E-MAIL

### Definitions

| TERM | DEFINITION |
|---|---|
| **Anti-Spoofing:** | A technique for identifying and dropping units of data, called packets, that have a false source address. |
| **Antivirus:** | Software used to prevent, detect, and remove malicious software. |
| **The electronic mail system:** | Any computer software application that allows electronic mail to be communicated from one computing system to another. |
| **Electronic mail (e-mail):** | Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system. |
| **E-mail spoofing:** | The forgery of an e-mail header so the message appears to have originated from someone other than the actual source. The goal of e-mail *spoofing* is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer. |
| **Inbound filters:** | A type of software-based traffic filter allowing only designated traffic to flow towards a network. |
| **Quarantine:** | Suspicious e-mail messages may be identified by an antivirus filter and isolated from the normal mail inbox. |
| **SPAM:** | Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e-mail |

### Overview

E-mail at Montego Pet Nutrition must be managed as a valuable and mission-critical resource. Thus, this Policy is established to:

- Create prudent and acceptable practices regarding the use of information resources.
- Educate individuals who may use information resources concerning their responsibilities associated with such use.
- Establish a schedule for retaining and archiving e-mail.

## Purpose

The purpose of this Policy is to establish rules for the use of Montego Pet Nutrition e-mail for sending, receiving, or storing electronic mail.

## Audience

This Policy applies equally to all individuals granted access privileges to any Montego Pet Nutrition information resource with the capacity to send, receive or store electronic mail.

## Legal

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libellous, defamatory, offensive, racist, or obscene remarks.
- Sending or forwarding confidential information without permission.
- Sending or forwarding copyrighted material without permission.
- Knowingly sending or forwarding an attachment that contains a malicious program.

## Policy Detail

## General

- **Corporate e-mail is not private**. Users expressly waive any right of privacy in anything they create, store, send, or receive on Montego Pet Nutrition's computer systems. Montego Pet Nutrition can but is not obliged to monitor e-mails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by Montego Pet Nutrition, may be subject to open records requests, and may be accessed under this Policy.
- **Incoming e-mails** must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All e-mail is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to Montego Pet Nutrition systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.
- **Anti-*spoofing* practices** have been initiated for detecting *spoofed* e-mails. Employees should be diligent in identifying a *spoofed* e-mail. If e-mail *spoofing* has occurred, IT must be immediately notified.
- **Incoming e-mails are scanned** for malicious file attachments. If an attachment is identified as having an extension known to be associated with *malware*, prone to abuse by *malware* or bad actors or otherwise poses a heightened risk, the attachment will be removed from the e-mail before delivery.

- **E-mail rejection** is achieved by listing domains and *IP Addresses* associated with malicious actors. Any incoming e-mail originating from a known malicious actor will not be delivered.
- **Any e-mail account misbehaving** by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.
- **E-mail is to be used for business purposes** and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for viruses and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system but also harm Montego Pet Nutrition's reputation.

### The following activities are prohibited by this Policy:

- **Sending e-mails** that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to abusive language, sexually explicit remarks or pictures, profanities, and defamatory or discriminatory remarks regarding race, creed, colour, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- **Using e-mail** to send **SPAM** or other unauthorised solicitations.
- **Violating copyright** laws by illegally distributing protected works.
- **Sending an e-mail** using another person's e-mail account, except when authorised to send messages to another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- **Forging** or attempting to forge e-mail messages.
- Using unauthorised e-mail software.
- Knowingly **disabling the automatic scanning of attachments** on any Montego Pet Nutrition personal computer.
- Knowingly circumventing e-mail security measures.
- **Sending or forwarding joke e-mails**, chain letters, or hoax letters.
- Sending **unsolicited messages to large groups**, except as required to conduct Montego Pet Nutrition business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding an e-mail with **computer viruses**.
- Setting up or responding on behalf of Montego Pet Nutrition without management approval.
- **E-mail is not secure**. Users must not e-mail passwords, identification numbers, account numbers, PINs, dates of birth, mother's maiden name, etc. to parties outside the Montego Pet Nutrition network without encrypting the data.
- All **user activity** on Montego Pet Nutrition information system assets is subject to logging and review. Montego Pet Nutrition has software and systems in place to monitor e-mail usage.
- E-mail users must not give the impression that they are **representing**, giving opinions, or otherwise making statements on behalf of Montego Pet Nutrition, unless appropriately authorised (explicitly or implicitly) to do so.

- Users must not send, forward, or receive **confidential or sensitive Montego Pet Nutrition information** through non-Montego Pet Nutrition e-mail accounts. Examples of non-Montego Pet Nutrition e-mail accounts include, but are not limited to: *Hotmail, Yahoo mail, Gmail,* and e-mail provided by other *Internet Service Providers* (ISP).
- Users with **non-Montego Pet Nutrition-issued mobile devices** must adhere to the *Personal Device Acceptable Use and Security Policy* for sending, forwarding, receiving, or storing confidential or sensitive Montego Pet Nutrition information.

## Incidental Use

- Incidental personal use of sending e-mail is restricted to Montego Pet Nutrition-approved users; it does not extend to family members or other acquaintances.
- Without prior management approval, incidental use must not result in direct costs to Montego Pet Nutrition.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for or embarrassment to Montego Pet Nutrition.
- Storage of personal files and documents within Montego Pet Nutrition's IT systems should be nominal.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 8 – E-mail* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 9 – FIREWALL

### Definitions

| TERM | DEFINITION |
|---|---|
| **Firewall:** | Any hardware and/or software designed to examine network traffic using Policy Statements (ruleset) to block unauthorised access while permitting authorised communications to or from a network or electronic equipment. |
| **Firewall configuration:** | The system setting affects the operation of a *firewall* appliance. |
| **Firewall ruleset:** | A set of Policy Statements or Instructions used by a *firewall* to filter network traffic. |
| **Host firewall:** | A *firewall* application that addresses a separate and distinct host, such as a personal computer. |
| **Internet Protocol (IP):** | Primary Network Protocol used on the Internet. |
| **Network firewall:** | A *firewall* appliance attached to a network to control traffic flows to and from single or multiple hosts or *subnet(s)*. |
| **Network topology:** | The layout of connections (links, nodes, etc.) of a computer network. |
| **Simple Mail Transfer Protocol (SMTP):** | An Internet Standard for electronic mail (e-mail) transmission across *Internet Protocol* (IP) Networks. |
| **Virtual private network (VPN):** | A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organisation's network. |

### Overview

Montego Pet Nutrition operates network *firewalls* between the Internet and its private internal network to create a secure operating environment for Montego Pet Nutrition's computer and network resources. A *firewall* is just one element of a layered approach to network security.

## Purpose

This Policy governs how the *firewalls* will filter Internet traffic to mitigate the risks and losses associated with security threats to Montego Pet Nutrition's network and information systems.

The *firewall* will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the *firewall ruleset*.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide robust authentication.
- Provide *Virtual Private Network* (VPN) connectivity

## Policy Detail

### General

All network *firewalls*, installed and implemented, must conform to the current standards as determined by Montego Pet Nutrition's IT Department, or designee. Unauthorised or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this Policy.

### Outbound – allows all Internet traffic to authorised groups

All traffic is authorised by *Internet Protocol* (IP) address and port.

The *firewalls* will provide:

- Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.
- Application proxy – every packet is stopped at the proxy *firewall* and examined and compared to the rules configured into the firewall.
- Stateful Inspection – a *firewall* technology that monitors the state of active connections and uses this information to determine which network packets to allow through the *firewall*.

The *firewalls* will protect against:

- *IP spoofing* attacks – the creation of *IP packets* with a forged source I*P* address to conceal the identity of the sender or impersonate another computing system.
- *Denial-of-Service* (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.
- Any network information utility that would reveal information about the Montego Pet Nutrition domain.
- A *Change Control Process* is required before any *firewall* rules are modified. Before implementation, the Third-Party Vendor and Montego Pet Nutrition Network Administrators are required to have the modifications approved by Senior Management. All related documentation is to be retained for three (3) years.
- All *firewall* implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.
- *Firewall rulesets* and configurations require periodic review to ensure they afford the required levels of protection:
    - Montego Pet Nutrition must review all network *firewall rulesets* and configurations during the initial implementation process and periodically thereafter.
    - *Firewall rulesets* and configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

## Responsibilities

The IT Department, or designee, is responsible for implementing and maintaining Montego Pet Nutrition's *firewalls*, as well as for enforcing and updating this Policy. Login access to the *firewall* will be restricted to a primary *firewall* Administrator and designees as assigned. Password construction for the *firewall* will be consistent with the strong password creation practices outlined in Montego Pet Nutrition *Password Policy*.

The specific guidance and direction for Information Systems Security is the responsibility of IT. Accordingly, IT will manage the configuration of Montego Pet Nutrition *firewalls*.

Montego Pet Nutrition can contract a Third-Party Vendor to manage the external *firewalls*. This vendor's responsibilities may include:

- Retention of the *firewall* rules
- *Patch* Management
- Review the *firewall* logs for:
    - System errors
    - Blocked websites

    - Attacks
- Sending alerts to Montego Pet Nutrition Network Administrators in the event of attacks or system errors
- Backing up the firewalls

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 9 – Firewall* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 10 – HARDWARE AND ELECTRONIC MEDIA DISPOSAL

### Definitions

| TERM | DEFINITION |
|---|---|
| **Beyond reasonable repair:** | Refers to any equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement. |
| **Chain of Custody (CoC):** | Refers to the chronological documentation of the custody, transportation, or storage of evidence to show it has not been tampered with before destruction. |
| **Disposition:** | Refers to the reselling, reassignment, recycling, donating, or disposal of IT equipment through responsible, ethical, and environmentally sound means. |
| **Non-leased:** | Refers to any IT assets that are the sole property of Montego Pet Nutrition, that is, equipment not rented, leased, or borrowed from a third-party supplier or partner company. |
| **Obsolete:** | Refers to any equipment that no longer meets requisite functionality. |
| **Surplus:** | Refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements. |

### Overview

Hardware and electronic media disposition are necessary at Montego Pet Nutrition to ensure the proper disposition of all non-leased Montego Pet Nutrition IT hardware and media capable of storing member information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

### Purpose

Montego Pet Nutrition-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this Policy. Where assets have not reached the end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This Policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner. Montego Pet Nutrition's surplus or obsolete IT assets and resources (i.e., desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Montego Pet

Nutrition's Upgrade Guidelines. All Disposition Procedures for retired IT assets must adhere to company-approved methods.

## Policy Detail

### General

Disposition Procedures for all IT assets and equipment will be centrally managed and coordinated by Montego Pet Nutrition's IT Department, or designee. The IT Department, or designee, is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment.

IT is also responsible for the chain-of-custody in acquiring credible documentation from contracted third-parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations.

It is the responsibility of any employee of Montego Pet Nutrition's IT Department, or designee, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the *Hardware and Electronic Media Disposal Procedure*. All dispositions must be done appropriately, responsibly, and according to *IT Lifecycle Standards,* as well as with Montego Pet Nutrition's *Resource Planning* in mind.

Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives
- Flash memory

Other portable storage devices

- Secure disposal must include a certificate verifying the destruction of the media or device before recycling.
- Assets selected for redeployment or sale are to be securely cleared and reset to factory defaults before deployment or sale by the IT Department. A *Decommissioning Form* needs to be completed for each asset specifying the steps taken and signed by the Technician. Where the item is to be removed from the

ownership of Montego Pet Nutrition, verification that the Asset Tag Numbers have been removed from both the asset and the register need to be included in the Decommissioning Form.

- A *Gate Pass* or similar clearance document must accompany the equipment off the premises and a copy stamped by Security must be retained by IT for a reasonable period.

Where an item is sent to a vendor for repair and after inspection, it is deemed to be beyond reasonable repair, the IT Department may ask the vendor to dispose of the item on condition that the vendor can provide a Certificate of Disposal, to save on unnecessary transport costs.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 10 – Hardware and Electronic Media Disposal* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 11 – SECURITY INCIDENT MANAGEMENT

### Definitions

| TERM | DEFINITION |
|---|---|
| **Security incident:** | Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include but are not limited to, unauthorised access, malicious code, network probes, and denial of service attacks. |

### Overview

Security Incident Management at Montego Pet Nutrition is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify Montego Pet Nutrition members of the breach.

### Purpose

This Policy defines the requirement for reporting and responding to incidents related to Montego Pet Nutrition Information Systems and Operations. Incident Response provides Montego Pet Nutrition with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This Policy applies to all Information Systems and Information System Components of Montego Pet Nutrition. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralised computing capabilities.
- Devices that provide centralised storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- *Firewalls, Intrusion Detection/Prevention (IDP) Sensors*, and other devices that provide dedicated security capabilities.

In the event a breach of a member's information occurs, Montego Pet Nutrition is required by law to notify the individual(s).

## Policy Detail

## Program Organisation:

### Computer Emergency Response Plans

Montego Pet Nutrition Management must prepare, periodically update, and regularly test Emergency Response Plans that provide for the continued operation of Critical Computer and Communication Systems in the event of an interruption or degradation of service. For example, charter connectivity is interrupted by an isolated *malware* discovery.

