eHealth Saskatchewan

Security Policy Framework

Version 1
March 1, 2011

DOCUMENT APPROVALS

Nick Giesinger		
Chief Security Officer	**Signature**	**Date**
Brenda Jameson		
A/Chief Executive Officer	**Signature**	**Date**

Table of Contents

0 Overview

Introduction

In today's age of information sharing and availability, information is accessible to a regional, provincial and world-wide audience. Building health information systems that are distributed over the province presents an important need to ensure privacy of personal health information. With such a wide range of opportunities it becomes difficult to guarantee the security of the information. Security models must understand the types of environments that the information must pass through as well as the type of information being transmitted. Information and environments vary in degrees of sensitivity and trust and as such may require additional levels of protection and assurance.

Through the security policies, structured processes are identified and a set of protection levels are established, which then acts as the communication tool necessary to direct security measures to users and stakeholders of the information.

Information security is the protection of data against accidental or malicious disclosure, modification, or destruction. Information should be protected based on its value or sensitivity or criticality to the company, and the risk of loss or compromise.

Security Policy Objectives

The objective of the eHealth Saskatchewan (eHealth) security policies is to create the foundation and structure in which will be used to ensure that a comprehensive security framework can be developed. In that context the security policies enforce rules and regulations through a structured security framework including procedures and technology.

The security policies document will be a living document that allows the health sector enterprise within Saskatchewan, its management team and stakeholders to draw very clear and understandable objectives, goals, rules and formal procedures that help to define the overall security posture and architecture.

The primary objectives of the security policies are:

- The protection, prevention, and detection of malicious activities;
- To assist in the understanding of the potential security exposures, and risks;
- To educate, communicate and promote security responsibilities to all stakeholders;
- To ensure compliance with legislative, privacy and contractual requirements;
- To identify consequences of security policy violations.

This document is written as a security policy collection. Once endorsed by management as a whole, policies and sub-policies within sections four to twelve may be re-visited, revised and re-approved independently of the entire document. It is expected that each policy section and sub-section be re-approved every two years.

The Security Office shall coordinate and conduct assessments and reviews to ensure the Security policies and the IT Security Standards are updated appropriately to correspond with technological changes. Recorded events shall be reviewed and remedies incorporated into these documents as necessary to ensure vulnerabilities are appropriately addressed.

1 Security Policy Scope

This policy applies to any individual, services or entities that have been granted access to the Saskatchewan Electronic Health Record (EHR), Provincial Repositories (PR), Health Information Access Layer (HIAL) information resources, Personal Health Information (PHI), Personal Information (PI), eHealth Financial Information and eHealth Corporate Business Information.

The scope of the security document includes:

Individuals, services and or entities that are:

- contractors;
- consultants;
- external auditors;
- vendors;
- other governmental agencies;
- other third party accesses.

Information resources specific to electronic domain*, which are:

- Applications/software/databases;
- Storage media/removable storage;
- Personal Computers/Laptops/tablets/PDA's/Wireless devices
- Servers/minicomputers/mainframes;
- peripherals;
- Data Centres/service centres/any facilities that house the above defined information.

** It is expected that stakeholders will have local policies to address any hardcopy, written or printed formats of information.*

Components used in the processing of the information:

- Data Components
- Hardware Components
- Software Components
- Personnel Components

Related Environments that will have access to the information:

- Management Environments
- Development Environments
- Production Environments

Physical facilities and locations that will manage and contain the information:

- Call Centers
- Data Centers
- Development Facilities

The Information itself through its lifecycle:

- Initiation Phase
- Construction Phase
- Delivery Phase
- Usage Phase
- Retirement Phase

Security Principles

Security principles must be concerned with both the technical and non-technical issues, combined to satisfy legislative and business requirements. More specifically, the users must be considered at the centre of the security principles, as they are critical to success. If the security designs do not consider the users, failure is guaranteed.

The following security principles should be used to help identify and understand the requirements for the architecture:

- **Authentication:** Proving your identity. To be able to access information, authentication via a password or some combination of tokens, biometrics, and passwords must be

accomplished. In some cases multiple factor authentications maybe required. In that case the questions: Who you are, what you have, what you know, where you are can be used to derive the multiple factor authentication.

- **Authorization:** The act of granting approval. Authorization to information within an application can be based on individual or role based access controls.
- **Encryption:** To encrypt a file by applying a mathematical function that transforms every character in the file into some other character. Encryption renders the file unreadable. This means no one can read the file until it is decrypted. Only the authorized users can decrypt the file.
- **Integrity:** Ensuring the information is protected from unauthorised alteration or destruction, whether accidental or deliberate.
- **Accountability:** The ability to track and monitor activities associated with the access and use of systems, interactive and automated, messaging and online.
- **Non-Repudiation:** The ability to associate specifically to an individual, within a legal framework, access, activities and transactions that can not be disputed.
- **Availability:** The ability of the health information to stay operational and accessible to the system users. Generally this is discussed in terms of uptime. As uptime increases the steps required to ensure fail-over, redundancy and fault tolerance increase.

Non-Compliance

Non-Compliance to these policies by any individuals working on behalf of eHealth may lead to disciplinary action including dismissal if the breach is intentional, major or relates to Personal Health Information. User Organizations and Application Providers will be responsible for implementing similar non-compliance policies for their individuals.

Monitoring

eHealth will put reasonable procedures in place to monitor use and access of eHealth information assets.

Contractors providing service to eHealth have a responsibility for managing, monitoring and auditing access to eHealth information assets based on the data classification of the information assets.

Audit

An impartial annual security review or audit of eHealth's security practices shall be conducted by a qualified independent government agency, manager, or third-party organization in order to measure compliance with eHealth Security Policies and IT Security Standards.

Interpretation

For advice and assistance in interpreting and implementing this policy, the following entities should be contacted:

eHealth Saskatchewan Security Office.
eHealth Saskatchewan Privacy Office.

Exception Management

It is recognized that due to the nature of business conducted within eHealth there may be needs to perform tasks that are seen as non-compliant with the Security Policy framework. When a valid need arises, approval from management and the Security Office will be granted on a case by case basis.

Additional Notes:

2 Normative References

Security Documentation Standard

eHealth has purchased the International Organization for Standardization (ISO) 27001, 27002, 27005, and 27799 documents to be used as a reference. International Organization for Standardization ISO 27xxx series is the most widely recognized security standard which is based upon BS 7799, last published in May 1999. The first version of ISO 17799 was published in December 2000.

It is important to note that the numbering sequenced used in this document follows the ISO 27XXX series. It is in no way intended on being a sequential representation of points or policies. The number system maps directly to the security control objectives as defined by the ISO standard.

ISO 27799 is comprehensive in its coverage of managing security safeguards and controls in the health sector.

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

Asset: anything that has value to the corporation.

Availability: the property of being accessible and usable upon demand by an authorized entity.

Confidentiality: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control: is used as a synonym for 'measure'.

Information security: preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

Information security management system (ISMS): that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. This will include but not be limited to corporate structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity: the property of safeguarding the accuracy and completeness of assets.

Need to Know: (1) The legitimate requirement of a person, or organization, to know, access, or possess sensitive, or classified, information that is critical to the performance of an authorized, assigned mission.
(2) The necessity for access to, or knowledge, or possession of, specific information required to carry out official duties.

