**SECURITY AND ACCEPTABLE USE OF INFORMATION AND INFROMATION TECHNOLOGY**

The use of electronic communication, the internet and computer systems are a regular part of our work environment at [Company Name] (“Company”). Efficiency and access to information are essential in helping us carry out our various tasks and responsibilities. However, any abuse or inappropriate use of these resources, either knowingly or unknowingly can lead to time loss, potential virus transmission, reduced network speed and any number of other operational and legal effects that may be prejudicial to the Company’s activities and/or cause damage to its image and reputation.

It is the responsibility of every User to know these guidelines, and to conduct their activities accordingly.

Definitions

“Computer systems” include programs, networks, printers, modems, faxes, scanners and all computer files, supplies and accessories.

“Information” includes any data relating to the Company or any of its clients, suppliers, agents or representatives that is accessible electronically or otherwise, in whatever form.

“Network” includes the collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information.

“Supervisors” include all individuals who have other Users under their supervision as well as those who are responsible for contractor / consultant access to the Company Network.

“Users” include all Company employees, as well as all service providers, consultants and other workers or entities with direct or indirect access to the Company’s Computer systems and/or who handle Information.

Purpose

This policy outlines the basic requirements for utilizing the Company’s computing resources and for protecting customer, employee, and other Information. It focuses on the appropriate and efficient use of electronic communication, the Internet and Computer systems and provides guidelines outlining each User’s responsibilities and obligations. This policy applies to all Users and Supervisors at the Company.

Handing Information

Users may only handle Information that is relevant to the performance of their job functions. For example, a User may not transmit Information to individuals or Web sites unless the Information is used for transacting authorized Company business. Any User who receives Information that is irrelevant to the performance of their job must immediately tell the sender to discontinue sending Information of this nature.

Users must not initiate or disseminate illegal or inappropriate information, including any of the Information, by any means, including but not limited to Computer systems, e-mail, the Internet, instant messaging, telephone, fax or regular mail.

Protecting Information

Each User is responsible for protecting the confidentiality, integrity, and accessibility of all Information. Unauthorized acts of destruction or any disclosure of any Information are prohibited. Restricted and confidential Information may not be transmitted outside of the Company (e.g., posted on an Internet site/social media, or given to third parties) without the prior written consent to the contrary of the Company’s management team.

Protecting Personal Information

Privacy laws in Canada, such as Canada’s Personal Information Protection and Electronic Documents Act (“PIPEDA”) have been enacted to protect personal information, such as individual names, addresses, phone numbers and identification numbers. All employees are responsible for complying with applicable legislation and the Company’s policy on the Collection, Use and Disclosure of Personal Information.

ACCESS TO COMPANY COMPUTER SYSTEMS AND NETWORK

Supervisors are responsible for granting Users under their supervision access to Company Computer systems. Any changes to or discontinuation of any such access must be immediately reported by the Supervisor to the Company’s IT group.

Users may only connect to Company Computer systems and Network using Company owned devices (e.g., workstations, laptops). The only exception is access via approved Web technologies (i.e. access to e-mail through Web mail). A User may not bring a personally owned laptop on company premises and connect to the Network using their personal device.

Unauthorized access to or use of another User’s computer is strictly prohibited. Users are not permitted to allow any unauthorized person (e.g., consultant, visitor, friend, family member, client, etc.) to use their Internet account, e-mail address, or other Company provided computer resource.

To ensure that all required security software is installed (e.g., anti-virus), all Company owned equipment used to access the Company’s Computer systems and Network must be provided or approved by the IT group. Security related software configurations must not be removed or altered.

Use of Computer Systems

All electronic communication received or sent through the Network or other Company Computer systems is considered to be Company property. As such, the Company possesses exclusive intellectual property rights over all electronically communicated information and content. Without prior written authorization to the contrary from the Company, no User is permitted to save or to transmit information, including any Information, for personal means or on behalf of a third party except for the purposes of the User’s job functions or the Company’s operations. The Company’s electronic communication technology should be used, as a rule, for professional activities only.

All rights to computer and software programs belong exclusively to the Company and cannot be copied or used in any manner without the written consent of the Company. Even the temporary downloading of data and installation of software programs other than those installed by the Company IT group is strictly prohibited, unless there is a prior written authorization to the contrary.

Any Computer systems provided to a User or otherwise made available at work is the property of the Company and must be used only to perform workplace functions. Technical or physical modifications to any Computer systems are strictly prohibited. Any loss or defect associated with any Computer systems or other related items must be reported immediately to the Company’s IT group.

In order to ensure the suitable and appropriate usage of the Internet and of corporate electronic communications, the Company reserves the right to enforce the present policy through verification and surveillance techniques, as well as other control methods at its disposal. In light of the foregoing, information obtained by such means, techniques and mechanisms will not be treated as confidential or private. Under certain circumstances, misuse of the Company’s Computer systems will give rise to progressive discipline, up to and including termination of employment.