### Incident Response Plan Contents

The Montego Pet Nutrition *Incident Response Plan* must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:

- Specific Incident Response Procedures
- Business Recovery and Continuity Procedures
- Data Backup Processes
- Analysis of legal requirements for reporting compromises
- Identification and coverage for all critical system components
- Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

### Incident Response Testing

At least once every year, the IT Department, or designee, must utilise simulated incidents to mobilise and test the adequacy of the response. Where appropriate, tests will be integrated with testing of related plans (*Business Continuity Plan, Disaster Recovery Plan*, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

### Incident Response and Recovery

A Security Incident Response Capability will be developed and implemented for all information systems that house or access Montego Pet Nutrition controlled information. The Incident Response Capability will include a defined plan and will address the seven (7) stages of Incident Response:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery

- Post-Incident Activity

To facilitate Incident Response Operations, responsibility for incident handling operations will be assigned to an Incident Response Team. If an incident occurs, the members of this team will be charged with executing the Incident Response Plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in Incident Response Operations on an annual basis. Incident Response Plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based on the documented results of previously conducted tests or live executions of the Incident Response Plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

### Intrusion Response Procedures

The IT Department, or designee, must document and periodically revise the Incident Response Plan with Intrusion Response Procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

### Malicious Code Remediation

The steps followed will vary based on the scope and severity of a Malicious Code Incident as determined by Information Security Management. They may include but are not limited to *malware* removal with one or more tools, data *quarantine*, permanent data deletion, hard drive wiping, or hard drive/media destruction.

### Data Breach Management

Montego Pet Nutrition Management should prepare, test, and annually update the Incident Response Plan that addresses Policies and Procedures for responding in the event of a breach of sensitive customer data.

### Incident Response Plan Evolution

- The Incident Response Plan must be updated to reflect the lessons learned from actual incidents.
- The Incident Response Plan must be updated to reflect developments in the industry.

### Reporting to Third Parties

- Unless required by law or regulation to report information security violations to external authorities, Senior Management, in conjunction with legal representatives, and the IT Department, or designee, must weigh the pros and cons of external disclosure before reporting these violations.

- If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third-party private or confidential information to be exposed to unauthorised persons, these third parties must be immediately informed about the situation.
- If sensitive information is lost, disclosed to unauthorised parties, or suspected of being lost or disclosed to unauthorised parties, both its Owner and the Managing Partners must be notified immediately.

## Display of Incident Reporting Contact Information

Montego Pet Nutrition's contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the *intranet*.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 11 – Security Incident Management* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 12 – INFORMATION TECHNOLOGY PURCHASING

### Overview

Information Technology purchasing at Montego Pet Nutrition must be managed to ensure compatibility and to control the costs of the technology and services requested.

### Purpose

The purpose of this Policy is to define standards, procedures, and restrictions for the purchase of all IT hardware, software, computer-related components, and technical services purchased with Montego Pet Nutrition funds. Purchases of technology and technical services for Montego Pet Nutrition must be approved and coordinated through the IT Department, or designee.

### Scope

The scope of this Policy includes, but is not limited to, the following Montego Pet Nutrition Technology Resources:

- Desktops, laptops, smartphones/*PDA*s, cellphones, tablets, *TCDs*, and servers
- Software running on the devices mentioned above
- Peripheral equipment, such as printers and scanners
- Cables or connectivity-related devices
- Audio-visual equipment, such as projectors and cameras

This Policy extends to technical services, such as off-site disaster recovery solutions and *Internet Service Providers* (ISPs), as well as professional services, such as consultants and legal professionals hired through the IT Department, or designee. These include, but are not limited to, the following:

- Professionals or firms contracted for application development and maintenance
- Web services provided by a third party
- Consulting professionals
- Recruiting services
- Training services
- Disaster recovery services
- Hosted telephone services
- Telephone network services
- Data network services

### Policy Detail

- All hardware, software, or components purchased with Montego Pet Nutrition funds are the property of Montego Pet Nutrition. This also includes all items purchased using a personal credit card, for which the employee is later reimbursed.
- All purchase requests for hardware, software, computer-related components, internet services, or third-party electronic services must be submitted to the IT

Department, or designee, via the *Helpdesk*, for final purchase approval. If the requested item is already in inventory, then it will be made available to the requestor, assuming that it meets organisational unit goals.

**Purchasing within IT**, or designee falls under four (4) general categories.

### 1. Standard Items

Purchase of items, which have been pre-approved by IT Management, requires only a *Helpdesk* request. The standard items list, located in the IT Procedure documentation, contains preapproved vendors and products which Montego Pet Nutrition has standardised. Standard items have been proven to be both supportable by the IT Department, or designee, as well as cost-effective.

### 2. Non-Standard Items

- Purchase of non-standard items/services, which are not classified as capital expenses, such as non-standard hardware/software that is expensed or contracted services. Non-standard purchases should be minimised as much as reasonably possible. Requests for non-standard items will go through a formal selection process that will involve thorough vendor sourcing. IT will review non-standard purchases for the viability of support and compatibility.
- The selection process may vary depending on the type, cost, and other purchase significance factors. Before approval will be granted, employees or departments requesting non-emergency specialised software, or components, must submit a plan detailing how this item will be supported. Support options include assigning a staff member to maintain and/or support the component, arranging for external vendor support, or arranging for a service Level Agreement with the IT Department, or designee.
- Individuals requesting non-standard items for purchase can suggest a potential vendor if a pre-existing relationship exists between that vendor and Montego Pet Nutrition.

### 3. Capital Expenses

Purchase of non-standard capitalised hardware, software, or equipment:

Capitalized expenditures, defined as hardware, software, or equipment above a prescribed amount to be confirmed by the IT Department, or as specified in the Montego Pet Nutrition *Fixed Asset Policy*, which is capitalised by Montego Pet Nutrition, must go through the EXCO for approval. These purchases may only be requisitioned by Department Managers. The purchase selection process for these expenditures will be evaluated by Senior Management.

## 4. System replacement

Major technology purchases are approved through the budgetary process. Equipment replaced during any period shall be based on a minimum annual review of the *Asset Management Program and Hardware Replenishment Schedule*, *Hardware Inventory*, and *Fixed Asset Budget Schedules*.

### Asset Management Program

Certain classes of Montego Pet Nutrition assets, as defined below ("Qualified Assets" or "Asset"), procured, or curated by the Montego Pet Nutrition Information Technology Department shall be duly managed with the objective of protecting them from misappropriation and unplanned obsolescence.

Methods shall be devised and followed to allow for asset identification, assignment, tracking, lifecycle management, reporting, and disposition.

Included asset classes are as follows:

- Technology equipment
- Computer hardware
- Peripherals, and
- Other items purchased by Montego Pet Nutrition IT or managed by same that are semi-permanent in their end-user assignment (example: specific person, department) or purpose (example: loaner laptop, projector) AND are valued at greater than a specified amount to be confirmed with the IT Department AND are not high-turnover or frequently moved devices (example: small peripherals such as mouses and keyboards).

### Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 12 – Information Technology Purchasing* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 13 – INTERNET

### Definitions

| TERM | DEFINITION |
|---|---|
| **Internet:** | A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organisations, government agencies, companies, and colleges. |
| **Intranet:** | A private network for communications and sharing of information that, like the Internet, is based on *Transmission Control Protocol/Internet Protocol* (TCP/IP) but is accessible only to authorised employees within an organization. An organization's *intranet* is usually protected from external access by a *firewall*. |
| **User:** | An individual or automated application or process that is authorised access to the resource by the system owner, following the system owner's Procedures and Rules. |
| **World Wide Web (www):** | A system of Internet hosts that supports documents formatted in *Hypertext Markup Language* (HTML) that contains links to other documents (hyperlinks) and audio, video, and graphic images. Individuals can access the Web with special applications called browsers, such as *Microsoft Internet Explorer*. |

### Overview

Internet access and usage at Montego Pet Nutrition must be managed as valuable and mission-critical resources.

This Policy is established to:

- Create prudent and acceptable practices regarding the use of the Internet.
- Educate individuals who may use information resources concerning their responsibilities associated with such use.

### Purpose

The purpose of this Policy is to establish the rules for the use of Montego Pet Nutrition Internet for access to the Internet or the *Intranet*.

### Audience

This Policy applies equally to all individuals granted access privileges to any Montego Pet Nutrition information system or resource with the capacity to access the Internet, the *Intranet*, or both.

## Policy Detail

### Accessing the Internet

- Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked. IT may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by *malware*. Montego Pet Nutrition will use internet filters to block high-risk content and deny access to any unwanted material or *malware* in support of the *Acceptable Use Policy*.
- All software used to access the Internet must be part of the Montego Pet Nutrition Standard Software Suite or approved by IT. Such software must incorporate all vendor-provided *security patches*.
- Users accessing the Internet through a computer connected to Montego Pet Nutrition's Network must do so through an approved Internet *firewall* or other security devices. Bypassing Montego Pet Nutrition's Network Security is strictly prohibited.
- Users are prohibited from using Montego Pet Nutrition Internet access for:
    - unauthorised access to local and remote computer systems
    - software piracy
    - illegal activities
    - the transmission of threatening, obscene, or harassing materials, or
    - personal solicitations

### Expectation of privacy

- Users should have no expectation of privacy in anything they create, store, send, or receive using Montego Pet Nutrition's Internet access.
- Users expressly waive any right of privacy in anything they create, store, send, or receive using Montego Pet Nutrition's Internet access.

### File downloads and virus protection

- Users are prohibited from downloading and installing software on their PC without proper authorisation from IT. Technical controls may be utilised to limit the download and installation of software.
- Downloaded software may be used only in ways that conform to its license and copyrights.
- All files, downloaded from the Internet, must be scanned for viruses using Montego Pet Nutrition-approved Virus Detection Software. If a user suspects a file may be infected, he/she must notify IT immediately.
- Users are prohibited from using the Internet to deliberately propagate any virus, *worm*, *Trojan Horse*, *trapdoor*, or other malicious programs.

## Monitoring of computer and Internet usage

All user activity on Montego Pet Nutrition IT assets is subject to logging and review. Montego Pet Nutrition has the right to monitor and log all aspects of its systems including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

## Frivolous use

- Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources.
- The user must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others.
- These acts include but are not limited to:
  - spending excessive amounts of time on the Internet
  - playing games
  - engaging in online chat groups
  - uploading, or downloading large files
  - accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.
- Personal use, beyond incidental use of the Internet, may be done only in compliance with this Policy.

## Content

- Montego Pet Nutrition utilises software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace. The display, storing, archiving, or editing of such content on any Montego Pet Nutrition PC is prohibited.
- Users are prohibited from attempting to access or accessing inappropriate sites from any Montego Pet Nutrition PC. If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to IT.
- Montego Pet Nutrition Departments may not host their websites or contract for the hosting of websites by a vendor without the permission of IT.
- Content on all Montego Pet Nutrition hosted websites must comply with the Montego Pet Nutrition *Acceptable Use of Information Systems and Privacy Policies*. No internal data will be made available to hosted Internet websites without the approval of IT.
- No personal or non-Montego Pet Nutrition commercial advertising may be made available via hosted Montego Pet Nutrition websites.

## Transmissions

- All sensitive Montego Pet Nutrition material transmitted over the Internet or external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained following departmental records retention schedules.

## Incidental use

- Incidental personal use of Internet access is restricted to Montego Pet Nutrition-approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Montego Pet Nutrition.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, Montego Pet Nutrition.
- Storage of personal files and documents within Montego Pet Nutrition's IT should be nominal.
- All files and documents, including personal files and documents, are owned by Montego Pet Nutrition and may be subject to open records requests and may be accessed under this policy.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 13 – Internet* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 14 – LOG MANAGEMENT

### Definitions

| TERM | DEFINITION |
|---|---|
| **Endpoints:** | Any user device connected to a network. *Endpoints* can include personal computers, personal digital assistants, scanners, etc. |
| **Flow:** | The traffic that corresponds to a logical connection between two processes in the network. |
| **IP:** | *Internet Protocol* is the method or protocol by which data is sent from one computer to another on the Internet. |
| **Packet:** | The unit of data that is routed between an origin and a destination on the Internet or any other *packet-switched* network. |

### Overview

Most components of the IT Infrastructure at Montego Pet Nutrition are capable of producing Logs chronicling their activity over time.

These Logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications. Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and are critical to have for forensics analysis.

### Purpose

Log Management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance.

Montego Pet Nutrition will perform a periodic Risk Assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilisation – how much capacity is used by services
- Security Events – what activity occurred during an incident and when
- User Activity – what people are doing with services

## Policy Detail

### Log Generation

- Depending on the volume of activity and the amount of information in each Log entry, Logs have the potential of being very large. Information in Logs often cannot be controlled by the application, system, or Network Administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.
- *Application Logs* identify what transactions have been performed, at what time, and for whom. Those Logs may also describe the hardware and Operating System Resources that were used to execute that transaction.
- *System Logs* for Operating Systems and Services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of System Administration. When related to *Application Logs*, they provide an additional layer of detail that is not observable from the application itself. *Service Logs* can also aid in intrusion analysis when an intrusion bypasses the application itself.
- *Change Management Logs*, which document changes in the IT or business environment, provide context for the automatically generated Logs.
- Other sources, such as *Physical Access or Surveillance Logs*, can provide context when investigating security incidents.
- Client workstations also generate *System Logs* that are of interest, particularly for local authentication, *malware* detection, and host-based *firewalls*.

### Network Logs

- Network devices, such as *firewalls*, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These Logs have a value of their own to Network Administrators, but they also may be used to enhance the information in the application and other Logs.
- Many components of the IT infrastructure, such as routers and network-based *firewalls*, generate Logs. All of the Logs have potential value and should be maintained. These Logs typically describe flows of information through the network, but not the individual packets contained in that flow.
- Other components for the network infrastructure, such as *Dynamic Host Configuration Protocol* (DHCP) and *Domain Name System* (DNS) servers, provide valuable information about network configuration elements, such as *IP* addresses, that change over time.
- Time synchronisation
    - One of the important functions of a Log Management Infrastructure is to relate records from various sources by time. Therefore, all components of the IT infrastructure must synchronise clocks. Montego Pet Nutrition uses *Network Time Protocol* (NTP) for time synchronisation.

## Use of Log Information

Logs often contain information that, if misused, could represent an invasion of the privacy of members of Montego Pet Nutrition. While Montego Pet Nutrition must perform regular collection and monitoring of these Logs, this activity should be done in the least invasive manner.

## Baseline Behaviour

It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behaviour allows for the detection of anomalous behaviour, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information is reviewed on a regular and timely basis.