Residual risk: the risk remaining after risk treatment.

Risk acceptance: decision to accept a risk.

Risk analysis: systematic use of information to identify sources and to estimate the risk.

Risk assessment: overall process of risk analysis and risk evaluation.

Risk evaluation: process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk management. coordinated activities to direct and control the corporation with regard to risk.

Risk treatment: process of selection and implementation of measures to modify risk.

Security event: an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Security incident: a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Statement of applicability: documented statement describing the control objectives and controls that are relevant and applicable to the corporation's ISMS.

4 Control of Documents

Version	Date	Comments
0.9	February 4, 2011	Initial version as taken directly from the Saskatchewan Health Information Network (SHIN) Security Policy Framework V2.3.3
1.0	March 1, 2011	Revision and Effective date set

5 Security Policy Management

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a) establishing a Security Policy;
b) establishing a Information Security Management System (ISMS);
c) ensuring that ISMS objectives and plans are established;
d) establishing roles and responsibilities for information security;
e) communicating to the corporation the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
f) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);
g) deciding the criteria for accepting risks and the acceptable levels of risk;
h) ensuring that internal ISMS audits are conducted (see 6); and
i) conducting management reviews of the ISMS (see 7).

5.2 Resource management

5.2.1 Provision of resources

The corporation shall determine and provide the resources needed to:

a) establish, implement, operate, monitor, review, maintain and improve an ISMS;
b) ensure that information security procedures support the business requirements;
c) identify and address legal and regulatory requirements and contractual security obligations;
d) maintain adequate security by correct application of all implemented controls;
e) carry out reviews when necessary, and to react appropriately to the results of these reviews; and
f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competence

The corporation shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work effecting the ISMS;
b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;
c) evaluating the effectiveness of the actions taken; and
d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The corporation shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6 Organizational Security

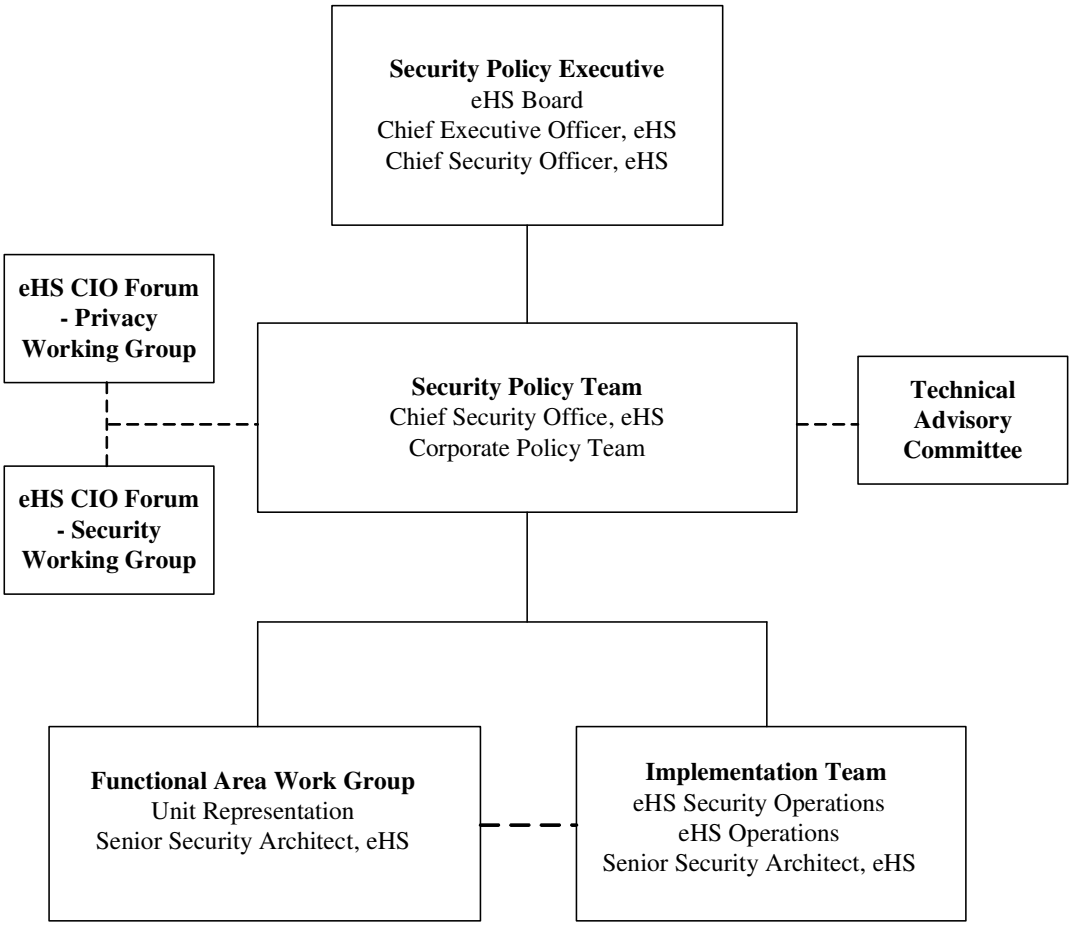
Policies within this section of the framework require the approval from the eHealth Board. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective: To manage information security within eHealth.

eHealth has created a Management Framework to initiate and control the implementation of information security within eHealth.

These policies will engage members from various stakeholder groups: eHealth, Regions, Agencies, and professional bodies. Any policy incorporating organizational roles and responsibilities requires senior leadership approval. The following chart identifies the high level organization of the governance structure and the reporting relationships.

Figure 1.1 High level organizations of the governance structure and the reporting relationships



6.1 Organization Information Security
eHealth Saskatchewan

Subject/Title: *Organization Information Security*	Revision Number: 1.0
Approving Authority: eHealth Executive Management Name: Title: CHIEF EXECUTIVE OFFICER	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate organizational structure to support the standards, processes and procedures that ensure the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

An information security framework must be established to initiate and control the corporation's information security for the following reasons:

- To protect the confidentiality, integrity, availability and value of information in the custody or control of eHealth in a manner that supports public trust and confidence.
- To clarify roles and responsibilities in maintaining the security of information and in the management of situations that may threaten or compromise information security.
- To comply with the provisions of the Freedom of Information and Protection of Privacy Act (FOIPP) and the Health Information Protection Act (HIPA)

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Information Security Organization

Information security is a business responsibility shared by all members of the management team. The management team must ensure that there is clear direction and visible management support for security initiatives. Management is responsible for ensuring the promotion of security within eHealth through appropriate commitment and adequate resourcing.

