Category: **Corporate Information Management / Information Technology Policies**	
Subject/Title: Network Acceptable Use Policy	Reference Number: **IMIT - 110**
	Effective Date: 12 February 2008
Approved by: PHSA Executive Leadership Council	Revision Number:

1. PURPOSE / POLICY OBJECTIVES

The purpose of this policy is to clarify acceptable use of the *PHSA network*, *data* and information technology services in order to minimize disruptions, prevent misuse, avert security breaches, and comply with government regulations.

2. BACKGROUND INFORMATION

Network access is a critical mechanism for *PHSA* business. All *data record*s, which includes, but is not limited to, *email*s, *instant messaging*, documents, files, images, audiovisual recordings and any other information stored on *computers*, *server*s and related *devices* owned by the *PHSA*, or that utilize the *PHSA network*, are the property of the *PHSA*. Audit trails can be used to monitor *user* access to *record*s, messages, files or other *data* each time an account accesses the *PHSA network. PHSA* reserves the right to disclose any electronic *record* to law enforcement agencies without notice to the employee who sent or received the *record.*

3. POLICY

All *user*s of the *PHSA computer network* and its resources have a legal and ethical duty to protect the confidentiality, integrity and availability of *PHSA* electronic *data* and *network* services.

Network access to *user*s is provided for the purpose of conducting *PHSA* business, professional development and training of employees. This must always be the primary rational for *network* usage. The language, tone, style and presentation of all *data*, information and *record*s must conform and meet acceptable social and professional standards, as defined in the **PHSA Standard Business Conduct Policy, Respectful Workplace Policy, Code of Ethics Policy and Human Rights Policy.** *Network* usage must be able to survive public scrutiny and/or disclosure.

ACCEPTABLE USE

USER MUST

- Utilize the *PHSA network* and resources for the purpose of conducting *PHSA* business.
- Comply with all applicable *PHSA* policies, Provincial and Federal laws and regulations.
- Protect the confidentiality, integrity and availability of all electronic information.
- Take reasonable steps to ensure that they do not cause offence to others.

PERSONAL USE

Personal use is allowable, but must be limited in number and duration and must not interfere with the performance of official business duties and affect employee productivity as defined by their immediate supervisor, disrupt the *network* system, harm the *PHSA*s reputation and/or be used for any activity considered unacceptable (see below). Users must have no expectation of privacy while utilizing the *PHSA computer network*. Personal use may be removed at any time by management as deemed necessary.

UNACCEPTABLE USAGE

The *PHSA network* must **NOT** be used for:

- Any activity in violation of the **PHSA Human Rights Policy, the Code of Ethics Policy, the Theft, Fraud, Corruption, Non-Compliant Activities Policy, the Standard of Business Conduct Policy and the Respectful Workplace Policy**.
- The intentional alteration or destruction of a *record* for the purpose of evading an access request under the *Freedom of Information and Protection of Privacy* Act or as required under the *Document Disposal Act***.**
- Illegal or unlawful purposes, including, but not limited to, infringement of intellectual property rights, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation and soliciting for pyramid schemes.
- Broadcasting unsolicited personal views on social, political, union or other non-business related matters.
- Activities in a conflict of interest with the *PHSA*.
- Soliciting to buy or sell goods or services for personal gain that is unrelated to the *PHSA*.
- Participating in Internet based gaming activities.
- *Computer* tampering (including, but not limited to, *computer* hacking or gaining unauthorized access to *network* accounts and systems, spreading of *computer virus*es, *worm*s, *adware* or installing *spyware software*). Unauthorized users must not attempt to test the *PHSA network* for potential security weaknesses as this act will be interpreted as misuse.
- Using excessive amounts of Information Management & Information Technology *network* resources and *data* services unless authorized by IMIT.
- Using *network* resources for non-business related *streaming video or audio* services.
- Any activity in violation of the **PHSA IMIT IT Security Policy, the Internet and Electronic Messaging Policy, Electronic Data Policy or the Remote Computing Policy.**

4. RESPONSIBILITIES

MANAGER RESPONSIBILITIES

Managers, or delegates, are responsible for requesting *network access accounts* through the *IT Contact Centre* and determining the appropriate *network* access levels for each individual in their department. *Generic accounts* will not be created unless there is a justified business requirement which cannot be

addressed by other alternatives. Department Heads and an IMIT Director must approve all *generic account* access. It will be the responsibility of the requesting manager to monitor the access and usage of a *generic account*.

Managers and/or Human Resources are responsible for notifying the *IT Contact Centre* of employee transfers, temporary leaves or terminations so that *network account* can be reassessed or deleted.

Managers are responsible for ensuring all employees reporting to them are made aware of the terms and conditions of use set forth in this policy prior to using *network* resources.

Managers, in consultation with the *PHSA* Chief Humans Resources Officer, or PHSA Internal Assurance may request employee usage reports if non-compliance is suspected.

IMIT RESPONSIBILITIES

IMIT will create *user accounts* to access the *PHSA network* and *computer* resources in accordance to management specified job duty requirements.

IMIT will enable a *network account* once a *user* acknowledgment of the **PHSA Network Acceptable Use Policy** has been recorded.

IMIT will monitor the *PHSA network* for resource usage, non-compliance and security breaches and will investigate any wrong doings in consultation with *PHSA* Internal Assurance and the Chief Human Resources Officer. All investigations will be performed on a case by case basis.

USER RESPONSIBILITIES

Any person requiring access to the *PHSA network* must comply with the following statement prior to gaining access to the *PHSA network*.

> "I hereby acknowledge that I have read and understand the **Network Acceptable Usage Policy**. I agree to abide by this policy and make every effort to ensure that persons working under my supervision abide by this policy. I realize that failure to comply with this policy will result in temporary or permanent removal of access to the PHSA network and may lead to disciplinary action up to and including termination, cancellation of contractual arrangement, as well as civil and criminal action."

All *user*s are responsible for taking appropriate action when inappropriate use or non-compliance of this policy is suspected. Please see **PHSA Whistleblower Policy**.

Failure to comply with this policy will result in temporary or permanent removal of access to the PHSA network and may lead to disciplinary action up to and including termination, cancellation of contractual arrangement, as well as civil and criminal action.

5. REFERENCES

PHSA Policy Standard Business Conduct
PHSA Policy Human Rights
PHSA Policy Respectful Workplace
PHSA Policy Code of Ethics
PHSA Policy Theft, Fraud, Corruption, Non-Compliant Activities

PHSA Policy Whistleblower
PHSA Policy IMIT Remote Computing
PHSA Policy IMIT Electronic Data
PHSA Policy IMIT Internet and Electronic Messaging
PHSA Policy IMIT IT Security
Network Acceptable Use Agreement
Freedom of Information and Protection of Privacy Act
Document Disposal Act

6. APPENDIX

Glossary of Terms