## Investigation

When an incident occurs, various *ad hoc* questions will need to be answered. These incidents may be security-related, or they may be due to a malfunction, a change in the IT Infrastructure, or a change in usage patterns.

Whatever the cause of the incident, it will be necessary to retrieve and report Log Records. Thresholds shall be established that dictate what level of personnel or management response is required for any given Log entry or group of entries and detailed in a Procedure.

## Log Record Life-Cycle Management

When Logs document or contain valuable information related to activities of Montego Pet Nutrition's Information Resources or the people who manage those resources, they are Montego Pet Nutrition Administrative Records, subject to the requirements of Montego Pet Nutrition to ensure that they are appropriately managed and preserved and can be retrieved as needed.

## Retention

To facilitate investigations, as well as to protect privacy, the retention of Log Records should be well defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain Log records that are not needed. The cost of long-term retention can be significant and could expose Montego Pet Nutrition to the high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

## Log Management Infrastructure

A *Log Management Infrastructure* will be established to provide common management of Log records. To facilitate the creation of *Log Management Infrastructure*, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build *Log Management Infrastructure*
- Typical retention periods for common examples of logged information

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 14 – Log Management* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 15 – SAFEGUARDING MEMBER INFORMATION

### Definitions

| TERM | DEFINITION |
|---|---|
| **Member:** | An individual who has an established, ongoing relationship with Montego Pet Nutrition. This includes both members and non-members who have co-signed on loans. Examples of non-members include non-member joint account holders. |
| **Service provider:** | A third party that maintains, processes, or otherwise is permitted access to member information while performing services for Montego Pet Nutrition. |
| **Member information:** | Any record maintained by, or on behalf of, Montego Pet Nutrition that contains information regarding an individual who has an established, ongoing relationship with Montego Pet Nutrition. This includes records, data, files, or other information in paper, electronic, or other forms that are maintained by, or on behalf of, any service provider on behalf of Montego Pet Nutrition. |
| **Member information system:** | Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of member information. |

### Overview

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Member Information Security Controls
- Vendor Management Review Program
- Software Inventory
- Hardware Inventory
- Critical Systems List
- Records Management
- Clean Desk Policy
- Hardware and Electronic Media Disposal Policy
- IT Acquisition Policy
- Incident Response Plan
- Information Sharing
- Training
- Testing

## Purpose

The purpose of this Policy is to ensure that Montego Pet Nutrition complies with existing laws and to ensure that information regarding members is kept secure and confidential.

## Policy Detail

It is the policy of Montego Pet Nutrition to protect the confidentiality, security, and integrity of each member's non-public personal information under existing laws. Montego Pet Nutrition will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for member records and information.

- Montego Pet Nutrition will maintain Physical, Electronic, and Procedural Safeguards, which comply with national standards, to guard members' non-public personal information.
- Montego Pet Nutrition will not gather, collect, or maintain any information about its members that is not necessary to offer its products and services, to complete member transactions, or for other relevant business purposes.
- Montego Pet Nutrition does not sell or provide any member information to third parties, including list services, telemarketing firms, or outside companies for independent use.
- Executive Committee (EXCO) must approve the *Safeguarding Member Information Policy*.
- Montego Pet Nutrition's IT Department, or designee, is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training.
- Montego Pet Nutrition Management is responsible for ensuring that its departments comply with the requirements of the program.

## Information Security Program

Management is responsible for developing, implementing, and maintaining an effective information security program to:

- Ensure the security and confidentiality of member records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorised access to, or use of, such records or information that would result in substantial harm or inconvenience to any member.
- Management shall report to the EXCO, at least annually, on the current status of Montego Pet Nutrition's *Information Security Program*. EXCO will also be notified of any security breaches or violations and the Management Team's response and recommendations for changes in the *Information Security Program*.

## Risk Assessment

Montego Pet Nutrition maintains a risk assessment that identifies potential threats to member information and evaluates the potential impact of the threats. On an annual basis, the risk assessment is reviewed and updated by the IT Department, or designee, and Montego Pet Nutrition's Management. Montego Pet Nutrition's controls are then updated accordingly.

## Management and Control of Risk

To manage and control the risks that have been identified, Montego Pet Nutrition will:

- Establish written Procedures designed to implement, maintain, and enforce Montego Pet Nutrition's *Information Security Program*.
- Limit access to Montego Pet Nutrition's Member Information Systems to authorised employees only.
- Establish controls to prevent employees from providing member information to unauthorised individuals.
- Limit access at Montego Pet Nutrition's physical locations containing member information, such as building, computer facilities, and records storage facilities, to authorised individuals only.
- Provide encryption of electronic member information including, but not limited to, information in transit or in the storage on networks or systems to which unauthorised individuals may have access.
- Ensure that Member Information System modifications are consistent with Montego Pet Nutrition's *Information Security Program*.
- Implement *Dual-control Procedures*, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information.
- Monitor Montego Pet Nutrition's Systems and Procedures to detect actual and attempted attacks on, or intrusions into, the Member Information Systems.
- Establish response programs that specify actions to be taken when Montego Pet Nutrition suspects or detects that unauthorised individuals have gained access to Member Information Systems, including appropriate reports to regulatory and law enforcement agencies.
- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures.
- Regularly test, monitor, evaluate, and adjust, as appropriate, the *Information Security Program* in light of any relevant changes in technology, the sensitivity of member information, business arrangements, outsourcing arrangements, and internal or external threats to Montego Pet Nutrition's *Information Security Systems*.

## Member information Security Controls

Montego Pet Nutrition has established a series of member information security controls to manage the threats identified in the risk assessment. The controls fall into ten (10) categories.

### 1. Vendor Management Review Program

Montego Pet Nutrition will exercise appropriate due diligence when selecting service providers. When conducting due diligence, Management will conduct a documented vendor review process as outlined in the *Vendor Due Diligence Procedure*.

All service providers, who may access member information, must complete a *Non-Disclosure Agreement* requiring the provider to maintain the safekeeping and confidentiality of member information in compliance with applicable laws. Such agreements must be obtained before any sharing of member information. Once the agreement has been completed, Management will, according to risk, monitor service providers by reviewing audits, summaries of test results, or other evaluations.

### 2. Software Inventory

Montego Pet Nutrition will maintain an inventory of its desktop, server, and infrastructure software.

The information from this collection will provide critical information in identifying the software required for rebuilding systems.

A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The *Software Inventory List* will be reviewed and updated continually.

### 3. Hardware Inventory

Montego Pet Nutrition will maintain an inventory of its desktop, server, and infrastructure hardware.

The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems.

A template incorporated into the hardware inventory ensures that Montego Pet Nutrition standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The *Hardware Inventory List* will be reviewed and updated continually.

### 4. Critical Systems List

Montego Pet Nutrition will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of

these systems is crucial for securing member information from vulnerabilities, performing an impact analysis, and preparing for unscheduled events that affect the operations of Montego Pet Nutrition.

## 5. Records Management

The industry-wide general principles of Records Management apply to records in any format. Montego Pet Nutrition will adhere to Policies and Procedures for protecting critical records from all outside and unauthorised access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.

Montego Pet Nutrition will adhere to the required National Guidelines designated for record retention. Montego Pet Nutrition will adhere to the *Records Retention Policy* for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of the types of records that are disposed of, including certification that the records have been destroyed.

## 6. Clean Desk Policy

Montego Pet Nutrition employees will comply with the *Clean Desk Policy*. This Policy was developed to protect sensitive data from being readily available to unauthorised individuals.

## 7. Hardware and Electronic Media Disposal Procedure

Montego Pet Nutrition will take precautions, as outlined in the *Hardware and Electronic Media Disposal Policy*, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.

## 8. IT Acquisition Policy

Montego Pet Nutrition will adhere to Policies and Procedures for the acquisition of computer-related items. Computer-related purchases will be reviewed by designated IT personnel for compliance with Security Plans and alignment with Operational and Strategic Plans.

An annual review of acquisition Policies and Procedures will occur with input from the IT Department or designee. A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current-year plans or long-range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.

## 9. Incident Response Plan

Incident response is defined as an organised approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

As required in the *Incident Response Plan*, Montego Pet Nutrition will assemble a team to handle any incidents that occur. Necessary actions to prepare Montego Pet Nutrition and the Incident Response Team will be conducted before an incident as required in the *Incident Response Plan*.

Below is a summary of the steps the IT Department, or designee, as well as Montego Pet Nutrition Management, would take:

- The IT Department, or designee, will immediately investigate the intrusion to:
  - prevent any further intrusion into the system.
  - determine the extent of the intrusion and any damage caused.
  - take any steps possible to prevent any future such intrusions .
- The IT Department, or designee, will notify Administrative Management and Risk Management of the intrusion. Administrative Management will be responsible for notifying EXCO.
- The IT Department, or designee, will follow Escalation Processes and Notification Procedures as outlined in the *Incident Response Plan*. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies, or the public.

## 10. Information Sharing

Montego Pet Nutrition recognises the value of the concept of information and intelligence sharing. This may be done through free or paid subscriptions to periodicals, especially electronically disseminated content such as email and *RSS* feeds, websites, and threat intelligence feeds that are accurate to the day and even up to the minute.

Management will ensure that they and appropriate staff have access to information-sharing forums or platforms and the means to use them and use them in our information security practice. Also, certain channels may be conducive to out-sharing pertinent information to peers, law enforcement, regulatory bodies, or other authorities.

The information shared and the receiving party must be considered in reporting candidly, anonymously, or otherwise to ensure there is no breach of confidence.

## Training

Montego Pet Nutrition recognises that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. Montego Pet Nutrition will conduct regular IT training through methods such as staff meetings and computer-based tutorial programs. In addition, employees will be trained to recognise, respond to, and where appropriate, report any unauthorised or fraudulent attempts to obtain member information.

All new employees will receive IT Security Training, as part of their orientation training, emphasising security and IT responsibility. The Human Resources, or designee, is responsible for training new employees on Information Security.

## Testing

The Information Security Officer annually audits Montego Pet Nutrition's *Safeguarding Member Information Program*. The Information Security Officer provides a formal report of its findings to Senior Management, the Security Officer, and the Partners.

Montego Pet Nutrition will require periodic tests of the key controls, systems, and procedures of the information Security Program. By current industry standards, the frequency and nature of such tests shall be determined by the IT Department or designee.

The Information Security Officer will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 15 – Safeguarding Member Information* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 16 – NETWORK SECURITY AND VPN ACCEPTABLE USE

### Definitions

| TERM | DEFINITION |
|---|---|
| **Virtual Private Network (VPN):** | A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some *VPNs* allow employees to securely access a corporate *intranet* while located outside the office. |
| **User Authentication:** | A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used. |
| **Multi-Factor Authentication:** | A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two (2) of the following categories:<br>• Knowledge (something they know)<br>• Possession (something they have)<br>• Inherence (something they are) |
| **Dual Homing:** | Having concurrent connectivity to more than one network from a computer or network device. Examples include:<br>• Being logged into the corporate network via a local *Ethernet* connection and dialling into another Internet Service Provider (ISP).<br>• Being on a Montego Pet Nutrition provided remote access home network, and connecting to another network, such as a spouse's remote access |
| **Digital Subscriber Line (DSL):** | *Digital Subscriber Line (DSL)* is a form of high-speed Internet access competing with cable modems. *DSL* works over standard phone lines and supports data speeds of over 10 *Mbps* downstream (to the user) and slower speeds upstream (to the Internet).<br>This also includes *Fibre* and *LTE* connections. |
| **Remote Access:** | Any access to Montego Pet Nutrition's corporate network through a non-Montego Pet Nutrition controlled network, device, or medium. |
| **Split-tunnelling:** | Simultaneous direct access to a non-Montego Pet Nutrition network (such as the Internet, or a home network) from a remote device (PC, *PDA*, *WAP* phone, etc.) while connected to Montego Pet Nutrition's corporate network via a *Virtual Private Network (VPN)* tunnel. *VPN* |

| | |
|---|---|
| | is a method for accessing a remote network via "tunnelling" through the Internet. |
| **IPsec Concentrator:** | A device in which *VPN* connections are terminated. |
| **CHAP:** | *Challenge Handshake Authentication Protocol (CHAP)* is an authentication method that uses a one-way hashing function. *Data Link Connection Identifier (DLCI)* is a unique number assigned to a *Permanent Virtual Circuit (PVC)* endpoint in a frame relay network. *DLCI* identifies a particular *PVC* endpoint within a user's access channel in a frame relay network and has local significance only to that channel. |

## Overview

This Policy is to protect Montego Pet Nutrition's electronic information from being inadvertently compromised by authorised employees connecting to the Montego Pet Nutrition network locally and remotely via *VPN*.

## Purpose

The purpose of this Policy is to define standards for connecting to Montego Pet Nutrition's network from any host. These standards are designed to minimise the potential exposure to Montego Pet Nutrition from damages, which may result from the unauthorised use of Montego Pet Nutrition resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Montego Pet Nutrition internal systems, etc. Remote access implementations that are covered by this Policy include, but are not limited to *DSL, VPN, SSH* and fibre modems, etc.

## Audience

This Policy applies to all Montego Pet Nutrition employees, volunteers, Directors, contractors, vendors, and agents with a computer or workstation used to connect to the Montego Pet Nutrition network.

This Policy applies to remote access connections used to do work on behalf of Montego Pet Nutrition, including reading or sending emails and viewing *intranet* resources.

## Policy Detail

### Network Security

- Users are permitted to use only those network addresses assigned to them by Montego Pet Nutrition's IT Department, or designee.