Members of the management team will include the following:

i. **Executive Management** is the eHealth Board, Chief Executive Officer and Chief Security Officer. The role of management is to provide leadership for protecting the privacy,

confidentiality, and security of personal health information. Responsibilities include assigning adequate resources to information protection issues (e.g., Privacy and Security Officers), supporting educational awareness initiatives, and demonstrating security conscious behaviour at all times ("leading by example"). Other responsibilities would include:

- Obtain corporate commitment, and maintain commitment throughout the life cycle of the policy.
- Ensure that the necessary personnel and resources are available to support the delivery of the policy.
- Approve changes in the scope or the direction of this policy.
- Make key decisions regarding the direction or outcomes of the policy, when the Policy Team cannot reach decisions.
- Review recommendations of the Policy Team, the Technical Advisory Committee (when separate from the Policy Team).
- Communicate objectives, scope, and status of the policy to all stakeholders.
- Responsible for reviewing and monitoring security incidents.
- Define and create ad hoc committees as required.

ii. **Security Officer*** - The role of the security officer is to manage the security function within eHealth, to ensure protection for data in the system and for taking into account privacy requirements when architecting a system. This includes the security of physical and information assets. The security officer will be part of the Security Office and ensures that the three goals of security: confidentiality, integrity, and availability are addressed. The Security Officer requires a sound understanding of the information technologies used within the corporation, an expert knowledge of security technologies and techniques, and a current knowledge of threats and risks to information systems. Responsibilities of the Security Officer can include:

- Establishing security policies and procedures.
- Raising awareness and understanding of the physical, technical and procedural security measures to protect the confidentiality, integrity and availability of information system assets. Helping implement such measures in conjunction with others.
- Conducting Threat Risk Assessments (TRA's) to identify vulnerabilities and recommending appropriate countermeasures.
- Investigating security incidents and taking appropriate follow-up action to prevent future incidents.
- Monitoring information system activity to identify potential security breaches.
- Monitors and reports progress to the Executive Management.
- Working jointly with the Privacy Office to ensure corporate compliance with relevant privacy legislation.
- Working jointly with the Privacy Office and/or Client Relations to investigate and report security incidents and privacy breaches.
- Identifying medical-legal cases so that they can block access to sensitive information if required.
- Working jointly with the Privacy Office and Health Records to collect, store, transfer, and dispose of medical-legal records.

iii. **Privacy Officer*** – This role is to assist management in providing leadership for protecting the privacy of personal health information through specialist skills and advice. This should include knowledge of relevant privacy legislation and fair information principles, privacy processes and technologies, privacy requirements in contractual obligations, and the information needs of workers in eHealth and the health sector in general. Addressing issues of pseudonymity, anonymity, link ability of data and observability of data are all key elements

* Refer to Guidelines for the Protection of Health Information (2004), Canada's Health Informatics Association (COACH) - ISBN 0-9688851-2-8

that privacy architecture and the privacy office needs to address directly. They also need to be tested upon design and deployment. Responsibilities of the Privacy Officer can include:

- Ensuring the corporation complies with relevant privacy legislation.
- Designing and implementing corporate information protection initiatives such as the educational awareness program and the development of policies and procedures. (See the section on Policies and Procedures in the Process chapter.)
- Investigating and reporting privacy breaches and the privacy implications of security breaches in conjunction with Risk Management and/or Client Relations.
- Developing and using assessment and compliance tools in conjunction with Information Technology/Information Management. (See the section on Assessment and Compliance Tools in the Process chapter.)
- Authorizing the release of, and access to, personal health information for research and other non-care related purposes. For example, The Privacy Officer could sit on the Research Ethics Review Board and assist charitable foundations affiliated with the health organization to address privacy issues.
- Responding to client, user or partner queries regarding information management practices.
- Reporting directly to the Chief Executive Officer, President or the Chief Operating Officer about information protection issues.

eHealth will create teams from across the health sector of management and non-management representatives from relevant effected parts to co-ordinate the implementation of information security controls.

These groups will be made up from the following teams:

- **Security Office**
- **Privacy Office**
- **Operations**
- **Security Operations**
- **Technical Advisory Committee**

Security Roles and Responsibilities
For identification of security roles and responsibilities within eHealth refer to eHealth **Security Roles and Responsibilities V1.0.doc**

7 Asset Classification and Control

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective: to maintain appropriate protection of corporate assets.

All major assets, technology assets and information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

7.1.1 Information Assets

eHealth Saskatchewan

Subject/Title: ***Information Assets***	**Revision Number: 1.0**
Approving Authority: eHealth Executive Management **Name:** **Title: Chief Executive Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate asset management and controls to ensure that the information produced or processed by is used appropriately and in conjunction with defined uses and purposes to ensure compliance with legislation.

Scope/ Purpose

The information produced or processed by eHealth must be categorized according to its sensitivity to loss or disclosure. Based on this categorization, policy for allowing access to information or for transmitting information over different networks, including the Internet, can be defined.

All information and physical assets generated or maintained for use within eHealth will be inventoried and documented prior to project implementation. All users of the data must be aware of the information inventory, data models, data classification and the specific usage and management requirements.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

For business purposes, such as health and safety, insurance or financial reasons, inventories of assets will be maintained. An inventory of will be drawn up and maintained of important assets associated with an information system. Each asset is clearly identified together with its current location, which is required to mitigate risk when attempting to recover from system loss or damage. Examples of assets inventoried as part of the information systems are:

- **information assets:** databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information;
- **software assets:** application software, system software, development tools and utilities;
- **physical assets:** computer equipment, communications equipment, magnetic media, other technical equipment, furniture, accommodation;

- **services: computing and communications services, general utilities.**

7.1.2.1 Releasing Source Code

eHealth Saskatchewan

Subject/Title: ***Contributing to the Open Source Community***	**Revision Number: 1.0**
Approving Authority: eHealth Executive Management **Name:** **Title: CHIEF EXECUTIVE OFFICER**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate controls over the development of source code and the related intellectual property to ensure that it retains the copyright and ownership of all eHealth created products and services in compliance with legislation.

Scope/ Purpose

This policy will address the ability for individuals acting on behalf of eHealth to share source code that was internally developed. This applies to any external agent, organization, open source community, or jurisdiction (regional, provincial, or national)

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

All source code assets generated or maintained for use within eHealth will be subject to this policy. All source code that has been developed by internal eHealth resources is the intellectual property of eHealth. Any release of source code beyond eHealth must be approved prior to release. This would include but not limited to: scripts, batch files, applications, applets, and web pages regardless of the platform or tool set used in the creation. Authorship is recognized by the contributors/developers but ownership of all intellectual property will be retained by eHealth.

A request to release source code shall be given in writing to the Chief Executive Officer for consideration. Finial decision on how and who can use the source code assets beyond eHealth is the responsibility of the Chief Executive Officer.

With respect to the Open Source Community, a license agreement must be incorporated as part of the source code. The license agreement must clearly detail that eHealth is the Intellectual Property owner. For additional license agreement information refer to the eHealth **Intellectual Property Right License Agreement Template v.0.1**

7.1.3 Appropriate Use of Assets
eHealth Saskatchewan

Subject/Title: *Appropriate Use of Assets*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure that all assets are used by eHealth authorized individuals for eHealth business as it complies with legislation.

Scope/ Purpose

This policy guides users of the eHealth's Information Technology (IT) infrastructure. It balances the individual's ability to benefit fully from IT with eHealth's need for secure and effectively allocated IT resources.

