Saskatchewan Cancer Agency

DIVISION:	Corporate Services	**POLICY #:**	IM 0002
DEPARTMENT:	Information Management Services	**ISSUE DATE:**	Sept 5, 2008
CATEGORY:	Use of Network, Systems, and Information	**REVISED DATE:**	June 1, 2015
POLICY TITLE:	**Acceptable Use**		

Policy Statement

In order to protect the interests and the operations of the Agency, and to protect the privacy of patients, employees, clients, and individuals, the Agency monitors the use of the SCA infrastructure. Unacceptable use of SCA network, systems and information is prohibited.

Purpose

This policy outlines the acceptable use of IMS infrastructure at SCA; these rules are in place to protect the health and privacy of patients, protect the reputation of employee and the SCA while providing required IT services at agreed target. Inappropriate/unacceptable use exposes the privacy of the patients; compromises the IMS infrastructure to virus attacks and takeover by hackers.

Application

This policy and standards apply to all employees, contractors, consultants, temporary and other workers at SCA, including all personnel affiliated with third parties that utilize information/data either directly or indirectly managed by IMS (including information/data stored on leased or rental resources in Cloud).

All users of SCA's information systems must follow the control matrix as per Standard section of this document. If users see data in any form that is incorrectly classified, it should be reported to their supervisor.

Any employee, agent, consultant, or contractor found to have violated this policy and standards may have their access to Saskatchewan Cancer Agency network and data terminated. They may also be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by an agent, temporary worker, contractor or vendor may result in the termination of their contract or assignment with Saskatchewan Cancer Agency.

Authority

ELT

Information

CIO
VP - Corporate Services
Information Management Services
Human Resources - enforcement

Approved by: _____ Signature	Date: June 10, 2015

Definitions

MS Infrastructure:

- Network (wired and wireless)
- Servers
- Applications
- Workstations/Tablets
- SCA provided technology
- Personal Devices connected to the SCA IMS Infrastructure

Procedure

1.0 Standards

Employees are expected to exercise good judgment regarding personal use of Agency equipment, based on department-specific policies, related IMS policies and management guidance. Electronic communication is subject to The Health Information Protection Act (HIPA), Local Authority Freedom of Information and Protection of Privacy Act and to SCA's policies such as HR-501 Confidentiality Agreement, PRI-0100 – PRI-0800 Privacy Policies, HR-508 Respectful Workplace and HR-509 Code of Conduct.

The following activities are strictly prohibited:

1. 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 SCA.
2. 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 SCA or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a SCA computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any SCA account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior approval from IMS Management.
11. 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.

12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/Intranet/Extranet.
15. Providing information about, or lists of, SCA employees to parties outside SCA without appropriate approval.

Related Policies

1.1 Related Policies

1.2 Supersedes/Replaces:

- IMS 0102 Network Acceptable Use Policy
- IM 0103 Identity and Access Management Policy
- IM 0104 IMS Infrastructure Security Policy
- IM 0105 Mobile device policy
- IM 0107 Antivirus policy
- IM 0108 Hardware & Software Standardization policy
- IM 0119 Email acceptable use policy
- IM 0120 BYOD policy
- IM 0121 Social Media acceptable use policy
- IM 0122 Internet use monitoring and filtering policy

References

2.1