- All remote access to Montego Pet Nutrition will either be through a secure *VPN* connection on a Montego Pet Nutrition-owned device that has up-to-date anti-virus software, or on approved mobile devices (see the Montego Pet Nutrition *Owned Mobile Device Acceptable Use and Security Policy* and the *Personal Device Acceptable Use and Security Policy*).
- Remote users may connect to Montego Pet Nutrition Information Systems using only protocols approved by IT.
- Users inside the Montego Pet Nutrition *firewall* may not be connected to the Montego Pet Nutrition network at the same time a remote connection is used to an external network.
- Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the Montego Pet Nutrition network without Montego Pet Nutrition IT approval.
- Users must not install network hardware or software that provides network services without Montego Pet Nutrition IT approval.
- Non-Montego Pet Nutrition computer systems that require network connectivity must be approved by Montego Pet Nutrition IT.
- Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, Montego Pet Nutrition users must not run password-cracking programs, *packet sniffers*, network *mapping tools*, or *port scanners* while connected in any manner to the Montego Pet Nutrition network infrastructure. Only the IT Department, or designee, is permitted to perform these actions.
- Users are not permitted to alter network hardware in any way.

### Remote Access

It is the responsibility of Montego Pet Nutrition employees, volunteers, Directors, contractors, vendors, and agents, with remote access privileges to Montego Pet Nutrition's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to Montego Pet Nutrition.

General access to the Internet, through the Montego Pet Nutrition network, is permitted for employees for business purposes. Montego Pet Nutrition employees are responsible to ensure that they:

- Do not violate any Montego Pet Nutrition Policies
- Do not perform illegal activities
- Do not use the access for outside business interests
- Montego Pet Nutrition employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this Policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of Montego Pet Nutrition's network:

- *Virtual Private Network (VPN)*
- Wireless Communications

*Dial-in* modem usage is not a supported or acceptable means of connecting to the Montego Pet Nutrition network.

## Requirements

- Secure remote access must be strictly controlled. Control will be enforced with *Multifactor Authentication (MFA).*
- Montego Pet Nutrition employees, volunteers, Directors, and contractors should never provide their login or email password to anyone, including family members.
- Montego Pet Nutrition employees, volunteers, Directors and contractors with remote access privileges:
  - Must ensure that their computer, which is remotely connected to Montego Pet Nutrition's corporate network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
  - Must not use non-Montego Pet Nutrition email accounts (i.e., *Hotmail, Yahoo, AOL*), or other external resources to conduct Montego Pet Nutrition business, thereby ensuring that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for *split-tunnelling* or *dual-homing* is not permitted at any time.
- For remote access to Montego Pet Nutrition hardware, all hardware configurations must be approved by IT.
- All hosts that are connected to Montego Pet Nutrition's internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.
- Organisations or individuals who wish to implement non-standard Remote Access Solutions to the Montego Pet Nutrition production network must obtain prior approval from IT.

## Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for *Remote Access IPsec* or *L2TP Virtual Private Network (VPN)* connections to the Montego Pet Nutrition corporate network. This applies to implementations of *VPNs* that are directed through an *IPsec Concentrator.*

This applies to all Montego Pet Nutrition employees, volunteers, Directors, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilising *VPNs* to access the Montego Pet Nutrition network.

Approved Montego Pet Nutrition employees, volunteers, Directors and authorised third parties (customers, vendors, etc.) may utilise the benefit of a *VPN* on a Montego Pet Nutrition device, which is a "user-managed" service. This means that the user is

responsible for selecting an *Internet Service Provider (ISP)*, coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

- It is the responsibility of employees or volunteers, Directors, with *VPN* privileges, to ensure that unauthorised users are not allowed access to Montego Pet Nutrition's internal networks.
- *VPN* use is controlled using a multi-factor authentication paradigm.
- When actively connected to the corporate network, *VPNs* will force all traffic to and from the PC over the *VPN tunnel*; all other traffic will be dropped.
- *VPN gateways* will be set up and managed by Montego Pet Nutrition IT.
- All computers connected to Montego Pet Nutrition's internal networks via *VPN*, or any other technology must use up-to-date, anti-virus software applicable to that device or platform.
- *VPN* users will be automatically disconnected from Montego Pet Nutrition's network after thirty (30) minutes of inactivity. The user must then log on again to reconnect to the network. *Pings* or other artificial network processes are not to be used to keep the connection open.
- The *VPN concentrator* is limited to an absolute connection time of twenty-four (24) hours.
- To ensure protection from viruses, as well as protection of member data, only Montego Pet Nutrition-owned equipment or non-Montego Pet Nutrition devices following the *Personal Device Acceptable Use and Security Policy (BYOD)* will have *VPN* and Remote Access.
- Only IT-approved *VPN* clients may be used.
- By using *VPN* technology, users must understand that their machines are an extension of Montego Pet Nutrition's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

## VPN Encryption and Authentication

All computers with wireless *LAN* devices must utilise a Montego Pet Nutrition-approved *VPN* configured to drop all unauthenticated and unencrypted traffic and will be provisioned with *split-tunnelling* disabled.

As with all Montego Pet Nutrition computers, *Windows*, or other *OS* and/or browser Internet proxy settings will be enabled to effectively route Internet access to the device through Montego Pet Nutrition *firewalls* and Internet filters.

To comply with this Policy, wireless implementations must maintain point-to-point hardware encryption of at least 128 *bits*, support a hardware address that can be registered and tracked (i.e., a *MAC address*), and support and employ strong user authentication, which checks against an external database such as *TACACS+, iDiTJS,* or something similar. Any deviation from this practice will be considered on a case-by-case basis.

## VPN Approval, Acceptable Use Review and Acceptance

Approval from the Administrative Director or higher authority is required for a user's *VPN* access account creation. An *Acceptable Use Form* is attached to the *VPN Procedure* maintained by IT and shall be reviewed and signed by each approved user to acknowledge having read and understood the policy.

This form shall in turn be approved, collected, and retained by IT Management before the user's *VPN* account's first use.

## Wireless Communications

Access to Montego Pet Nutrition networks is permitted on wireless systems that have been granted an exclusive waiver by IT for connectivity to Montego Pet Nutrition's Networks.

This section covers any form of wireless communication device capable of transmitting *packet data*. Wireless devices and/or networks without any connectivity to Montego Pet Nutrition's networks do not fall under the review of this Policy.

### 1. Register Access Points and Cards

All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by IT. If they are installed in corporate PCs, all wireless *Network Interface Cards* (i.e., PC cards) used in corporate laptops or desktop computers must be registered with IT.

### 2. Approved Technology

All wireless *LAN* access must use Montego Pet Nutrition-approved vendor products and security configurations.

### 3. Setting the Service Set Identifier (SSID)

The *SSID* shall be configured so that it does not contain any identifying information about the organisation, such as the company name, division title, employee name, or product identifier.

## Review and Acceptance

Montego Pet Nutrition employees who required loan equipment are responsible for the review and acceptance of *IT Policy 16 – Network Security and VPN Acceptable Use* upon approval to remove IT assets.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 17 – PERSONAL DEVICE ACCEPTABLE USE AND SECURITY (BYOD)

### Definitions

| TERM | DEFINITION |
|---|---|
| **Bring Your Own Device (BYOD):** | Privately owned wireless and/or portable electronic handheld equipment. |

### Overview

Acceptable use of *BYOD* at Montego Pet Nutrition must be managed to ensure that access to Montego Pet Nutrition's resources for business is performed safely and securely for participants of the Montego Pet Nutrition *BYOD program*.

A participant in the *BYOD program* includes, but is not limited to:

- Employees
- Contractors
- Partners
- Volunteers
- Related constituents who participate in the *BYOD program*

This Policy is designed to maximise the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

### Purpose

This Policy defines the standards, procedures, and restrictions for end-users who have legitimate business requirements to access corporate data using their device. This Policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the Montego Pet Nutrition *BYOD program* which contains stored data owned by Montego Pet Nutrition, and all devices and accompanying media that fit the following device classifications:

- Laptops, Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any non-Montego Pet Nutrition-owned mobile device capable of storing corporate data and connecting to an unmanaged network

Refer to the *Company and Personally Owned Mobile Device Procedure*.

This Policy addresses a range of threats to, or related to, the use of Montego Pet Nutrition data:

| Threat | Description |
|---|---|
| **Loss** | Devices used to transfer, or transport work files could be lost or stolen. |
| **Theft** | Sensitive corporate data is deliberately stolen and sold by an employee. |
| **Copyright** | Software copied onto a mobile device could violate licensing. |
| **Malware** | Virus, *Trojan Horses*, *Worms*, *Spyware*, and other threats could be introduced via a mobile device. |
| **Compliance** | Loss or theft of financial and/or personal and confidential data could expose Montego Pet Nutrition to the risk of non-compliance with various Identity Theft and Privacy Laws. |

The addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This Policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Montego Pet Nutrition Network.

## Audience

This Policy applies to all Montego Pet Nutrition employees, including full and part-time staff, Directors, volunteers, contractors, freelancers, and other agents who utilise personally owned mobile devices to access, store, back up, relocate, or access any organisation or member-specific data.

Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Montego Pet Nutrition has built with its members, suppliers, and other constituents. Consequently, employment at Montego Pet Nutrition does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

## Policy Detail

This policy applies to:

Any privately owned wireless and/or portable electronic handheld equipment is hereby referred to as *BYOD*. Montego Pet Nutrition grants potential participants of the *BYOD* program the privilege of purchasing and using a device of their choosing at work for their convenience.

Related software that could be used to access corporate resources.

This Policy is intended to protect the security and integrity of Montego Pet Nutrition's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The Audience, as defined above, must agree to the terms and conditions outlined in this Policy to be able to connect their devices to the company network. If users do not abide by this policy, Montego Pet Nutrition reserves the right to revoke this privilege.

The following criteria will be considered initially, and continuously, to determine if the Audience is eligible to connect a personal smart device to the Montego Pet Nutrition network.

- Management's written permission and certification of the need and efficacy of *BYOD* for that employee.
- Sensitivity of data the audience can access.
- Legislation or regulations prohibiting or limiting the use of a personal smart device for Montego Pet Nutrition business.
- Must be listed on the Information Technology Department's list of approved mobile devices.
- Audience's adherence to the terms of the *Bring Your Own Device Agreement* and this Policy and other applicable policies.

## Technical limitations

Other eligibility criteria deemed relevant by Montego Pet Nutrition or IT.

## Responsibilities of Montego Pet Nutrition

- IT will centrally manage the *BYOD program* and devices including, but not limited to, onboarding approved users, monitoring *BYOD* connections, and terminating *BYOD* connections to company resources upon the user's leave of employment or service to Montego Pet Nutrition.
- IT will manage Security Policies, network, application, and data access centrally using whatever technology solutions it deems suitable.
- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to Montego Pet Nutrition and Montego Pet Nutrition-connected

infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts Montego Pet Nutrition's systems, data, users, and members at risk.

- IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the Montego Pet Nutrition infrastructure. To find out if a preferred device is on this list, an individual should contact the Montego Pet Nutrition IT Department, or designee, *Helpdesk*.
- Although IT currently allows only listed devices to be connected to the Montego Pet Nutrition infrastructure, IT reserves the right to update this list in the future.
- IT will maintain Enterprise IT Security Standards.
- IT will inspect all mobile devices attempting to connect to the Montego Pet Nutrition network through an unmanaged network (i.e., the Internet) using technology centrally managed by the IT Department, or designee.
- IT will install the *Mobile VPN Software* required on Smart mobile devices, such as Smartphones, to access the Montego Pet Nutrition network and data.
- Montego Pet Nutrition's IT Department, or designee, reserves the right to:
  - Install anti-virus software on any *BYOD* participating device
  - Restrict applications
  - Limit the use of network resources
  - Wipe data on lost/damaged devices or upon termination from the *BYOD program* or Montego Pet Nutrition employment
  - Properly perform job provisioning and configuration of *BYOD*-participating equipment before connecting to the network.
  - Through policy enforcement and any other means, it deems necessary, to limit the ability of end-users to transfer data to and from specific resources on the Montego Pet Nutrition network.

## Responsibilities of *BYOD* Participants Security and Damages

- All potential participants will be granted access to the Montego Pet Nutrition Network on the condition that they read, sign, respect, and adhere to the Montego Pet Nutrition Policies concerning the use of these devices and services (see Annexure C).
- Before initial use on the Montego Pet Nutrition network or related infrastructure, **all personally owned mobile devices must be registered with IT.**
- Participants of the *BYOD* program and related software for network and data access **will**, without exception:
  - Use secure Data Management Procedures. All *BYOD* equipment, containing stored data owned by Montego Pet Nutrition, must use an approved method of encryption during transmission to protect data.
  - Be expected to adhere to the same Security Protocols when connected with approved *BYOD* equipment to protect Montego Pet Nutrition's infrastructure.
- Montego Pet Nutrition data is not to be accessed on any hardware that fails to meet Montego Pet Nutrition's established enterprise IT Security Standards.

- Ensure that all Security Protocols normally used in the management of data on conventional storage infrastructure are also applied to *BYOD* use.
- Utilise a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to the Montego Pet Nutrition *Password Policy* for additional information.
- Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.
- Passwords and confidential data should not be stored on unapproved or unauthorised non-Montego Pet Nutrition devices.
- Exercise reasonable physical security measures. It is the end user's responsibility to keep their approved *BYOD* equipment safe and secure.
- A device's firmware/operating system **must** be up to date to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.
- Any non-corporate computers used to synchronise with *BYOD* equipment will have installed anti-virus and anti-*malware* software deemed necessary by Montego Pet Nutrition's IT Department, or designee. Anti-virus signature files must be up to date on any additional client machines – such as a home PC – on which this media will be accessed.
- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.
- If A) any *BYOD* device is lost or stolen, immediately contact Montego Pet Nutrition IT; and, if B) any *BYOD* device is scheduled to be upgraded or exchanged, the user must contact IT in advance. IT will disable the *BYOD* and delete associated company data.
- *BYOD* equipment that is used to conduct Montego Pet Nutrition business will be utilised appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.
- Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with under Montego Pet Nutrition's overarching *Security Policy*.
- The user agrees to and accepts that his or her access and/or connection to Montego Pet Nutrition's networks may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains Montego Pet Nutrition's highest priority.
- Employees, Partners, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of Montego Pet Nutrition-owned and installed hardware or software without the express approval of Montego Pet Nutrition's IT Department, or designee.
- The **end-user agrees to immediately report**, to his/her manager and Montego Pet Nutrition's IT Department, or designee, **any incident or suspected incidents of**

**unauthorised data access**, data loss, and/or disclosure of Montego Pet Nutrition resources, databases, networks, etc.

## Third-Party Vendors

Third-party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-*malware* software relevant or applicable to a device or platform.