The networked office has also created the opportunity to access material and use resources in ways that may not be acceptable. Inappropriate use of IT could expose the Government to potential embarrassment and possible litigation. eHealth is committed to ensuring that this valuable resource is not brought into disrepute in the workplace through inappropriate use. Individuals are to follow this policy to ensure that their own use of the eHealth's IT resources is appropriate.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Individuals acting on behalf of eHealth Saskatchewan will follow guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations and policies. eHealth will periodically redefine and enhance these guidelines and policies.

eHealth policies which apply to:

- Freedom of information and protection of privacy;
- Harassment;
- Performance improvement;
- Conflict of interest; and
- Corrective discipline.

also apply when individuals use the eHealth's IT infrastructure. This policy addresses circumstances which are new and evolving, or at least unfamiliar. It augments, rather than replaces, existing eHealth policies. Individuals who violate this policy will be subject to a full range of disciplinary actions.

There are three usage types for eHealth's IT infrastructure: core, incidental, and unacceptable.

CORE

Core uses are activities required to conduct the business of eHealth. They help fulfill eHealth's mandate. eHealth's IT infrastructure primarily exists to facilitate Core eHealth mandate, delivery of the Electronic health Record.

INCIDENTAL

Incidental uses are those which are neither explicitly permitted nor explicitly denied. Incidental applications never require any action or intervention by anyone at the workplace other than their user. Individuals are to cover costs incurred in personal incidental use such as long distance calls or photocopying. Incidental usage that becomes an imposition on others or burdens systems is no longer incidental, but unacceptable, and is not permitted.

UNACCEPTABLE

Unacceptable use impedes the work of others or needlessly squanders IT resources. It may unintentionally damage the IT infrastructure, and affect eHealth's ability to carry out its work. Unacceptable use may generate extra costs. The definition of unacceptable can be drawn back to eHealth's mission, vision and values and information needed to perform the work of the organization. For example, access to objectionable Internet sites may be appropriate to specific investigations, but may be unacceptable and not permitted for general use.

It is unacceptable to:

- Use, copy, or otherwise access anyone else's files without permission.
- Use the eHealth's IT infrastructure for activities that contravene the law, existing policies or regulations.
- Use the eHealth's IT infrastructure for any activities that are offensive or perceived to be offensive.
- Download data or introduce data from an external source such as a diskette without ensuring that it is virus-checked.
- Use any part of the eHealth's IT infrastructure for personal financial gain.
- Infringe copyright or proprietary rights.
- Permit unauthorized access.
- Create or knowingly propagate computer viruses.
- Damage files, equipment, software, or data belonging to others.
- Use or attempt to use unauthorized access methods or abilities.

The above list is not exhaustive.

While eHealth does not prohibit limited incidental use of IT for personal reasons, users should recognize that the primary intention of providing this resource is to support the core work of eHealth.

eHealth's IT infrastructure provides access to outside networks. Individuals may encounter offensive or objectionable material. eHealth does not assume responsibility for the content of any of these outside networks. Without specific authorization, individuals must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment.

Monitoring

Individuals should be aware that computer usage can be traced by site logs and other tracked information. eHealth reserves the right to access the contents of all files stored on its systems and all messages transmitted through its IT infrastructure.

Internet Access

If individuals have access to the Internet through work, they must not intentionally access sites or engage in practices on the Internet that have the potential to bring the public service into disrepute. The individual's access to the Internet is a privilege, not a right. Access entails personal responsibility and individuals are responsible for any activity carried out under their account.

Individuals who use the Internet should be familiar with:

- Copyright laws as they apply to software and electronic forms of information, and
- Applicable libel and slander laws.

The use of the Internet for professional activities and career development need not be directly related to one's current position. Rather, it may relate to the full range of professional, technical and policy issues of interest to the public service. As long as an activity is related to and necessary for the completion of the individual's work, then that activity is generally considered to be an acceptable use of the Internet and is allowed.

The use of the Internet is unacceptable when that use:

- Compromises the privacy of users and their personal data.
- Damages the integrity of a computer system, or the data or programs stored on a computer system.
- Is offensive, or perceived to be offensive.
- Results in personal financial gain for the user.
- Brings the eHealth into disrepute.
- Disrupts the intended use of system or network resources.
- Facilitates unauthorized access attempts on other computer systems.
- Results in the uploading, downloading, modification, or removal of files on the network for which such action is not authorized.

Individuals who access the Internet through eHealth have their on-line experience enhanced by site-blocking. Site blocking prevents access to websites in pre-selected categories. When individuals attempt to visit these sites, a warning screen appears. The software filters Internet content by working in conjunction with an expanding master database of more than 2.6 million sites organized into more than 75 categories.

Blocked categories for eHealth users currently include (but are not limited to):

- Pornography/Adult Content;
- Gambling;
- Racism; and
- Sites that offer web anonymising (proxy avoidance) capabilities.

If the individual attempts to access a website within one of the blocked categories, the request is blocked. Instead of the requested website, a warning screen is displayed on the individual's computer and the incident is logged. These logs are available to the individual's supervisor.

E-Mail

E-mail that is of a personal or transitory nature need not be archived. However, e-mail that is an official record of eHealth is to be retained. Remember that e-mail is accessible under the terms of The Freedom of Information and Protection of Privacy Act.

The Archives Act as it refers to official eHealth records. E-mail is an official record if:

- It was created or received as part of the normal business practices of eHealth and it relates to eHealth's mandate,
- It documents, interprets or otherwise supports eHealth policy, decisions, transactions and events or it contains informational value of significance to eHealth.

Individuals must not attempt to read another person's e-mail unless otherwise authorized. The e-mail system is the property of eHealth. Individuals should have no reasonable expectation of privacy in e-mail transmitted, received and stored on and/or through the eHealth's system. An e-mail is the property of eHealth and is not a private individual communication (whether created or received).

It is unacceptable to send large files such as singing Christmas cards or animated Valentine's greetings as attachments to e-mail - such attachments can seriously affect the performance of the eHealth network. Remember that e-mail is the leading source of computer viruses; be especially suspicious of attachments. Unencrypted e-mail does not protect against viruses. Individuals have a responsibility to put only non-sensitive information in an e-mail. The recipient is responsible for handling the message with respect and securing the sender's permission before forwarding it.

Individuals must have their supervisors' permission before using eHealth's IT resources for large scale distribution of e-mail. The e-mail's subject line should always be filled out. Individuals are encouraged to create separate signature files for personal and official e-mail that is sent from eHealth accounts. The text of the official signature file must list job title, unit, eHealth and telephone or fax number. Personal signature file text must contain a disclaimer indicating that the e-mail does not represent the views of the eHealth Saskatchewan.

The use of individual’s personal HotMail, Gmail, Smartphone’s or any other external e-mail service providers for eHealth official purposes by an individual is considered unacceptable. Forwarding of email to a personal external e-mail service provider is strictly forbidden by an individual. If irresponsible use of web-based e-mail damages eHealth computers and networks, permission to access web-based e-mail from work may have to be reviewed. Individuals who access web-based e-mail with eHealth computers, Mobile Computing Devices (i.e. Personal Digital Assistants (PDA's)), cell phones and networks are to follow the guidelines below.

