Saskatchewan Cancer Agency

DIVISION: QUALITY AND INFORMATION MANAGEMENT

POLICY #: IMS-0110

DEPARTMENT: INFORMATION MANAGEMENT SERVICES

ISSUE DATE: 22/12/2008

CATEGORY: INFORMATION SECURITY

REVISED DATE: 05/04/2012

POLICY TITLE: ENCRYPTION POLICY

Policy Statement When required by Policy IMS-0101 Information Classification Policy, sensitive data must be encrypted for protection against unauthorized disclosure while in storage or in transit.

Purpose To create a set of standards for data encryption used in the SCA.

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

Authority Vice President, Quality and Information Management

Information Provincial Leader, Information Management Services

Approved by: Kevin Signature	Date: April 5/12

Procedure

1.0 Roles and Responsibilities

1.1 Information Management Services

1.1.1. Is responsible for training users with the appropriate use of encryption tools.

1.1.2. Must approve, test and document standard encryption tools based on current industry standards.

1.2 All SCA employees and affiliates

1.2.1. Are responsible for making appropriate use of encryption as required by the classification of the data to be stored, sent or received. See IMS-0101 Information Classification Policy Appendix A.

2.0 Guidelines for Key Management

2.1 Information Management Services must establish strict guidelines for automated Key Management.

2.2 Key length should be long enough to provide the necessary level of protection.

2.3 SCA's key length requirements should be reviewed and upgraded as technology evolves.

2.4 Keys must be stored and transmitted by secure means.

2.5 The key's lifetime must correspond with the sensitivity of the information it is protecting (less secure data may allow for a longer key lifetime, whereas more sensitive data may require a shorter key lifetime), and the frequency of the key usage.

2.6 Keys must be securely backed up or escrowed in case of emergencies.

2.7 Keys must be treated at the highest level possible of data classification and properly destroyed when their lifetimes come to an end.

3.0 Related Policies

3.1 IMS-0101 Information Classification Policy

3.2 IMS-0105 Mobile Computing and Storage Devices Policy

3.3 Supersedes / Replaces: IMS-001-10 Encryption Policy

4.0 References