All new connection requests between third parties and Montego Pet Nutrition require that the third party and Montego Pet Nutrition representatives agree to and sign the *Third-Party Agreement*. This agreement must be signed by the Manager of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced Policies. The document is to be kept on file. All non-publicly accessible information is the sole property of Montego Pet Nutrition.

The IT Department, or designee, can supply a non-Montego Pet Nutrition Internet connection utilising a US Cellular hot spot if needed.

## Help and Support

Montego Pet Nutrition's IT Department, or designee, is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department, or designee.

## Organisational Protocol

Montego Pet Nutrition may offer reimbursement of expenses to employees if they choose to use their own mobile devices instead of accepting a Montego Pet Nutrition-issued device. This may vary on the employees' function within the company and will be per the schedule in the associated procedure. Refer to the *Company and Personally Owned Mobile Device Procedure*.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 17 – Personal Device Acceptable Use and Security (BYOD)* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

# BRING YOUR OWN DEVICE (BYOD) AGREEMENT

This *Bring Your Own Device (BYOD) Agreement* is entered into between the User and Montego Pet Nutrition (PTY) Ltd. (Montego Pet Nutrition), effective the date this agreement is executed by Montego Pet Nutrition's Information Technology (IT) Department.

The parties agree as follows:

**Eligibility**

- The use of a supported smart device owned by the User in connection with the Montego Pet Nutrition business is a privilege granted to the User, by Management approval, per the *Personal Device Acceptable Use and Security Policy*.
- A supported smart device is defined as an *Android*- or *IOS*-based cellphone or tablet running a manufacturer's supported version of its operating system.
- If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to Montego Pet Nutrition and ensure the data remains secure.
- In the event of a security breach or threat, Montego Pet Nutrition reserves the right, without prior notice to the User, to disable or disconnect some or all *BYOD* services related to the connection of a personal smart device to the Montego Pet Nutrition network.

**Reimbursement Considerations**

- Montego Pet Nutrition offers a fixed reimbursement to eligible Users starting the month following *BYOD* enrolment. Reference the *Company and Personally Owned Mobile Device Procedure* (Policy 5 and 17) for the reimbursement schedule.
- The User is personally liable for the device and carrier service.
- Accordingly, Montego Pet Nutrition will NOT reimburse the User, over and above the monthly reimbursement, for any loss, cost, or expense associated with the use or connection of a personal smart device to the Montego Pet Nutrition network. This includes, but is not limited to, expenses for voice minutes used to perform Montego Pet Nutrition business, data charges related to the use of Montego Pet Nutrition services, expenses related to the text or other messaging, cost of handheld devices, components, parts, or data plans, cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by Montego Pet Nutrition, loss related to unavailability of, disconnection from, or disabling the connection of a smart device to the Montego Pet Nutrition network, and loss resulting from compliance with this Agreement or applicable Montego Pet Nutrition Policies.

**Security Considerations and Acceptable Use**

- Compliance by the User with the following Montego Pet Nutrition Policies, published elsewhere and made available, is mandatory
  - Acceptable Use of Information Systems
  - Personal Device Acceptable Use and Security

- and other related policies including, but not limited to, Anti-Virus, E-Mail, Network Security, Password, Safeguarding Member Information, and Telecommuting.

- The User of the personal smart device shall not remove sensitive information from the Montego Pet Nutrition Network, attack Montego Pet Nutrition assets or violate any of the *Security Policies* related to the subject matter of this Agreement.

**Support**

Montego Pet Nutrition will offer the following support for the personal smart device:

- Connectivity to Montego Pet Nutrition servers, including email and calendar
- Security services, including policy management, password management
- Decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), or change of ownership.

Montego Pet Nutrition is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system outages that result in a failure of connectivity to the Montego Pet Nutrition network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the Montego Pet Nutrition network, programming and other errors, *bugs*, viruses, and other software or hardware failures resulting in the partial or complete loss of data, or which render the smart device inoperable.

**DISCLAIMER**

Montego Pet Nutrition expressly disclaims, and the User releases Montego Pet Nutrition from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of the Agreement.

**Device Description:**

| | |
|---|---|
| **Device Make:** | |
| **Device Model:** | |
| **Device Serial Number:** | |
| **Device IMEI Number:** | |

_____ _____

SIGNATURE: USER DATE

_____ _____

SIGNATURE: IT DEPARTMENT MANAGEMENT DATE

## Policy 18 – PASSWORD

### Definitions

| TERM | DEFINITION |
|---|---|
| **Application Administration Account:** | Any account that is for the administration of an application (i.e., *SQL* database administrator, etc.). |
| **Password:** | A string of characters that serve as authentication of a person's identity, which may be used to grant or deny access to private or shared data. |
| **Strong Password:** | A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system.<br><br>Typically, the longer the password, the stronger it is. It should never be a name, a dictionary word in any language, an acronym, a proper name, or a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on. |

### Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Montego Pet Nutrition's entire corporate network. As such, all Montego Pet Nutrition employees, directors and volunteers (including contractors and vendors with access to Montego Pet Nutrition systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### Purpose

The purpose of this Policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

### Audience

This Policy applies to all personnel, directors and volunteers who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any Montego Pet Nutrition facility, and has access to the Montego Pet Nutrition network, or stores any non-public Montego Pet Nutrition information.

## Policy Detail

### User Network Passwords

Passwords for Montego Pet Nutrition network access must be implemented according to the following guidelines:

- Passwords must be changed every ninety (90) days
- Passwords must adhere to a minimum length of ten (10) characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (! @#$%^&*_+=?/~';',<>|\)
- Passwords must not be easily tied back to the account owner such as username, ID number, nickname, relative's name, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for one (1) year

### System-Level Passwords

All system-level passwords must adhere to the following guidelines:

- Passwords must be changed at least every six (6) months
- All administrator accounts must have 12-character passwords which must contain three (3) of the four (4) items:
  - upper case (ABC), lower case (abc), numbers (123), and special characters (@#*).
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the *Password Policy* for the sake of ease of use.

### Password Protection

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Montego Pet Nutrition information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, "my family name").
- Montego Pet Nutrition passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office.
- Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.

- If the security of an account is in question, the password must be changed immediately.
- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the passwords and protect them
  - Report the discovery to IT
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts, or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- Security tokens (i.e., smartcards, RSA hardware tokens, etc.) must be returned upon demand or termination of the relationship with Montego Pet Nutrition.

## Application Development Standards

Application developers must ensure their programs follow security precautions in this policy and industry standards.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 18 – Password* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 19 – PATCH MANAGEMENT

### Overview

*Patch Management* at Montego Pet Nutrition is required to mitigate risk to the confidential data and the integrity of Montego Pet Nutrition's systems.

*Patch Management* is an effective tool used to protect against vulnerabilities, a process that must be done routinely, and should be as all-encompassing as possible to be most effective. Montego Pet Nutrition must prioritise its assets and protect the most critical ones first; however, it is important to ensure patching takes place on all machines.

### Purpose

- **Security vulnerabilities** are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing Montego Pet Nutrition at risk. To effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.
- Given the number of computer workstations and servers that comprise the Montego Pet Nutrition network, it is necessary to utilise a comprehensive *Patch Management Solution* that can effectively distribute security *patches* when they are made available. Effective security is a team effort involving the participation and support of every Montego Pet Nutrition employee and the Partners.
- This Policy is to assist in providing direction, establishing goals, enforcing governance, and outlining compliance.

### Audience

This Policy applies to all employees, contractors, consultants, temporaries, and members at Montego Pet Nutrition.

This Policy applies to all equipment that is owned or leased by Montego Pet Nutrition, such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this Policy is mandatory.

### Policy Detail

- Many computer operating systems, such as *Microsoft Windows, Linux*, and others, include software application programs that may contain security flaws.
- Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the Montego Pet Nutrition Network, and all computers connected to it. Almost all operating systems and many software applications have periodic security *patches*, released by the vendor, that

need to be applied. *Patches,* which are security-related or critical, should be installed as soon as possible.

- If a critical or security-related *patch* cannot be centrally deployed by IT, it must be installed promptly using the best resources available.
- Failure to properly configure new workstations is a violation of this Policy.
- Disabling, circumventing, or tampering with Patch Management Protections and/or Software constitutes a violation of policy.

## Responsibility

- The Manager of IT is responsible for providing a secure network environment for Montego Pet Nutrition. It is Montego Pet Nutrition's policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to Montego Pet Nutrition's Network, have the most recent operating system, security, and application *patches* installed.
- Every user, both individually and within the organisation, is responsible for ensuring the prudent and responsible use of computing and network resources.
- IT is responsible for ensuring all known and reasonable defences are in place to reduce network vulnerabilities while keeping the network operating.
- IT Management and Administrators are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches. Monitoring will include, but not be limited to:
    - Scheduled third-party scanning of Montego Pet Nutrition's Network to identify known vulnerabilities.
    - Identifying and communicating identified vulnerabilities and/or security breaches to Montego Pet Nutrition's Manager of IT.
    - Monitoring *Computer Emergency Readiness Team (CERT),* notifications, and Web sites of all vendors that have hardware or software operating on Montego Pet Nutrition's network.
- The IT Security and System Administrators are responsible for maintaining the accuracy of *Patching Procedures* which detail what, where, when, and how to eliminate confusion, establish a routine, provide guidance, and enable practices to be auditable.
- Documenting the implementation details provides the specifics of the *Patching Process*, which includes specific systems or groups of systems and the timeframes associated with patching.
- Once alerted to a new *patch,* IT Administrators will download and review the new *patch*. The *patch* will be categorised by criticality to assess the impact and determine the installation schedule.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 19 – Patching* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 20 – PHYSICAL ACCESS CONTROL

### Definitions

| TERM | DEFINITION |
|---|---|
| **Information systems:** | This is any combination of information technology and individuals' activities using that technology, to support operations management. |
| **Display mechanisms:** | A monitor on which to view output from an information system. |

### Overview

*Physical Access Controls* define who is allowed physical access to Montego Pet Nutrition facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems.

Without *Physical Access Controls*, the potential exists that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

### Purpose

- This Policy applies to all facilities of Montego Pet Nutrition, within which information systems or information system components are housed. Specifically, it includes:
  - Data centres or other facilities for which the primary purpose is the housing of IT infrastructure.
  - Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure.
  - Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure.

### Policy Detail

- Access to facilities, information systems, and information system display mechanisms will be limited to authorised personnel only. The authorisation will be demonstrated with authorisation credentials (badges, identity cards, fingerprints, etc.) that have been issued by Montego Pet Nutrition.
- Access to facilities will be controlled at defined access points with the use of a card or fingerprint reader and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorised personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorisation, and all deliveries and removals will be logged.

- A list of authorised personnel will be established and maintained so that newly authorised personnel are immediately appended to the list and that personnel who have lost authorisation are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.
- If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorisation, must be positively identified, and must have their authorisation verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 20 – Physical Access Control* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 21 – CLOUD COMPUTING ADOPTION

### Definitions

| TERM | DEFINITION |
|---|---|
| **Cloud computing:** | Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or *cloud* provider interaction. |
| **Public cloud:** | This is based on the standard *cloud* computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public *cloud* services may be free or offered on a pay-per-usage model. |
| **Private Cloud:** | Is based on the standard *cloud* computing model but uses a proprietary architecture at an organisation's in-house facilities or uses an infrastructure dedicated to a single organisation. |
| **Financial information:** | Is any data for Montego Pet Nutrition, its employees, members, or other third parties. |
| **Intellectual property:** | Is any data that is owned by Montego Pet Nutrition or provided by a third party that would not be distributed to the public. |
| **Other non-public data or information:** | Are assets deemed the property of Montego Pet Nutrition. |
| **Other public data or information:** | Are assets deemed the property of Montego Pet Nutrition. |
| **Personally Identifiable Information (PII):** | Is any data that contains personally identifiable information concerning any members, employees, or other third parties. |

### Overview

*Cloud Computing* would allow Montego Pet Nutrition to take advantage of technologies for storing and/or sharing documents and other files, and virtual on-demand computing resources. *Cloud Computing* can be beneficial in reducing costs and providing flexibility and scalability.

## Purpose

The purpose of this Policy is to ensure that Montego Pet Nutrition can potentially make appropriate *cloud adoption* decisions and at the same time does not use, or allow the use of, inappropriate *cloud* service practices. Acceptable and unacceptable *cloud adoption* examples are listed in this Policy.

All other *cloud* use cases are approved on a case-by-case basis.

## Policy Detail

It is the policy of Montego Pet Nutrition to protect the confidentiality, security, and integrity of each member's non-public personal information. Montego Pet Nutrition will take responsibility for its use of *Cloud Computing* services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best interest of Montego Pet Nutrition. This Policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to Montego Pet Nutrition data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy.
- Explicit procedures for all handling of Montego Pet Nutrition information regardless of the storage, sharing or computing resource schemes.

## Cloud Computing Services

The category of *cloud* service offered by the provider has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks.

- *Infrastructure as a Service (IaaS)* is a form of *Cloud Computing* that provides virtualised computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.
- *Software as a Service (SaaS)* is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the *Service Level Agreement (SLA).*
- *Platform as a Service (PaaS)* is a *cloud* computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with

developing and launching an application. Responsibility is likely shared between the customer and the provider.