- Web-based e-mail account names MUST be different from eHealth e-mail account names.
- Web-based e-mail account passwords MUST not be the same as eHealth passwords.
- Passwords MUST follow the Password Management Policy.
- Browsers should be configured to prompt the user before external code is run.
- Passwords MUST NOT be cached in the local browser.
- DON'T configure web-based e-mail to automatically forward to eHealth e-mail accounts.
- DON'T forward any work e-mail (internal, restricted or confidential) to external e-mail accounts.
- NEVER open suspicious or unexpected e-mail attachments.
- DON'T send large attachments.
- Always scan attachments with up-to-date virus software prior to opening.

On-Line Discussion Groups

When joining in public discussion individuals must identify whether they are participating as at a personal level or as a representative of eHealth. Whenever an individual engages in a public discussion through an eHealth account or is identified as being from eHealth, eHealth is reflected in what is written. Even though their messages may contain a disclaimer, such messages should conform to the standards of accuracy, courtesy and propriety.

Games

Games are a common feature of stand-alone computers and computers connected through a local area network, an intranet or the Internet. Using eHealth IT infrastructure to play games during working hours is an unacceptable use of a valuable resource and is not permitted. As well, individuals who waste valuable storage space and damage eHealth networks by playing multi media games are also using IT resources in an unacceptable manner. Computers may come equipped with a few games, solitaire is especially popular. Spending a few minutes playing solitaire over the lunch hour is considered incidental use but individuals are expected to use their common sense and good judgment. As always, "personal use on personal time" is a good rule to follow.

Voice-Mail

Individuals should ensure their recorded voice mail messages are appropriate, informative and timely. If callers reach your voice mail, at a minimum, they must be able to;

- Speak directly with another individual, or
- Leave a message.

Individuals are responsible for the security of their account and their password. They should change their password regularly and take precautions to prevent unauthorized access to their mailbox. Voice mail systems are provided to facilitate the eHealth's core work. Incidental use of voice mail by individuals is allowable but should not interfere with, or conflict with, business use. Individuals should exercise good judgment regarding the reasonableness of personal use. Individuals must not attempt to access others' voice-mail boxes unless specifically authorized.

Mobile Computing Devices

Mobile computing devices are all portable computing devices, including but not limited to notebook computers, smart phones, and hand held computing devices (such as iPad's, Personal Digital Assistants - PDA's). Individuals authorized to use a mobile computing device to carryout eHealth business are responsible for protecting the confidentiality, integrity, and availability of eHealth information and information systems. This responsibility includes the device itself, information and information systems resident on the device and information systems that can be accessed from the device. Individuals should ensure that the mobile computing device is protected from theft or removal at all times that the device is not in their immediate possession. Individuals are required to use the security procedures provided with the mobile device to prevent unauthorized access to the device. Loss of mobile computing devices MUST be reported immediately

Data Storage

Individuals should store all eHealth materials, such as data, documents, e-mail messages, spreadsheets, databases, programs, etc. that were received, created or edited on office computers in the course of carrying out eHealth business, on network storage devices (commonly referred to as "the network"). The use of network storage devices will provide for recovery of such materials in the case of loss. Individuals are strongly encouraged not to store copies of such materials on office computer hard drives, floppy disks, CD's or other local or removable media unless necessary. Storing materials on such devices exposes eHealth information and information systems to disclosure or unrecoverable loss.

Cellular Phones

Cellular phones are part of the eHealth's IT infrastructure. Telephones and services should only be used to conduct eHealth business. Agreements should be established to address the use of individual-owned cellular telephones for eHealth business. Cellular transmissions are not secure and individuals should use discretion in relaying confidential information.

Photocopiers

Photocopiers are part of the eHealth's IT infrastructure. Care must be taken when photocopying copyrighted material and ensure that any fees or licenses must be accommodated. The provincial government agreement that permits government individuals to legally photocopy copyright protected works in accordance with the federal Copyright Act does not apply to eHealth.

7.2.1 Information Asset Classification

eHealth Saskatchewan

Subject/Title: ***Information Assets Classification***	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate information categorization to ensure that the information produced or processed by eHealth is categorized and protected according to its sensitivity to loss or disclosure. Based on this categorization, supporting policies will define how access to information or for transmitting information over different networks, including the Internet, can be defined.

Scope/ Purpose

All information assets generated or maintained for use within eHealth will be classified according to the **Security Classification for Information V1.5.1** document prior to project implementation. All users of the data must be aware of the data classification and the specific usage and management requirements.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Information needs to be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality and some may require additional levels of protection or special handling. Refer to **Chart – Information Security Classification and Standards Chart** document.

The respective Manager/Director (or designate) of each administrative area shall establish and maintain an inventory of all internal, confidential, or restricted Information generated (see Information Security), and all IT Resources used to generate or store the Information.

All physical IT Resources (e.g., computers, Mobile Computing Devices) shall be clearly identified with a unique identification tag for tracking and audit purposes. A record of the identification tag, location, ownership, and the security classification of any Information generated by or stored on the Resource shall be included in the inventory.

The inventory shall be reviewed and updated annually in accordance with the **Retention Destruction Records Policy** and shall be made available to the Security Office or Privacy Office on request.
It is the responsibilities of all individuals within the corporation to ensure that all data is classified so that protection methods can be implemented that are cognizant of the appropriate sensitivity of data.

Default Information Classification

Any information asset that is not classified by the information owner will be assumed to be "Internal" and will be protected with the necessary measures.

Classification Guidelines

Business and legislative requirements will be used to assist in asset classification. In the cases where technology based applications are used to collect and maintain information assets the Privacy Impact Assessment (PIA) and Application Verification Toolkit (AVERT) will be used to assist in the classification process.

eHealth maintains the following four classification levels to identify the necessary assurance levels of information assets:

- **Public:** Non-sensitive information available to the general public.
- **Internal:** information that is generally available to health stakeholders and approved non-health stakeholders.
- **Confidential:** information that is sensitive within the health information system and is intended for use only by specified groups of health stakeholders.
- **Restricted:** information that has personal health identifiers and is intended for use only by specific individuals within the health information system.

Refer to **Chart – Information Security Classification and Standards Chart document.**

For further description and details of information classifications please refer to the **Security eHealth SP 7.2.1 – Information Asset Classification**

7.2.2 Information labelling and Security

eHealth Saskatchewan

Subject/Title: ***Information Labelling and Security***	**Revision Number: 1.0**
Approving Authority: eHealth Corporate Services **Name:** **Title: Director Corporate Services**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate categorization labeling processes to ensure that the classification is clearly understood by all users of the information to ensure compliance with legislation.

Scope/ Purpose

eHealth is responsible to ensure that data is clearly identified with its proper classification so the appropriate level of protection can be applied. eHealth should put in place reasonable operating procedures for the eHealth Network including the protection of data within eHealth's control.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students and other persons acting on behalf of eHealth.

Detailed Policy

Information labelling and Handling

Rules shall be established for the handling and storage of information in order to protect information from unauthorized disclosure or misuse. They should be used in conjunction with the Information Classification Guidelines.

The procedures provided below cover how to label, store, dispose of, communicate/ physically transfer and copy different types of information, depending on its classification and medium (e.g. paper, diskette).

If in doubt about any of these activities, individuals should contact their line manager or the Information Security Manager for assistance.

Labelling

Information deemed Public or Internal does not need to be physically labelled in any way.

