Electronic Monitoring and Acceptable Use of SMDHU IT Equipment

Reviewed Date		**Number**	*TQ0101*
Revised Date	*August 24, 2022*	**Approved Date**	*April 26, 2006*

Introduction

While the Employment Standards Act (ESA) requires SMDHU to advise employees of any electronic monitoring of devices or other electronic equipment issued to employees it does not require the employer to provide employees with a right to privacy. SMDHU is required to be transparent about the electronic monitoring of employees and as such, in accordance with the ESA, a complaint alleging a contravention of this policy on electronic monitoring cannot be made, or be investigated by, an employment standards officer of the electronic monitoring by an employer.

The ESA's rules on electronic monitoring do not affect or limit an employer's ability to use information obtained through the electronic monitoring of its employees in any way.

The ESA states that electronic monitoring includes all forms of employee monitoring that is done electronically.

Under the ESA, the employer is required to state in its written policy the purposes for which it may use information obtained through electronic monitoring. However, the ESA does not limit the employer's use of the information to the stated purposes outlined within this policy.

Accordingly, this policy describes appropriate use of the Simcoe Muskoka District Health Unit's computer systems and computerized information including but not limited to computer software and hardware, mobile technologies, electronic mail, electronic documents, operating systems, network connections, internet access and related technologies. The policy applies to all equipment that is owned or leased by the Simcoe Muskoka District Health Unit and all information that is stored on agency owned or operated systems or transmitted by or through agency owned or operated systems.

Purpose

The objective of this policy is to protect the health unit's employees, partners and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly, by outlining the acceptable use of the agency's computer resources. Inappropriate use exposes the health unit to risks including virus attacks, compromise of network systems and services, unauthorized collection, access, disclosure or destruction of information and legal issues and to advise employees they may be monitored while using SMDHU supplied IT equipment and resources.

This policy applies to employees, board members, consultants, volunteers, students and other workers at the Simcoe Muskoka District Health Unit including all personnel affiliated

with third parties. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly.

Legislative Authority

Municipal Freedom of Information and Protection of Privacy Act
Personal Health Information Protection Act
Regulated Health Professions Act
Employment Standards Act, 2000

Policy Definitions and Interpretation

This policy applies to all users involved in the operations of the health unit or provision of services. Any person who accesses or uses the technology infrastructure or uses an electronic product or service provided by Simcoe Muskoka District Health Unit is a ***"user"***.

A "***person"*** includes any individual, person, estate, trust, firm, partnership or corporation. For clarity, user in this policy does not apply to the client.

Computer systems and information includes but is not limited to: computer software and hardware, mobile technologies, electronic mail, electronic documents, operating systems, network connections, internet access and related technologies. This includes all equipment that is owned or leased by the Simcoe Muskoka District Health Unit and all information that is stored on agency owned or operated systems or transmitted by or through agency owned or operated systems.

Policy

Use and Ownership

Simcoe Muskoka District Health Unit's (SMDHU) computer systems and the information stored on computer systems owned or operated by the health unit are under the custody and/or control of the Simcoe Muskoka District Health Unit. These systems are to be used for business purposes only in serving the interests of the agency, and of health unit clients and customers in the course of normal operations.

As a courtesy to employees SMDHU allows users very limited, reasonable personal use of SMDHU's computer systems and mobile devices within defined parameters. All users are responsible for exercising good judgment regarding the reasonableness of very limited personal use. If there is any uncertainty, users will contact their Direct Supervisor or manager. All personal or non-business information saved on, or transmitted by, agency owned or operated devices or a product or service provided by the health unit may be monitored, accessed and viewed by the employer at any time and for any reason.

There is to be no expectation of privacy of any SMDHU business, personal or non-business information whatsoever stored or transmitted on the agency's computer systems or mobile devices by users.

Accordingly, for security, internal investigations, policy compliance, alleged misconduct, employee productivity/efficiency/performance and network maintenance purposes, authorized individuals within the Simcoe Muskoka District Health Unit may at any time and for any reason monitor SMDHU IT equipment, systems and network traffic.

Users are advised that the Simcoe Muskoka District Health Unit reserves the right to monitor and audit any and all computer systems without prior notice to the user including mobile devices owned and operated by the health unit. Information transmitted by these systems including employee productivity and efficiency and any user's personal, non-business, business files, the tracking of websites accessed, e-mails, chats, Teams, ZOOM, voice mails and communications of any nature stored on these systems or technologies may also be monitored and audited without prior notice to the user on a periodic basis.

The information obtained through electronic monitoring may be used to evaluate employee performance, to ensure the appropriate use of employer equipment, and to ensure work is being performed during working hours.

Inappropriate and Unacceptable Uses

Under no circumstances is a user authorized to engage in any activity that is illegal under local, provincial, national or international law while utilizing Simcoe Muskoka District Health Unit-owned or operated computer resources or related services provided by the health unit.