### Privacy Concerns

There are information security and data privacy concerns about the use of *Cloud Computing* services at Montego Pet Nutrition. They include:

- Montego Pet Nutrition may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.
- Montego Pet Nutrition's dependency on a third party for critical infrastructure and data handling processes.
- Montego Pet Nutrition may have limited *SLAs* for a given provider's services and the third parties that a *cloud* vendor might contract with.
- Montego Pet Nutrition is reliant on vendors' services for the security of the computing infrastructure.

### Diligence

In evaluating the potential use of a particular *cloud* platform, Montego Pet Nutrition will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

### Exit Strategy

*Cloud* services should not be engaged without developing an *Exit Strategy* for disengaging from the vendor or service and integrating the service into business continuity and *Disaster Recovery Plans*. Montego Pet Nutrition must determine how data would be recovered from the vendor.

### Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 21 – Cloud Computing Adoption* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 22 – SERVER SECURITY

### Definitions

| TERM | DEFINITION |
|---|---|
| **File Transfer Protocol (FTP):** | This is a standard Internet protocol for transmitting files between computers on the Internet. |

### Overview

The servers at Montego Pet Nutrition provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for Montego Pet Nutrition. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department, or designee, to secure the hardware against such attacks.

### Purpose

The purpose of this Policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on Montego Pet Nutrition's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (*FTP* servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources

This Policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers if that equipment resides in the *98ontego.co.za domain* or appears to be owned by Montego Pet Nutrition.

The overriding goal of this Policy is to reduce operating risk. Adherence to the Montego Pet Nutrition *Server Security Policy* will:

- Eliminate configuration errors and reduce server outages
- Reduce undocumented server configuration changes that could allow security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect Montego Pet Nutrition data, networks, and databases from unauthorised use and/or malicious attack

Therefore, all server equipment that is owned and/or operated by Montego Pet Nutrition must be provisioned and operated in a manner that adheres to company-defined processes for doing so.

This Policy applies to all Montego Pet Nutrition company-owned, company-operated, or company-controlled server equipment. The addition of new servers, within Montego Pet Nutrition facilities, will be managed at the sole discretion of IT. Non-sanctioned server installations, or the use of unauthorised equipment that manages networked resources on Montego Pet Nutrition property, is strictly forbidden.

## Policy Detail

### Responsibilities

Montego Pet Nutrition's IT Manager has the overall responsibility for the confidentiality, integrity, and availability of Montego Pet Nutrition data.

Other IT personnel members, under the direction of the IT Manager, are responsible for following the Procedures and Policies within IT.

### Supported Technology

- All servers will be centrally managed by Montego Pet Nutrition's IT Department, or designee, and will utilise approved server configuration standards. Approved server configuration standards will be established and maintained by Montego Pet Nutrition's IT Department, or designee.
- All established standards and guidelines for the Montego Pet Nutrition IT environment are documented in an IT storage location.
- The following outlines Montego Pet Nutrition's minimum system requirements for server equipment supporting Montego Pet Nutrition's systems.
- *Operating System (OS)* configuration must follow approved procedures.
    - Unused services and applications must be disabled, except were approved by the IT Manager.
    - Access to services must be logged or protected through appropriate access control methods.
    - Security *patches* must be installed on the system as soon as possible through Montego Pet Nutrition's *Configuration Management Processes*.
    - Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
    - Authorised users must always use the standard security principle of "Least Required Access" to perform a function.
    - System administration and other privileged access must be performed through a secure connection. The root is a user account that has administrative privileges which allow access to any file or folder on the system. Do not use the root account when a non-privileged account will do.

- All Montego Pet Nutrition servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled network access (i.e., offices).

- This Policy is complementary to any previously implemented policies dealing specifically with security and network access to Montego Pet Nutrition's network.

It is the responsibility of any employee of Montego Pet Nutrition who is installing or operating server equipment to protect Montego Pet Nutrition's technology-based resources (such as Montego Pet Nutrition data, computer systems, networks, databases, etc.) from unauthorised use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to Montego Pet Nutrition's public image.

Procedures will be followed to ensure resources are protected.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 22 – Server Security* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 23 – SOCIAL MEDIA ACCEPTABLE USE

### Definitions

| TERM | DEFINITION |
|---|---|
| **Anonymous Content:** | A comment, reply, or post submitted to a Montego Pet Nutrition or affiliate site where the user has not registered and is not logged into the site. |
| **Montego Pet Nutrition Official:** | Is identified as an employee, officer, Board of Directors, or volunteer. |
| **Facebook:** | A free Social Networking Website. |
| **LinkedIn:** | A Social Networking site designed specifically for the business community. |
| **Microblogging:** | A web service that allows the subscriber to broadcast short messages to other subscribers of the service. |
| **Social Media:** | A form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. For purposes of this Policy, "Social Media" includes, but is not limited to, online blogs, chat rooms, personal websites, and social networking sites, such as *Facebook, Twitter, MySpace, LinkedIn, YouTube*, etc.<br><br>The absence of, or lack of, explicit reference to a specific social networking tool does not limit the extent of the application of this Policy. As new online tools are introduced, this Policy will be equally applicable without advance notice. |
| **Twitter:** | A free Social Networking Microblogging service that allows registered members to broadcast short posts called *tweets*. |
| **YouTube:** | A Video-sharing Website on which users can upload, share, and view videos. |
| **Member** | An individual who has an established, ongoing relationship with Montego Pet Nutrition. This includes both members and non-members who have co-signed on loans. Examples of non-members include non-member joint account holders. |

### Overview

The use of external *Social Media* (i.e. *Facebook, LinkedIn, Twitter, YouTube*, etc.) within organisations for business purposes is increasing. Montego Pet Nutrition faces exposure

to a certain amount of information that can be visible to friends of friends from *Social Media*. While this exposure is a key mechanism driving value, it can also create an inappropriate conduit for information to pass between personal and business contacts.

Tools to establish barriers between personal and private networks and tools to centrally manage accounts are only beginning to emerge. Involvement by the IT Department, or designee, for security, privacy, and *bandwidth* concerns is of utmost importance.

## Purpose of Using Social Media

There are several ways Montego Pet Nutrition can benefit from using external (public) *Social Media*, such as *Facebook, LinkedIn,* and *Twitter*.

- **Building a positive image:** Montego Pet Nutrition can use *Social Media* to promote a positive image. While this is particularly important for organisations generally vulnerable to negative press or consumer discontent, it can also be used to boost Montego Pet Nutrition's image within the community.
- **Increasing *Mind Share:*** *Social Media* can reach large audiences at a very low monetary cost, giving Montego Pet Nutrition another medium for promotion and increasing awareness of Montego Pet Nutrition.
- **Improving member satisfaction:** Members who receive more timely and personal service, in the medium that they prefer, will be more satisfied.
- **Gaining member insights**: *Social Media* can be used to monitor public opinion about Montego Pet Nutrition, its products and services, or its competitors.
- **Increasing member retention:** Using *Social Media* builds affinity and loyalty since members are engaged using a medium, they prefer – something Montego Pet Nutrition needs to offer to remain competitive.
- **Increasing revenue**: Use of *Social Media* to create custom network applications (a.k.a. *plug-ins*) for product promotion or integration with Montego Pet Nutrition's online services.
- **Member acquisition:** Use of *Social Media* to respond to member service issues quickly and efficiently. The answer to the problem can be public, making it searchable by other members who have the same request.
- **Disaster Recovery:** Use of *Social Media* to quickly and efficiently eliminate fears and communicate accurate information regarding recovery actions in the event of a disaster.

## Policy Detail

Montego Pet Nutrition encourages the use of *Social Media* as a channel for business communication, consistent with Montego Pet Nutrition's Corporate Marketing and Communications Strategy. It is the Policy of Montego Pet Nutrition to establish guidelines for safe *Social Media* usage to protect Montego Pet Nutrition's information. The safety and confidentiality of information are vital to Montego Pet Nutrition's success.

Montego Pet Nutrition has established this Policy to set parameters and controls related to Montego Pet Nutrition Official's usage of *Social Media* websites.

## Terms and Conditions of Use

All requests for a Montego Pet Nutrition official's use of external *Social Media*, on behalf of Montego Pet Nutrition, must be submitted to the Senior Management Team. Montego Pet Nutrition may allow access to select pre-approved *Social Media* Websites. Montego Pet Nutrition officials may only access these sites in a manner consistent with Montego Pet Nutrition's *Security Protocols* and Montego Pet Nutrition officials may not circumvent *IT Security Protocols* to access *Social Media* sites.

- Use of personal *Social Media* accounts and user IDs, for Montego Pet Nutrition use, is prohibited.
- Use of Montego Pet Nutrition *Social Media* user IDs, for personal use, is prohibited. Use of Montego Pet Nutrition e-mail addresses to register on *Social Media*, *blogs*, or other online tools utilised for personal use is prohibited. Examples of prohibited use of company User IDs include:
  - Downloading and installing *plug-ins* or helper applications such as those that try to access the Montego Pet Nutrition e-mail directory
  - Joining groups using a company user ID for personal reasons
  - Adding personal friends to a Montego Pet Nutrition official's friends list
- Montego Pet Nutrition officials are to acknowledge they have reviewed the *Social Media* service's *Terms of Service (TOS)* or *Terms of User (TOU)*, as applicable. Links for sites are below.
  - **Facebook:** https://www.facebook.com/terms.php
  - **LinkedIn:** http://www.linkedin.com/static?key=user_agreement
  - **Twitter:** http://twitter.com/tos
  - **YouTube:** http://www.youtube.com/t/terms

## Representing Montego Pet Nutrition

Montego Pet Nutrition Senior Management will designate a person or team to manage and respond to *Social Media* issues concerning Montego Pet Nutrition and will determine who will have the authority to contribute content. This person(s)'s responsibilities will include, but are not limited to:

- Managing *Social Media tools* and *channels*.
- Responding to questions internally and externally about the *Social Media* site.
- Addressing problems/providing direction for staff if a user becomes threatening, abusive, or harassing.
- Suggesting changes to this Montego Pet Nutrition *Social Media Policy* when warranted.
- Working with other staff to make sure opportunities aren't overlooked in marketing Montego Pet Nutrition services; and

- Training staff to ensure they understand how to use Montego Pet Nutrition's *Social Media* program.

Montego Pet Nutrition will take the necessary steps to make sure the content complies with applicable laws and regulations.

- All Montego Pet Nutrition officials who participate in *Social Media*, on behalf of Montego Pet Nutrition, are expected to represent Montego Pet Nutrition professionally. Failure to do so could harm Montego Pet Nutrition and could jeopardise a Montego Pet Nutrition official's ability to participate in *Social Media* in the future.
- Montego Pet Nutrition owns all authorised *Social Media* and networking content. Montego Pet Nutrition officials are prohibited from taking, saving, or sending any Montego Pet Nutrition content distributed via social media while employed, separated, serving on the Partners, or terminated by Montego Pet Nutrition.
- New technologies and social networking tools continually evolve. As new tools emerge, this Policy will be updated to reflect the changes.
- Platforms for online collaboration are fundamentally changing the work environment and offering new ways to engage with members and the community. Guiding principles for participating in social media should be followed.
- Post meaningful, respectful comments and refrain from remarks that are off-topic or offensive.
- Reply to comments quickly when a response is appropriate.
- Know and follow the laws that protect member confidentiality at all times.
- Protect proprietary information and confidentiality.
- When disagreeing with others' opinions, keep it professional.
- Know the Montego Pet Nutrition *Code of Conduct* and apply the standards and principles in social computing.

## Personal Blogs and Posts

- Montego Pet Nutrition takes no position on a Montego Pet Nutrition official's decision to start or maintain a *blog* or personal website or to participate in other online *Social Media* activities outside of work. Montego Pet Nutrition officials, identifying themselves as a Montego Pet Nutrition official on a *Social Media*, should ensure their profile and related content are consistent with how they and Montego Pet Nutrition wish for them to present themselves. This includes what the Montego Pet Nutrition official writes about himself/herself and the type of photos he/she publishes.
- Montego Pet Nutrition officials must not reveal proprietary information and must be cautious about posting exaggerations, obscenities, or other characterisations that could invite litigation.
- Montego Pet Nutrition officials must not make public reference to any of the Montego Pet Nutrition-related *Cash or Security Procedures*.
- Montego Pet Nutrition officials who comment on any Montego Pet Nutrition business or policy issue must identify themselves as a Montego Pet Nutrition official in their *blog* or *posting* and include a disclaimer that the views are their own and not those

of Montego Pet Nutrition. When generating content that deals with Montego Pet Nutrition or individuals associated with Montego Pet Nutrition, Montego Pet Nutrition officials should use a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Montego Pet Nutrition".

- Montego Pet Nutrition officials must not use *Social Media* Websites to harass, threaten, discriminate against, disparage, or defame any other Montego Pet Nutrition officials, members, vendors, or Montego Pet Nutrition products, services, or business philosophy.
- Montego Pet Nutrition officials are prohibited from disclosing confidential, proprietary, or otherwise sensitive business or personal information related to Montego Pet Nutrition or any of its Montego Pet Nutrition officials, vendors, or members. Montego Pet Nutrition officials are also prohibited from disclosing any confidential, proprietary, or otherwise sensitive business or personal information that could identify another Montego Pet Nutrition official, vendor, or member without that individual's prior authorisation.
- Montego Pet Nutrition officials should not take any action via *Social Media* Websites or personal blogs that would harm, or is likely to harm, the reputation of Montego Pet Nutrition or any Montego Pet Nutrition officials, members, or vendors.