Any documents deemed 'Confidential' or 'Restricted' must be marked with this text clearly in the header and footer prior to printing. If the material is already printed and has not been word-processed, it should be hand-written with this text in the top and bottom margins of the first page and stapled together.

Similar guidelines apply to remove-able media (e.g. USB keys and compact disks). These should be labelled with the text 'Confidential' or 'Management in Confidence', as appropriate, on the media's label.

If internal mail envelopes are used to pass such information between inter-office or regional staff, the above marking should also be included on the outside of the envelope.

Storage

All information should be stored in a manner appropriate to its classification, as follows.

Public – as this is information that is freely available to anyone, it does not require any safe storage, but periodical backups will be maintained for BCP/DRP reasons.

Internal (Default) – as this is information available to any individual within the eHealth domains, the information is not marked in any way and also does not require any safe storage (although does require secure shredding as explained below). It should not be taken away from work premises, e.g. left unsecured in individual's homes or left in public places.

Confidential – this sensitive information must be securely locked away in cabinets or pedestals at the end of each day or when not being used. This applies regardless of the format which this information is held on e.g. paper, disk, files, tapes, faxes, post. Some confidential information may not be able to be physically locked away and therefore should be protected by applying passwords or encryption to information held electronically. These types of documents should not be stored on shared network drives. Such documents should also be labelled 'Confidential'.

Care should also be taken when verbally discussing (including mobile phone conversations) confidential information in public places, public transport in order that the conversation is not overheard. The same applies for messages that can be left on answering machines, voicemail and information which is sent / received by fax.

Restricted – Care should also be taken that this information is not read or heard by people in the organisation that do not need to know it. Therefore similar controls to the 'confidential' section above must be implemented e.g. password protection or encryption of documents, locking away information etc. Documents should be labelled as 'Restricted'.

Storage of data will be controlled following the information classification guidelines described in the **Security Classification for Information Version 1.5.1 - Security Framework Strategy**

Disposal of Information Assets

Information assets, which are no longer required, will be disposed of safely and securely. There are many reasons why care should be taken when sensitive information is to be disposed as follows:

- It may cause damage to our reputation if the information fell into the wrong hands;
- It would be a breach of legislative requirements if patient details were not protected;
- It could result in costly litigation to eHealth.

The ways in which we can prevent the above scenarios from occurring include:

- Throwing all paper documentation, classed as 'Internal' into the secure shredding bins every day. An external company, who provide certificates of safe destruction as a receipt, then securely shreds this paper.
- Any electronic information media devices are securely destroyed.

Refer to in eHealth **SP 9.2.6 Information Technology Asset Disposal** as well as **eHealth Retention Destruction Records Guidelines**

Security of Information assets in Transit

If any individual providing services to eHealth are required to transport any kind of information, there are controls that must be used in order to avoid the loss of media in transit or its misuse, protect from unauthorised access or corruption.

- The transport method must appropriate for the classification of the media i.e. Canada Post, Courier etc.
- Obtain an approved list of couriers, if applicable.
- When the courier arrives in the reception area the courier is required to show identification prior to transferring custody of media and a receipt acknowledging the transfer of media.
- The packaging used must be consistent with the classification of the media. I.e. could the package be damaged or tampered with during transit.

Copying

All individuals providing services to eHealth should be aware that they should not copy information unless they are authorised to do so, under the 'need to know' definition.

8 Personnel Security

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To reduce the risks of human error, theft, fraud or misuse of facilities.

eHealth tries to address security responsibilities at the recruitment stage, including contracts and activity monitoring. Potential recruits are adequately screened, and required to sign a confidentiality (non-disclosure) agreement.

Objective 2.) To ensure that users are aware of information security threats and concerns, and are equipped to support corporate security policy in the course or their normal work.

Users need to be trained in security procedures and correct use of information processing facilities to minimize possible security risks.

Objective 3.) To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Incidents that affect security should be reported through appropriate management channels as quickly as possible. All individuals need to be made aware of the procedures for reporting the different types of incidents that might have and impact on the security of information within the control of eHealth.

8.1.1 Including Security in Job Responsibilities

eHealth Saskatchewan

Subject/Title: ***Including Security in Job Responsibilities***	**Revision Number: 1.0**
Approving Authority: eHealth Corporate Services **Name:** **Title: Director Corporate Services**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate processes to ensure all individuals working on behalf of eHealth understand that they are responsible for understanding and working with the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.

Scope/ Purpose

It is the individual's responsibility to assist to assure that the availability, confidentiality and integrity of eHealth information assets are maintained. By doing so, they work to reduce the risks of human error, theft, fraud or misuse of facilities.

This Policy will also clarify roles and responsibilities in maintaining the security of information and in the management of situations that may threaten or compromise information security

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

As a condition of commencement of service, each new eHealth individual, volunteer, student, individual of an eHealth third party contractor or any other persons acting on behalf of eHealth will be required to sign a confidentiality agreement prior to providing services to eHealth.

Employer Responsibilities

eHealth's responsibilities with respect to personnel related security issues are as follows:

- eHealth will have direct responsibility to ensure compliance of its individuals, volunteers and students;

- eHealth will ensure that it has agreements in place with its contractors and consultants requiring them to comply with this;
- eHealth will direct managers and supervisors to review the security policy with all new hires within two weeks start date.
- eHealth will offer security awareness training as part of new hire orientation on a regular basis, once a quarter.
- eHealth will put in place the following practices for its individuals, volunteers and students to address the issues in Recruitment, Personal Security Control, and Identification of Personnel:
  - All individuals, volunteers and students of eHEALTH shall have a Criminal Record Check completed in accordance to the eHealth **Criminal Record Check policy.**
  - All individuals, volunteers and students of eHEALTH shall have photo ID
- All contact information for the eHealth Service Desk shall be posted and communicated to all individuals working on behalf of eHealth at eHealth facilities.
- eHealth will implement problem management procedures as identified in eHealth **13.1 – Reporting Security Incidents**.
- A record will be maintained and be readily available documenting:
  - the issuance and retrieval of security related items such as keys, codes, combinations, badges and system passwords; and
  - the custody and use of all information system assets, such as loan or issuance of computer hardware, computer software and specialized equipment.
- If new duties or tasks require an individual's security and access level in their new position to be:
  - higher, then administrative arrangements should be made to ensure access to that higher level of data occurs only after an appropriate screening process is successfully completed; or
  - lower, then the individual should be informed of the new access requirements of the position or contract and reflect these changes in the individuals' position description.
- On termination or transfer of duties, or when the individual's duties no longer require access to data, eHealth will immediately:
  - revoke access privileges (e.g. User IDs and passwords) to system and data resources and secure areas;
  - retrieve sensitive information including access control items (e.g. keys and badges);
  - retrieve all hardware, software and documentation issued or loaned to the individual.

eHealth must have corrective and disciplinary procedures in place to address any breach of security.

Managers/supervisors (or designates) shall ensure that new or inexperienced individuals are adequately supervised to ensure that IT security is enforced.

In conjunction with applicable collective agreements a formal discipline process is in place for individuals who violate security policies and procedures.