Email Use

Users must not engage in any communication which includes inappropriate information, including any Information. Users should only send out information, including any Information, if they are authorized to do so. Furthermore, Users are required to consider the degree of sensitivity of any such information in selecting the most appropriate distribution list. Email accounts that do not belong to the Company may not be used to transmit commercial Information of any type or nature, all of which is strictly confidential and proprietary to the Company.

It is recommended that all e-mails and faxes sent outside the Company contain a notification indicating how messages sent to unintended recipients should be handled. The recommended text is:

“This email and any attachments are for the sole use of the intended recipient(s) and are confidential. If you are not an intended recipient and you have received this e-mail in error, please inform us immediately by email or by telephone at (514) 499-2777 x XXX and permanently delete this email and attachment(s).”

Attachments contained in incoming messages of suspicious or unknown origin should be deleted immediately without being opened, as they may contain viruses. The Company will endeavour to notify Users of known or suspected phishing scams or other unauthorized spam.

Internet Use

Internet use is provided by the Company for business related purposes. Users should not:

* Present their personal opinions on business, political or personal related issues as being or reflecting the opinions of the Company (unless authorized in writing by the Company in advance);
* Disclose any company related or inappropriate information, including any Information, on any Internet posting, bulletin board, news group, blog or chat room
* Access sites with inappropriate information;
* Create a business-related internet website/social media account/blog without the prior written consent of the Company

At all times, Users shall not visit or view internet sites of a defamatory, pornographic, obscene, racist, sexist or religiously prejudiced nature, or those which infringe on individual human rights.

Users will not use electronic communication or any Company Computer system to discriminate, defame, injure, harass or convey defamatory remarks or offensive material that could cause damages or otherwise be prejudicial to others.

Users should be aware that there is no reasonable expectation to privacy in the use of email or internet while in the workplace. The Company reserves the right to randomly monitor the Network and Computer systems and any misuse of the Company’s internet access or email systems may give rise to progressive discipline, up to an including termination of employment.

Passwords

A password is designed for the sole use of the User to whom it is given. It may not be disclosed to another party, except when required by the IT group to repair a computing device or application.

Passwords must be “strong”. Strong passwords have the following characteristics:

* Contain both uppercase and lowercase letters;
* Contain at least one digit, one character of punctuation, as well as letters
* Are at least eight (8) characters long;
* Are not dictionary words in any language;
* Are not based on personal information (date of birth, family name, etc.)

Passwords should never be written down or stored on-line. Passwords to gain access to the Network and Computer systems expire every 60 days, and the last 10 passwords cannot be reused.

All User accounts will be locked after 5 incorrect login attempts. In order to re-gain access to the Network, the User must contact the IT group.

Password protection should be applied to all electronic devices that contain restricted or confidential information, including any Information. In the event that a device cannot be password protected (e.g., USB, flash drive) the data or file must be appropriately protected (i.e. file password protected, encryption).

Unattended Equipment and Information

Reasonable precautions should be taken to protect unattended equipment and Information. Unattended electronic media (e.g., USB devices, backup tapes, etc.) must be locked in a drawer or filing cabinet. When Users leave their workstations unattended they must either log off or activate a password- protected screen saver. By default, the password-protected screen saver will be automatically activated after 15 minutes of computer inactivity.

Use of Company Software

The Company does not allow the use of unauthorized software on its equipment and devices, or to copy software licensed to the Company for personal use. All software must be approved by the IT group and acquired through the authorized purchasing process. This includes free licensed or trial software. Only software required for business purposes may be installed on Company equipment and devices.

Reporting

If you suspect a breach of this Policy and/or unauthorized access or use of Information, or to report computer related events, please contact a member of the IT group immediately at the following number or email address:

* By Phone: [123-456-7891]
* By email: [xyz@company.com]

Unauthorized Behaviours and Usage

The following list are examples of authorized behavior and usage. This list is not intended to be exhaustive of all unauthorized behaviours and usage under this policy.

* Unsecured or abusive Internet or electronic communication usage entailing the transmission of viruses or to increase the volume of network traffic so as to impair the efficiency and the security of computer systems;
* Transmission of confidential, proprietary or privileged Information without the consent of those involved or affected, thereby violating applicable laws pertaining to privacy and to the protection of personal information;
* Transmission of or participation in chain mail (i.e. “send this to all of your friends.”);
* Inappropriate use of distribution lists to communicate personal or irrelevant information to other employees;
* Engaging in illegal, unethical or immoral activities or those which cause damage or are prejudicial to and harm the business affairs, commercial relations and/or image and reputation of Medisys or of any of its clients, patients, suppliers, employees, suppliers, or other personnel, agents and representatives.

Non-Compliance

All Users are bound to uphold the provisions of this policy. In cases of non-compliance, rights of access may be suspended or withdrawn and other disciplinary measures, up to and including termination of employment, may also be taken.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

I have read and understand this letter and have signed below to acknowledge receipt.

Employee Name:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SIGNATURE DATE