## Rules of Engagement

- Protecting member information is everyone's number one responsibility. Information that can be used to disclose a member's personal information in <u>any</u> way should never be posted. Members trust Montego Pet Nutrition to protect their financial assets and information.
- Communication in written, audio, or video form will be around for a long time, so consider the content carefully and be judicious. Brand, trademark, copyright, fair use, and privacy laws must be respected. If any employee mentions a financial product in a *blog*, a *tweet*, or another form, Financial Disclosure Laws apply online. The employee must comply with *Advertising Disclosure Regulations* by providing a *link* back to Montego Pet Nutrition's website page that lists the proper disclosures.

What is written, produced, or recorded is ultimately the employee's responsibility.

- Participation in social computing on behalf of Montego Pet Nutrition is not a right and, therefore, needs to be taken seriously and with respect. Failure to comply could put an employee's participation at risk and can lead to discipline. Third-party site's terms and conditions must be followed.
- Denigration of competitors, Montego Pet Nutrition, or Montego Pet Nutrition affiliates is not permitted. Communication should be respectful when inviting differing points of view. Topics like politics or religion are not appropriate for Montego Pet Nutrition communications. Communicate carefully and be considerate; once the words or other materials are out there, they cannot be retracted.
- Personal information belongs to the members of Montego Pet Nutrition. It is their choice to share that information, not Montego Pet Nutrition's. Montego Pet Nutrition

will not publish material without first discussing it with a manager or legal representative.

## Rules of Composition

- Montego Pet Nutrition officials should write and *post* about their areas of expertise, especially as it relates to Montego Pet Nutrition.
- Write in the first person. Talk to the reader as if he/she were a real person in a professional situation.
- Avoid overly composed language.
- Consider content that is open-ended and invites responses.
- Encourage comments.
- Use a *spell-checker*.
- Make the effort to be clear, complete, and concise in the communication. Determine if the material can be shortened or improved.
- If a mistake is made, it must be acknowledged. Be upfront and be quick with the correction. If posting to a *blog*, make it clear if a modification has been done to an earlier post.
- Produce material Montego Pet Nutrition members will value. *Social Media* communication from Montego Pet Nutrition should help its members, partners, and co-workers. It should be thought-provoking and build a sense of community. It should help members improve their knowledge or understand Montego Pet Nutrition or an affiliate better.

Anonymous content is not allowed on Montego Pet Nutrition sites.

## Personal Use of Third-Party Sites During Work Hours

E-mail and Internet access are provided to support Montego Pet Nutrition's business purposes. If these tools are accessed, incidental personal use of them is permitted.

In general, Montego Pet Nutrition will limit the access of *Social Media* sites to Montego Pet Nutrition officials who use them on behalf of Montego Pet Nutrition.

Excessive personal use of any Internet tool during work time is not permitted and access privileges may be revoked for abuse of the system.

## Retaliation is Prohibited

Montego Pet Nutrition prohibits taking negative action against any Montego Pet Nutrition official for reporting a possible deviation from this Policy or for cooperating in an investigation.

Any Montego Pet Nutrition Official who retaliates against another Montego Pet Nutrition official for reporting a possible deviation from this Policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination of employment at Montego Pet Nutrition or removal from the Partners.

## Review and Acceptance

Montego Pet Nutrition employees who required loan equipment are responsible for the review and acceptance of *IT Policy 23 – Social Media Acceptable Use* upon approval to remove IT assets.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 24 – SYSTEMS MONITORING AND AUDITING

### Overview

Systems monitoring and auditing, at Montego Pet Nutrition, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

### Purpose

System monitoring and auditing are used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real-time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of Montego Pet Nutrition. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralised computing capabilities
- Devices that provide centralised storage capabilities
- Desktops, laptops, and other devices that provide distributed computing capabilities
- Routers, switches, and other devices that provide network capabilities
- *Firewall, Intrusion Detection/Prevention (IDP) sensors*, and other devices that provide dedicated security capabilities

### Policy Details

Information systems will be configured to record login/logout and all administrator activities into a Log File. Additionally, information systems will be configured to notify administrative personnel if inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to the IT Manager.

Information systems are to be provided with sufficient primary (online) storage to retain thirty (30) days' worth of log data and sufficient secondary (offline) storage to retain one (1) years' worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

System Logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

System Logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorisation and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 24 – Systems Monitoring and Auditing* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 25 – VULNERABILITY ASSESSMENT

### Overview

Vulnerability assessments, at Montego Pet Nutrition, are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are not only internal and external but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules while retaining business continuity and safety of Montego Pet Nutrition and member data.

### Purpose

The purpose of this Policy is to establish standards for periodic vulnerability assessments. This Policy reflects Montego Pet Nutrition's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

This Policy covers all computer and communication devices owned or operated by Montego Pet Nutrition. This Policy also covers any computer and communications device that is present on Montego Pet Nutrition premises, but which may not be owned or operated by Montego Pet Nutrition. Denial of Service testing or activities will not be performed.

### Policy Detail

The Operating System or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department, or designee, to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the Operating System or environment for information system resources must be identified and corrected to minimise the risks associated with them.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and ensure conformance to Montego Pet Nutrition's *Security Policies*
- Monitor user or system activity where appropriate
- To ensure these vulnerabilities are adequately addressed, the Operating System or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a third-party vendor or using an in-house product.

All data collected and/or used as part of the *Vulnerability Assessment Process* and related procedures will be formally documented and securely maintained.

IT Management will make vulnerability scan reports and ongoing correction or mitigation progress to Senior Management for consideration and reporting to the Partners.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 25 – Vulnerability Assessment* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 26 – WEBSITE OPERATION

### Overview

The Montego Pet Nutrition website provides information to members, potential members, and non-members regarding Montego Pet Nutrition. It is designed to allow members to transact business with Montego Pet Nutrition and assist non-members with information on how to join Montego Pet Nutrition. Montego Pet Nutrition's website may provide links to websites, outside its website, that also serve this purpose.

### Purpose

The purpose of this Policy is to establish guidelines concerning communication and updates of Montego Pet Nutrition's public-facing website. Protecting the information on and within the Montego Pet Nutrition website, with the same safety and confidentiality standards utilised in the transaction of all Montego Pet Nutrition business, is vital to Montego Pet Nutrition's success.

### Policy Detail

To be successful, the Montego Pet Nutrition website requires a collaborative, proactive approach by the stakeholders. All stakeholders share the same broad goals and objectives:

- Support the goals and key initiatives of Montego Pet Nutrition
- Develop content that is member-focused, relevant, and valuable, while ensuring the best possible presentation, navigation, interactivity, and accuracy
- Promote a consistent image and identity to enhance marketing effectiveness
- Periodically assess the effectiveness of web pages

### Responsibility

The Marketing Department is responsible for the website content and ensuring that materials meet legal and policy requirements.

The IT Department, or designee, is responsible for the security, functionality, and infrastructure of the website. The System Administrators will monitor the Montego Pet Nutrition website for response time and to resolve any issues encountered.

### Links

Montego Pet Nutrition is not responsible for and does not endorse, the information on any linked website unless Montego Pet Nutrition's website and/or this Policy states otherwise.

The following criteria will be used to decide whether to place specific links on the Montego Pet Nutrition website. Montego Pet Nutrition will place a link on the website if

it serves the general purpose of Montego Pet Nutrition's website and provides a benefit to its members.

The Montego Pet Nutrition website will not provide links to websites for:

- Illegal or discriminatory activities
- Candidates for the local, district, or national offices
- Political organisations or other organisations advocating a political position on an issue
- Individual or personal home pages

## Security

When a login is required, various forms of multi-factor authentication are implemented to ensure the privacy of member information and the security of their transactions.

The Montego Pet Nutrition website, as well as linked sites, may read some information from the users' computers. The website or linked transactional websites may create and place *cookies* on the user's computer to ensure the user does not have to answer challenge questions when returning to the site. The multi-factor authentication process will still be required at the next login. This c*ookie* will not contain personally identifying information and will not compromise the user's privacy or security.

## Website Changes

Changes to the website will be executed by the Montego Pet Nutrition Marketing Department, another trained and qualified employee, or a specialised firm or individual they may retain, and only with the explicit approval of the senior executive designated. Website changes require two (2) parties to implement. At the time of any significant changes to the website, a compliance review will be conducted by the legal counsel or another reputable third party compliance expert.

## Regulatory Compliance

The Montego Pet Nutrition website must comply with all regulations dealing with the security of member information.

At a minimum, the following disclosures will appear on the website:

- Privacy Policy and Web Privacy Policy
- E-Statements and Disclosures
- Web Links Disclaimer

## Website Design

The Montego Pet Nutrition website maintains a cohesive and professional appearance. While a sophisticated set of services is offered on the website, the goal is to maintain relatively simplistic navigation to ensure ease of use. Security on the website and

protection of member information is the highest priority in the layout and functionality of the site.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 26 – Website Operation* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 27 – WORKSTATION CONFIGURATION SECURITY

### Definitions

| TERM | DEFINITION |
|---|---|
| **Domain:** | In computing and telecommunication in general, a *domain* is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or several network points or addresses. |

### Overview

The workstations at Montego Pet Nutrition provide a wide variety of services to process sensitive information for Montego Pet Nutrition. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department, or designee, to secure the hardware against such attacks.

### Purpose

The purpose of this Policy is to enhance security and quality operating status for workstations utilised at Montego Pet Nutrition. IT resources are to utilise these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

The overriding goal of this Policy is to reduce operating risk. Adherence to the Montego Pet Nutrition's *Workstation Configuration Security Policy* will:

- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect Montego Pet Nutrition data, networks, and databases from unauthorised use and/or malicious attack

Therefore, all new workstation equipment that is owned and/or operated by Montego Pet Nutrition must be provisioned and operated in a manner that adheres to company-defined processes for doing so.

This Policy applies to all Montego Pet Nutrition company-owned, company-operated, or company-controlled workstation equipment. The addition of new workstations, within Montego Pet Nutrition facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or the use of unauthorised equipment that manages networked resources on Montego Pet Nutrition property, is strictly forbidden.

## Policy Detail

### Responsibilities

Montego Pet Nutrition's IT Manager has the overall responsibility for the confidentiality, integrity, and availability of Montego Pet Nutrition data.

Other IT staff members, under the direction of the IT Manager, are responsible for following the Procedures and Policies within IT.

### Supported Technology

All workstations will be centrally managed by Montego Pet Nutrition's IT Department, or designee, and will utilise approved *Workstation Configuration Standards*, which will be established and maintained by Montego Pet Nutrition's IT Department, or designee.

All established standards and guidelines for the Montego Pet Nutrition IT environment are documented in an IT storage location.

The following outlines Montego Pet Nutrition's minimum system requirements for workstation equipment.

*Operating System (OS)* configuration must be by approved procedures.

Unused services and applications must be disabled, except were approved by the IT Manager.

All *Patch Management* to workstations will be monitored through reporting with effective remediation procedures. Montego Pet Nutrition has deployed a *Patch Management Process*; reference the *Patch Management Policy*.

All workstations joined to the Montego Pet Nutrition *domain* will automatically receive a policy update configuring the workstation to obtain future updates from our *Desktop Management System*.

All systems within Montego Pet Nutrition are required to utilise anti-virus, *malware*, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.

All workstations will utilise the Montego Pet Nutrition *domain* so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model to efficiently manage and maintain *System Security Policies* and *Controls*.

Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.

Third-party applications, including browsers, shall be updated, and maintained by the Montego Pet Nutrition *Patch Management Program*.

Any critical security updates for all applications and *Operating Systems* need to be reviewed and appropriate actions were taken by the IT Department, or designee, to guarantee the security of the workstations under the Montego Pet Nutrition *Patch Management Program*.

Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department, or designee, will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.

By default, all workstations joined to the Montego Pet Nutrition *domain* will obtain local security settings through policies.

Workstation setup will be based on a standard image and only pre-approved programs will be permitted on them. This list must be reviewed and approved by the IT Manager.

Wherever possible, the principle of least access will be applied.

This Policy is complementary to any previously implemented policies dealing specifically with security and network access to Montego Pet Nutrition's Network.

It is the responsibility of each employee of Montego Pet Nutrition to protect Montego Pet Nutrition's technology-based resources from unauthorised use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to Montego Pet Nutrition's public image. Procedures will be followed to ensure resources are protected.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 27 – Workstation Configuration Security* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 28 – SERVER VIRTUALISATION

### Definitions

| TERM | DEFINITION |
|---|---|
| **Virtualisation** | The creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device, or network resources. |

### Overview

This Policy encompasses all new and existing workloads.

### Purpose

The purpose of this Policy is to establish server virtualisation requirements that define the acquisition, use, and management of server virtualisation technologies. This Policy provides controls that ensure that enterprise issues are considered, along with business objectives, when making server virtualisation-related decisions.

*Platform Architecture Policies, Standards, and Guidelines* will be used to acquire, design, implement and manage all server virtualisation technologies.

### Policy Detail

Montego Pet Nutrition's IT Manager has the overall responsibility for ensuring that policies are followed to establish contracts and the confidentiality, integrity, and availability of Montego Pet Nutrition data.

Other IT personnel members, under the direction of the IT Manager, are responsible for following the Procedures and Policies within IT.

Montego Pet Nutrition's legacy IT practice was to dedicate one physical server to a single workload. The result of this practice was excessive server underutilisation, an ever-expanding data centre footprint, and excessive data centre power consumption and cost.

Server virtualisation software allows the consolidation of new and existing workloads onto high-capacity servers. Consolidating workloads onto high-capacity servers allows Montego Pet Nutrition to reduce the server inventory, which in turn decreases the data centre footprint and data centre power consumption and cost.

Montego Pet Nutrition will migrate all new and existing workloads from physical servers to virtual machines. Hardware will be retired at such time as planned by IT management or required by incompatibility with *Operating Systems (OS)* and/or workload-specific software updates.