The following activities are strictly prohibited, with no exceptions:

a) Unauthorized collection, use, access, modification, disclosure, disposal destruction of computerized information.
b) Revealing your account password to others or allowing use of your SMDHU accounts or SMDHU computer technology/mobile device by others. This includes family and other household members.
c) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
d) Circumventing a computer system's access controls or disabling a computer system's protection settings including anti virus and browser controls and password protection systems.
e) Violations of the rights of any person or agency 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 Simcoe Muskoka District Health Unit.
f) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Simcoe Muskoka District Health Unit or the end user does not have an active license.
g) Establishing without approval connections for Internet, third party or peer-to-peer (i.e. hotspot).
h) Installing or using computer files and software not licensed by the health unit or approved for use by management and the Information Technology Supervisor or using or copying software or files in a manner inconsistent with applicable license or copyright. This includes but is not limited to the storage or sharing of audio or video files like MP3, WMA, MPG or AVI files.

i) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
j) Using a Simcoe Muskoka District Health Unit computer system to access streaming audio or video content such as internet radio, news video feeds or movie trailers without a clear agency purpose.
k) Installing and or playing games on SMDHU computer technology including mobile devices.
l) Vandalism, which is defined as any malicious attempt to harm or destroy the information of another user, the Internet or other networks.
m) Making fraudulent offers of products, items, or services originating from any Simcoe Muskoka District Health Unit account.
n) Using a Simcoe Muskoka District Health Unit computer system to access, view, store or transmit sexually explicit images, text, cartoons, jokes, or any other form of sexually explicit material or failing immediately to delete such material upon receipt.
o) Using Simcoe Muskoka District Health Unit computer systems for any of the following: threats or intimidation, discrimination or hate, trafficking in firearms or illegal drugs, violence, or gambling.
p) Activities that maliciously interfere with the ability of others to access or use computer systems or computerized information.
q) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
r) Participating in chain email, chat, or file sharing or other activities where the content or audience does not support the agency business.
s) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
t) Any use of Simcoe Muskoka District Health Unit computer systems to conduct or promote a personal business.
u) Any use that is prohibited or restricted by other SMDHU policies.
v) Any other activity that may expose the Simcoe Muskoka District Health Unit to civil liability.

Security Procedures

Users will take all necessary steps to prevent unauthorized access to confidential information.

a) Users must ensure that any credentials (login name, password, key fob etc.) used by the user to directly or indirectly gain access to the products, services or technology infrastructure are safeguarded and nor shared account information.
b) Authorized users are responsible for the security of their passwords and accounts including logging off when leaving a workstation/finishing use of device.
c) Users will not access information or conduct activities under the account of another user unless authorized to do so by the manager.
d) All devices in use will be secured with a password-protected screensaver.

e) Users must immediately notify their Direct Supervisor, the IT help desk and/or system administrator if they suspect or know that any credentials have been or may be breached or compromised.

Enforcement

a) Management will orient users to this policy and ensure users indicate agreement with this policy by signing and dating a copy of the policy. Management will ensure users are aware of and comply with the policy.
b) Management will ensure contractors with access to agency computer systems are oriented to the policy and indicate agreement with this policy by signing and dating a copy of the policy.
c) Human resources will maintain a copy of the acceptable use policy signed by the user in the user's personnel file.
d) The Information Technology Supervisor or designate will authorize access to agency systems following confirmation that the user has signed the acceptable use policy.
e) Users will report breaches of this policy to their Direct Supervisor.
f) Any employee, board member, contractor, consultant, volunteer, student and other worker at the Simcoe Muskoka District Health Unit found to have violated this policy may be subject to disciplinary action, up to and including termination of their relationship with the health unit.
g) Simcoe Muskoka District Health Unit reserves the right to investigate suspected breaches of this policy, and users will cooperate when asked to assist in any such investigation.
h) Simcoe Muskoka District Health Unit may, in its sole discretion, suspend or revoke a user's access to Simcoe Muskoka District Health Unit products, services, or technology infrastructure.
i) Breaches of this policy may result in criminal prosecution, civil liability in addition to any discipline and/or termination of employment.
j) Employees who despite training and orientation continue to have IT security lapses, access links or websites which may be subject to but not limited to malware, ransomware, and/or download and open phishing attachments, give away credentials, allow malicious Multi Factor logins etc., will be subject to progressive corrective action beginning with re training/coaching/a forewarning and then if necessary, discipline up to and including termination.
k) To avoid any unnecessary delays in any IT deemed emergency or urgent Health Unit situations that require immediate IT access and intervention, IT will forward a communication to their Direct Supervisor and the VP HRI with a cc to the SMDHU Privacy Officer outlining what is required to be done and why, so that a paper trail documents any and all actions taken by IT in such emergent situations.

Procedures

Related Policies

Related Forms

TQ0101 (F1) Acceptable Use

Final Approval Signature: _____

Review/Revision History:

September 2010 Policy re-numbered, previous number C4.110

January 11, 2017 – Revised

August 24,2022 Electronic Monitoring Clarification ESA