Confidentiality Agreements

All eHealth individuals, volunteer, student, individual of a eHealth third party contractor or any other persons providing services to eHealth are required to sign a Confidentiality Agreement at the time of acceptance of duties or appointment to verify that they agree to comply with Privacy and Security policies.

Terms and conditions of assigned duties

The terms and conditions of assigned duties with eHealth are covered under the written contracts or position descriptions.

Communications with the Media

All media inquires will be directed to the Saskatchewan Ministry of Health Communications Branch without exception.

Information Security Education and Training

The Manager/Director of each Unit shall ensure that all individuals are aware of, and appropriately trained with regard to the application of, processes to safeguard information, including all security updates. An Information Security Education and Awareness Training program shall include, but is not limited to

1. Awareness of the need to protect system resources and eHealth information assets (HIPA, FOIPP);
2. Information Classification (**eHealth SP 7.2.1 Information Asset Classification**);
3. Inform all individuals working on behalf of eHealth of the security policies and procedures (**eHealth Security Policies**);
4. Physical Security
5. Outline procedures for reporting security issues (**eHealth SP 13.1 Reporting IT Security Incidents**)
6. Disciplinary measures for Breach/Violation of eHealth policies and practices.

9 Physical and Environmental Security

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To prevent unauthorized access, damage and interference to business premises and information.

eHealth critical or sensitive information processing data centers are housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage and interference.

The level of protection provided by eHealth in using physical security is appropriate for the classification level of the information assets being protected.

Objective 2.) To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment should be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

Objective 3.) To prevent compromise or theft of information assets and facilities.

Information assets and facilities should be protected from disclosure to modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.

9.1 Secure Area Classification
eHealth Saskatchewan

Subject/Title: *Secure Area Classification*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate physical area categorization to ensure that the facilities and officers used by eHealth is categorized and protected according to its sensitivity to loss or disclosure in accordance with legislation.

Scope/ Purpose

The physical locations used by eHealth must be categorized. The physical area classification will then be used to assist in conjunction with eHealth **SP 7.2.1 – Information Asset Classification** in defining the security controls necessary to protect information according to sensitivity. Based on this categorization, policy for allowing physical access to information or equipment can be defined.

All physical locations that are use within eHealth will be classified according to the **Security Classification for Information V1.5.1** document prior to project implementation. All users of the data must be aware of the data classification and the specific usage and management requirements.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

For business purposes, such as health and safety, insurance or financial reasons, inventories of assets will be maintained. A registry of locations will be drawn up and maintained which will include the information assets contained in those locations. Each asset is clearly identified together with its location, which is required to mitigate risk when assessing security controls and safeguards

eHealth defines a hierarchy of zones for the purposes of the Environment Classifications:

Non-Secure Zones

1. Public
   - Public has uncontrolled access
2. Reception Zone
   - Initial Point of access control

- Information may be provided
- Access to secure zones is controlled

Secure Zones

2. Operations Zone
   - Access limited to authorized personnel and escorted visitors
   - Monitored periodically
3. Security Zone
   - Access limited to authorized personnel and escorted visitors
   - Continuous monitored (individuals, security operations analysts or electronic)
4. High-Security Zone
   - Controlled access
   - Continuous monitoring

It is essential that workstations with access to health data be located in areas that meet at least the requirements for a Reception Zone. It is essential that centralised data servers containing anonymised data for research and planning be located in areas that meet at least the requirements for a Security Zone. Centralised data servers containing personally identifiable health data should be located in areas that meet the requirements for a Security Zone.

Default Information Classification

Any zone that is not classified will be assumed to be an "Operations Zone" and will be protected with the necessary measures.

Additional Information and References

Refer to **Chart – Information Security Classification and Standards Chart document.**

For further description and details of information classifications please refer to the eHealth **SP 7.2.1 – Information Asset Classification**

9.1.1 Physical Security of NON-Government Services facilities

eHealth Saskatchewan

Subject/Title: *Physical Security of NON-Government Services (GS) facilities*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure the physical safety of personnel and information in its care and custody, in compliance with legislation.

Scope/ Purpose

Physical protection is achieved by creating several physical barriers around eHealth data centre premises. Each barrier provides a security perimeter, increasing the total protection provided.

Using secure areas, information assets will be protected from unauthorized access, damage and interference. Secure areas are protected by appropriate entry controls to ensure that only authorized individuals are allowed access.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Physical Security Perimeter

The following guidelines and controls will be considered and implemented where appropriate:

1. The security perimeter will be clearly defined.
2. The perimeter of a building or site containing an eHealth data center, must be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur). The external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access, e.g. control mechanisms, bars, alarms, locks etc.
3. A manned reception area or other means to control physical access to the site or building should be in place. Access to sites and buildings will be restricted to authorized personnel only.

4. Physical barriers will, if necessary, be extended from real floor to real ceiling to prevent unauthorized entry and environmental contamination such as that caused by fire and flooding.
5. All fire doors on a security perimeter should be alarmed and should slam shut.
6. When implementing a physically secure perimeter local fire safety rules must be observed.
7. Recording equipment is restricted in Secure Areas. Approval for recording equipment will be authorized by the Security Office.
8. Installing, monitoring, and maintaining equipment, communications wiring and equipment, hardware, electrical wiring and equipment, plumbing, and other utilities and services shall be consistent with the manufacturers' specifications and shall conform to local industrial sector codes.

Security Incident Reporting

Any potential or actual threat to the integrity of a physical access control shall be reported to the service desk immediately (See eHealth **SP 13.1 Reporting IT Security Incidents**). In instances where a physical access control is compromised the Security Office shall be contacted to assess the impact and risk, and complete an incident report.

Physical Entry Controls

The following will apply with respect to identification of personnel:

- Authorized identification and computer access codes consistent with appropriate level of access will be issued to all individuals working on behalf of eHealth and, where relevant, individuals providing services to eHealth.
- Identification cards or access badges will be issued to all authorized individuals working on behalf of eHealth. The cards or badges should be tamper resistant to meet minimum and appropriate standards.
- A temporary identification card or access badge can be issued to any individuals working on behalf of eHealth authorized to access the secured areas of eHealth.
- A standard operating practise will be established for the regular review and update of identification and access badges.
- Only one identification card or access badge will be issued to each person.
- eHealth will control and secure blank identification cards and access badge stock by documenting their use and retrieval and storing them in a secure container (e.g. fire resistant safe).
- Access cards, keys, or identification badges shall not be transferred, loaned, destroyed, or duplicated. The loss or theft of any access card, key, or identification badge shall be reported immediately to the Service Desk (see eHealth **SP 13.1 Reporting IT Security Incidents**).
- All items providing identity to individuals working on behalf of eHealth will remain the property of eHealth.

Visitor Access

Secure Areas are restricted to authorized personnel. Unauthorized personnel may be permitted, in some instances, to visit Secure Areas when escorted by authorized personnel. Recording equipment is restricted in Secure Areas.

Security Cameras

Security cameras may be installed in situations and places where the security of either equipment or people would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. When appropriate, the cameras may be placed inside buildings.

The main intent is to have the video in one room monitored by security operations analysts in a different room who is responsible for people and equipment in both rooms. In this case, pictures may or may not be stored. The live video can be monitored live by a security operations analyst; however any images stored must be stored remotely and access limited to the Security Office. If images are retained, the images should be retained for a period of at least one week and no longer than 70 days. If the images are part of an investigation the length of time retained will be determined as required. Information that directly

affects an investigation will be kept for at least one year (or for a period of time determined by the investigating agency.)

