Saskatchewan Cancer Agency

DIVISION:	Corporate Services	**POLICY #:**	IM 0003
DEPARTMENT:	Information Management Services	**ISSUE DATE:**	August 1, 2008
CATEGORY:	User Identity, Authentication and Authorization	**REVISED DATE:**	June 1, 2015
POLICY TITLE:	**Identity and Access Management**		

Policy Statement

All access to SCA's networks, applications and IT services will be controlled through use of User Identity, Authentication and Authorization. Users are strictly prohibited from sharing their user identity by making their authentication(s) available to other users. User activities on networks and systems may be tracked via their user identity.

Permission may be granted to allow access to SCA's applications and network data remotely from outside SCA's network using a Remote Access connection.

Purpose

The purpose of this policy is to define required access control measures to all SCA systems and applications to protect the privacy, security, and confidentiality of SCA information assets and systems, especially highly sensitive systems.

To ensure the security of the applications and data privacy by requiring user to manage their password(s) according to industry's best practices.

Application

This policy applies to all SCA employees, contractors, students, volunteers and other affiliates.

Authority

ELT

Information

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

Approved by: _____ Signature	Date: June 10, 2015

Standards

1.1 Identification

- Uniqueness- Each identifier is unique; that is, each identifier is associated with a single person or other entity; except in case of Generic Id
- One Identifier per Individual- An individual may have no more than one Agency identification number
- Non-Reassignment- Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.
- Identifiers assigned to Temporary Workers will have an expiry date, after which the Temporary Worker will be unable to make use of their login; unless the expiry date has been extended on request of the Department Head where Temporary Worker has been assigned

Active Directory is the authentication service at SCA, with directions to have a "single sign on" for the users IMS will require 3rd party application providers to be able to authenticate and authorize via Active Directory

1.2 Authentication

All systems and applications must use encrypted authentication mechanisms and abide by the following:

- Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable option exits.
- Initial passwords must be provided through a secure and confidential manner and initial passwords must be changed upon first logon
- Passwords must not be stored in clear text or in any easily reversible form.
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset upon installation of the affected application, device, or operating system.

To ensure that passwords are of adequate strength, passwords for users, systems, applications, and devices must meet, to the degree technically feasible, the following Information Security requirements:

Password expiration	Every 90 days
Minimum Length	7 characters
Password Complexity	Enabled
Password History	last 24 passwords
Account Lockout	After 9 unsuccessful consecutive logon attempts
Lockout counter reset	30 Minutes
Lock-Out Duration	Manual unlock required
Screensaver	Idle after 20 minutes, password protected

Where technically supported, users shall be required to change passwords at least every 90 days, to use complex passwords, and not to be able to reuse passwords within 24 iterations.

1.3 Authorization

Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify) based on the **Role** with which user had logged on. The system or application should determine if the user has permission to perform the requested operation.

Users are not permitted to access data unless the Data Owner has given permission through established business processes. The Data Owner is responsible for establishing data access procedures that must include, at a minimum, the following:

- Access request forms must be used to request, change, or delete existing access privileges to SCA systems that contain sensitive information. To maintain the requirements of minimum necessary and least privilege, when a user transfers, all accounts should first be disabled, privileges removed, then accounts re-enabled and privileges added that are required in the user's new role.
- For new accounts and changes to existing accounts, portions of the form must be completed and authorized by the:
    - User's supervisor and/or department head (or designated representative)
    - Data Owner
- For account deletions, report departures in a timely manner when workforce members are reassigned, promoted, or separated. For Termination with cause, deactivation must occur immediately.
- Periodic review of user privileges to ensure access is commensurate with user's current responsibilities, as well as modification, removal or inactivation of accounts when access is no longer required.

It is the manager's responsibility to ensure that all users attend security training (New User Orientation) as well as read and acknowledge the SCA Confidentiality Agreement.

Guidelines

1.1 Password Guidelines

A password that meets or exceeds the following requirements:

Contains characters from at least three of these four character groups:

- Lower case letters
- Upper case letters
- Digits
- Non-alphanumeric symbols

Related Policies

1.1 Related Policies

1.2 Supersedes/Replaces:

- Replaces following Policies & Procedures
- IMS-0103 Access Policy for Temporary Workers
- IMS-0113 Generic ID Policy

- IMS-0117 Password Freshness & Complexity Policy
- IMS-0118 Remote Access Security Policy

References
2.1