## Server Virtualisation Requirements:

- Support industry-wide open-standards
- Embedded security technology, such as *Trusted Platform Module (TPM)* or other technologies
- Single centralised management console
- Support industry-standard management tools
- Support industry-standard backup and recovery tools
- Interoperate with other platform technologies
- Support industry-standard hardware
- Support industry-standard storage
- Support unmodified guest operating systems
- Functionality to support virtual server management network isolation
- Migrate running guests without interruption
- Add disks to a running guest
- Automatically detect a hardware failure and restart guests on another physical server
- Functionality to configure role-based access for the administrative console
- Support *Lightweight Directory Access Protocol (LDAP)* for authentication and authorisation for administrative console
- Encrypt all interhost and administrative console traffic
- Integrated graphical *Central Processing Unit (CPU)*, memory, disk, and network performance monitoring, alerting, and historical reporting for hosts and guests
- Other industry-standard or best-in-class features as required

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 28 – Server Virtualisation* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## Policy 29 – TELECOMMUTING

### Definitions

| TERM | DEFINITION |
|---|---|
| **Telecommuting:** | A work arrangement in which employees do not commute or travel by bus or car to a central place of work, such as an office building, warehouse, or store.<br><br>*Telecommuters* often maintain a specific office or workspace and usually work from this alternative work site during predefined days of the week. This is differentiated from *teleworking* or *working remotely,* which may refer to *casual* or *occasional remote work* done by a traditional employee while away from their traditional company office. |

### Overview

*Telecommuting* allows employees to work at home. *Telecommuting* is a voluntary work alternative that may be appropriate for some employees and some jobs. This policy is to be read in conjunction with the *Hybrid Work Policy.*

### Purpose

For this Policy, reference is made to the defined *telecommuting* employee who regularly performs their work from an office that is not within a Montego Pet Nutrition building or suite. Casual *telework* by employees or remote work by non-employees is not included herein. Focusing on the IT equipment typically provided to a *telecommuter,* this Policy addresses the *telecommuting* work arrangement and the responsibility for the equipment provided by Montego Pet Nutrition.

### Policy Detail

*Telecommuting* arrangements are made on a case-by-case basis, focusing first on the business needs of the organisation.

The company may provide specific equipment for the employee to perform his/her current duties. This may include computer hardware, computer software, mobile phone, email, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary. To purchase, configure, ship, and install the required equipment to the remote location, the IT Department, or designee, shall be notified in advance of the *telecommuting* start date.

The use of equipment, software, and data supplies, when provided by Montego Pet Nutrition for use at the remote work location, is limited to authorised persons and for purposes relating to Montego Pet Nutrition business. Montego Pet Nutrition will provide

for repairs to or replacement of provided equipment. Damage to equipment owned by Montego Pet Nutrition, which is outside the employee's control, will be covered by the organisation's Insurance Policy.

In the event of such damage, loaner equipment may be provided when available and must be returned upon request.

The IT Department, or designee, will be responsible for all equipment installation, maintenance, security access, support, and necessary training related to Montego Pet Nutrition equipment and software at the remote site, even in the event IT chooses to outsource services. All provided, qualified equipment will be tracked in the *IT Asset Program*.

The employee shall designate a workspace, within the remote work location, for the placement and installation of equipment to be used while *teleworking*. The employee shall maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment. All Montego Pet Nutrition materials should be kept in the designated work area at home and not made accessible to others. All applicable policies for acceptable use, protection of member information, security, reimbursement of business voice and Internet charges, etc., shall be observed. Personally owned equipment may not be connected to Montego Pet Nutrition -owned equipment.

The employee must sign the *Telecommuting Equipment Agreement* document (see Annexture D). When the employee ceases to *telecommute* or is terminated, all Montego Pet Nutrition-owned equipment shall be returned to the IT Department, or designee, within five (5) business days.

## Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 29 – Telecommuting* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## TELECOMMUTING EQUIPMENT AGREEMENT

This document is to inventory the equipment used for the employee listed below at a remote location that has been approved by the employee's manager.

| | | | |
|---|---|---|---|
| **Employee Name:** | | **Employee's Manager** | |
| **Position** | | **Telecommuting Start Date** | |
| **The employee's alternative worksite is located at the following address:** | | | |
| **Worksite Address:** Street, Suburb, City, Province | | | |
| **Phone Number:** | | | |
| **E-mail Address:** | | | |

The employee understands and agrees to the following:

- The employee is responsible for securing the equipment provided to the employee by the Montego Pet Nutrition IT Department, or designee.
- No personally owned equipment may be connected to the Montego Pet Nutrition-owned equipment.
- This equipment is the sole and exclusive property of Montego Pet Nutrition.
- Except for normal wear and tear, the employee is liable for the condition of the equipment and any damages caused by any misuse, negligence, and/or unauthorised use of the equipment.
- The employee will not modify any Montego Pet Nutrition equipment without written authorisation from the IT Department, or designee.
- In the event of equipment failure, the employee will notify the IT Department, or designee, as soon as possible. Montego Pet Nutrition may supply temporary equipment in the event of equipment failure.
- All equipment provided by Montego Pet Nutrition is provided exclusively for use in providing services to Montego Pet Nutrition. Only the employee may use the equipment and only for Montego Pet Nutrition business-related purposes.
- Within five (5) business days after the employee ceases to telecommute or after the termination of employment at Montego Pet Nutrition, the employee shall return all supplied equipment to the IT Department, or designee. If it should become necessary for Montego Pet

Nutrition to resort to legal or other means to recover its equipment, the employee agrees to pay all related costs and attorneys' fees that may be incurred by Montego Pet Nutrition.

- The employee has read, understands, and acknowledges this agreement by signing below.

| | |
|---|---|
| SIGNATURE: EMPLOYEE | DATE |
| SIGNATURE: MANAGER | DATE |
| SIGNATURE: IT MANAGER | DATE |

cc: Manager File

## Policy 30 – INTERNET OF THINGS

### Definitions

| TERM | DEFINITION |
|---|---|
| **Internet of Things (IoT):** | Refers to network or Internet-connected devices such as appliances, thermostats, monitors, sensors, and portable items that can measure, store, and transmit information. The *IoT* connects billions of devices to the Internet and involves the use of billions of data points, all of which need to be secured. |
| **Data points:** | A discrete unit of information. Any single fact is a *data point*. |

### Overview

*IoT* devices may be business-oriented, consumer-based, or a hybrid of both. The devices may be company-provided or employee-owned, such as through a *BYOD policy*.

### Purpose

The purpose of this Policy is to establish a defined *IoT* structure to ensure that data and operations are properly secured. *IoT* devices continue making inroads in the business world; therefore, Montego Pet Nutrition must have this structure in place.

### Policy Detail

### IoT Device Procurement

*IoT* devices that are to be used for company operations should be purchased and installed by IT personnel.

Employee-owned *IoT* devices used for business purposes must be used under the policy: *Personal Device Acceptable Use and Security (BYOD).*

The use of all *IoT* devices, whether the company provided, or employee-owned, should be requested via **Annexure E** - *IoT Device Usage Request Form* and submitted to the IT Department, or designee, for approval. Only manager-level employees and above may request the usage and/or procurement of *IoT* devices.

The IT Department, or designee, is responsible for identifying compatible platforms, purchasing equipment, and supporting organisation-provided and authorised *IoT* devices.

## Cybersecurity Risks and Privacy Risk Considerations

Montego Pet Nutrition needs to understand the use of *IoT* because many *IoT* devices affect *cybersecurity* and privacy risks differently than IT devices do. Being aware of the existing *IoT* usage and possible future usage will assist Montego Pet Nutrition in understanding how the characteristics of *IoT* affect managing *cybersecurity* and privacy risks, especially in terms of risk response.

Montego Pet Nutrition needs to manage c*ybersecurity* and privacy risk for *IoT* devices versus conventional IT devices, determining how those risk considerations might impact risk management in general, risk response and particularly mitigation, and identifying basic *cybersecurity* and privacy control Montego Pet Nutrition may want to consider, adapt, and potentially include in requirements when acquiring IoT devices. The *IoT Risk Management Guide* contains insight into the differences in risk between conventional IT devices and *IoT* devices. This document resides in the IT document storage area.

## Review and Acceptance

Montego Pet Nutrition employees who are required to, will be requested to review and accept of *IT Policy 30 – Internet of Things* upon undertaking work of this nature at Montego Pet Nutrition.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.

## ANNEXURE F - IoT DEVICE USAGE REQUEST FORM

### INTERNET OF THINGS (IoT) DEVICE USAGE REQUEST FORM

| | |
|---|---|
| Request Date: | |
| Manager Name: | |
| Department: | |
| Type of Device(s): | |
| | |
| Describe the need for this device: | |
| | |
| | |
| Date needed: | |

SIGNATURE: REQUESTER _____ DATE _____

SIGNATURE: APPROVER _____ DATE _____

Montego
Pet Nutrition

## Policy 31 – WIRELESS (WI-FI) CONNECTIVITY

### Definitions

| TERM | DEFINITION |
|---|---|
| **Wireless Access Point (AP):** | A device that allows wireless devices to connect to a wired network using *Wi-Fi* or related standards. |
| **Keylogger:** | The action of recording or logging the keystrokes on a keyboard. |
| **Wi-Fi:** | A term for certain types of *Wireless Local Area Networks (WLAN)* that use specifications in the *802.11 families*. |
| **Wireless:** | A term used to describe telecommunications in which electromagnetic waves, rather than some form of wire, carry the signal over all or part of the communication path. |

### Overview

This Policy addresses the wireless connection of Montego Pet Nutrition-owned devices in remote locations.

### Purpose

The purpose of this Policy is to secure and protect the information assets owned by Montego Pet Nutrition and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by Montego Pet Nutrition.

Montego Pet Nutrition provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Montego Pet Nutrition grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

### Policy Detail

### Montego Pet Nutrition Wi-Fi Network

The Montego Pet Nutrition *Wi-Fi* network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access Montego Pet Nutrition online products and services. *Wi-Fi* access points, located at the office facilities and in most depot offices, allow for compatible wireless device connectivity.

*Microwaves*, cordless telephones, neighbouring *APs*, and other *Radio Frequency (RF)* devices that operate on the same frequencies as *Wi-Fi* have known sources of *Wi-Fi* signal interference. *Wi-Fi bandwidth* is shared by everyone connected to a given *Wi-Fi AP*.

As the number of *Wi-Fi* connections increases, the *bandwidth* available to each connection decreases and performance deteriorates. Therefore, the number and placement of *APs* in a given building is a considered design decision. Due to many variables out of direct Montego Pet Nutrition control, availability, *bandwidth*, and access are not guaranteed.

The Montego Pet Nutrition *Wi-Fi* network and connection to the Internet shall be:

- Secured with a *passphrase* and encryption, following current industry practice on *Passphrases* will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the *Wi-Fi*.
- Physically or logically separate from the Montego Pet Nutrition production wired *Local Area Network (LAN)* and its resources.
- Provided as a convenience for the use of Montego Pet Nutrition employees, their vendors while visiting Montego Pet Nutrition, the members of Montego Pet Nutrition, and other visitors with Montego Pet Nutrition's express permission via the provision of an appropriate *passphrase*.
- Optionally provided to members and qualifying visitors, by Montego Pet Nutrition staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format.
- Accessed by employees only by the *Acceptable Use Policy* and its cross-referenced policies seen in *Policy 2 - Acceptable Use of Information Systems*.
- Used for access to the Montego Pet Nutrition production *LAN* only for business use and with the approved use of a Montego Pet Nutrition-issued device or *Virtual Private Network (VPN)* connection.

Montego Pet Nutrition's *Wi-Fi* service may be changed, the *passphrase* re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of Montego Pet Nutrition business.

### Public Wi-Fi Usage

When using *Wi-Fi* on a mobile device in a public establishment, some precautions should be followed.

### Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the *firewall*, never perform a download on a public Internet connection, and use strong passwords.

- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all *Wi-Fi* links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given *Wi-Fi* link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared *passphrase* and infinitely better than one without a *passphrase*.
- Consider that one of two similar-appearing *SSIDs* or connection names may be rogue and could have been set up by a hacker. Inquire the manager of the establishment for information about their official *Wi-Fi* access point.
- Avoid free *Wi-Fi* with no encryption. Even if your website or other activity is using *HTTPS* (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open *Wi-Fi* connection (such as at coffee shops, some hotels, etc.).
- Seek out *Wi-Fi* connections that use current industry-accepted encryption methods and that generally will require the obtaining of a *passphrase* from the establishment.
- Consider using your cellphone data plan for sensitive activities rather than untrusted *Wi-Fi*, or your mobile *hotspot* if you have one or have been provided with one.
- If you must use open *Wi-Fi*, do not engage in high-risk transactions or highly confidential communication without first connecting to a *Virtual Private Network (VPN)*.
- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the *locked padlock icon* visible in the corner of the browser window, and make sure the web address begins with *HTTPS://*. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance, passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.
- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, *social media*, and any site where your credit card information is stored).
- If you need to connect to the Montego Pet Nutrition Network and are authorised to do so, choose a trusted and encrypted *Wi-Fi AP*, or use your *hotspot*. In every case, you must use your Montego Pet Nutrition-provided *VPN* at all times. The *VPN* tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous *APs*. Set your device to not connect automatically to public or unknown and untrusted networks.

### Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a *keylogger* to capture your keystrokes or other *malware* to monitor or intercept the device or connection.
- E-mail or originate other messages of a confidential nature or conduct banking or other sensitive activities, and not when connected to an open, unencrypted *Wi-Fi*.
- Allow automatic connection to or connection to the first *Wi-Fi AP* your device finds, as it may be a rogue *AP* set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

### Review and Acceptance

Montego Pet Nutrition employees with access to information systems are responsible for the review and acceptance of *IT Policy 31 – Wireless (Wi-Fi) Connectivity* upon starting work at Montego Pet Nutrition.

New Employee Onboarding and training shall include this Policy at a minimum, and in addition to all other applicable training and orientation material, instructions for acceptance shall be provided at that time.

Kindly complete, initial and sign the *User Acceptance Form* and send to the Human Resources Department to retain on file.