Requests for installation of security cameras should be made to and approved by the Privacy and/or Security Office. The following conditions must apply:

- Information obtained from the cameras would be used exclusively for law and/or policy enforcement.
- All camera installations are subject to federal and provincial laws.
- The places where these cameras may be installed may be restricted access sites such as a data centre; however, they are not places where a person has a reasonable expectation of privacy.
- Cameras will be located so that personal privacy is maximized. No audio should be recorded.
- Unless the camera is being used for criminal surveillance, or in extraordinary circumstances, the following places should not be monitored by security cameras:
    - Bathrooms
    - Locker rooms
    - Offices
    - Classrooms
- Unless the camera is being used for criminal surveillance, areas being monitored should have at least two signs indicating that security camera monitoring may be taking place. The wording on the signs should not create a false sense of security to lead someone to believe that the cameras were being monitored live when in fact they were not. These signs should be at the entrance to the area being monitored and should identify a contact person who can answer questions regarding the cameras.

9.1.5 Working in a Secure Environment

eHealth Saskatchewan

Subject/Title: *Working in a Secure Environment*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure the physical safety of personnel and information in its care and custody, in compliance with legislation.

Scope/ Purpose

Additional controls and guidelines may be required to enhance the security of a secure area. This includes controls for the personnel or third parties working in the secure area, as well as third party activities taking place there.

When equipment is removed from eHealth it must be physically protected from security threats and environmental hazards. Protection of equipment is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage.

Special controls may be required to protect against hazards or unauthorized access, and to safeguard data centers, such as the electrical supply and cabling infrastructure.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Working in Secure Areas

A record will be maintained and be readily available documenting:

- the issuance and retrieval of security related items such as keys, codes, combinations, badges and system passwords; and
- the custody and use of all information system assets, such as loan or issuance of computer hardware, computer software and specialized equipment.

If new duties or tasks require an individual's security and access level in their new position to be:

- higher, then administrative arrangements should be made to ensure access to that higher level of data occurs only after an appropriate screening process is successfully completed; or
- lower, then the individual should be informed of the new access requirements of the position or contract and reflect these changes in the individual's position description.

On termination or transfer of duties, or when the individual's duties no longer require access to eHealth information assets, eHealth will immediately:

- revoke access privileges (e.g. User IDs and passwords) used to access information assets and secure areas;
- retrieve sensitive information including access control items allowing entry into secure areas;
- retrieve all hardware, software, eHealth issued identification and documentation issued or loaned to the individual.

Equipment Protection

eHealth utilized the following controls to reduce environmental threats and hazards, and opportunities for unauthorized access:

a.) Equipment is situated to minimize unnecessary access into work areas.
b.) Data centers and storage facilities are positioned to reduce the risk of overheating during their use.
c.) Items requiring special protection should be isolated to reduce the general level of protection required.
d.) Controls are in place to minimize the risk of potential threats including:
    1) environmental (fire, water, wind)
    2) theft;
    3) explosives;
    4) smoke;
    5) water supply failure;
    6) dust;
    7) vibration;
    8) chemical effects;
    9) electrical supply interference and/or electromagnetic radiation.
e.) eHealth does not allow eating, drinking and smoking in its data centers.
f.) Environmental conditions are monitored for conditions which could adversely affect the operation of the data center systems.

Power Supplies

Equipment within eHealth data centers is protected from power failure and other electrical anomalies. Multiple sources of power are provided for systems that conform to the equipment manufacturer's specification.

eHealth protects its data center with the following methods:

a.) multiple feeds to avoid a single point of failure in the power supply;
b.) separate uninterruptible power supplies (UPS) for each power feed;
c.) access to a backup-up generator.

Cabling

Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage using the following mitigation techniques.

a.) Power and telecommunications lines into eHealth data centers are underground.
b.) Network cabling is protected from unauthorized interception or damage by avoiding routes through public areas.
c.) Power cables are segregated from communications cables to prevent interference.
d.) Fibre optic cable is used where possible.

Removal of Property

Equipment, information or software must not be taken off-site without authorization.

eHealth shall create and maintain an Off Premises Equipment Log, used to document the removal of physical IT Resources. The Log shall form part of the eHealth's IT Resource inventory, and shall identify the custodian, date of removal, specific Resource removed, unique asset tag number, destination, and expected date of return.

All authorized individuals working on behalf of eHealth are required to maintain the physical security of equipment taken off-site. They are also responsible to maintain the security of any information assets that may be contained on that equipment.

Security of Equipment off-premises

The security provided for equipment taken off-premises should be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside the premises. This equipment includes all forms of personal computers, organizers, mobile phones, paper or other form, which is held of home working or being transported away from the normal work location.

When equipment is used off-premises eHealth requires that the following, but not limited to, precautions are used:

- Portable computers should not be left out in public areas after business hours.
- Care should be used when carrying and placing portable computers.
- When traveling, do not to leave the portable computer unattended (except in a secure place out of public view) for any length of time.
- When at the airport, never check a portable computer with luggage.
- When passing through security be aware of the location of the computer at all times, as portable computer thefts occur during the security process.
- Do not store written passwords or instructions on how to logon to networks with portable computers.
- On shared computers always transfer confidential information off the portable computer.
- File encryption software must be used for confidential information stored on portable computers
- Manufactures' instructions for protecting equipment should be observed at all times.

Security risks, e.g. of damage, theft and eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls. More information about other aspects of protecting mobile equipment can be found in eHealth **SP 11.7.1 Mobile Computing.**

Clear Desk and Clear Screen

With open plan offices now common, the chance of the accidental exposure of confidential or internally classified information assets is high. Information can be read from papers on your desk or from your computer screen when left unattended.

All confidential or restricted information, regardless of its medium, shall be stored securely after working hours or while otherwise not in use.

Computers shall be configured with screensavers that automatically lock out monitor screens after **10 minutes of inactivity** and require password validation to be unlocked. Users shall manually lock out monitor screens when leaving a computer unattended and ensure that screensavers are used in accordance with Privacy and Security Policies.

Information shall be cleared from computer printers, scanners, photocopiers, and fax machines as soon as reasonably possible. Refer to eHealth **SP 7.2.2 Information Labelling and Security**

9.2.6 Information Technology Asset Disposal Policy
eHealth Saskatchewan

Subject/Title: *Information Technology Asset Disposal Policy*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure the physical safety of information in its care and custody, in compliance with legislation.

Scope/ Purpose

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner. eHealth's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and eHealth's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to approved methods.

This policy applies to the proper disposal of all eHealth IT hardware, including PCs, printers, handheld devices, servers, hubs, switches, bridges, and routers. eHealth owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where assets have not reached end of life, it is desirable to achieve some residual value of the IT asset in question through the Saskatchewan Community Donations Program.

Definitions

- "Non-leased" refers to any and all IT assets that are the sole property of eHealth; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.
- "Disposal" refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.
- "Obsolete" refers to any and all equipment over five (5) years old and/or that which no longer meets requisite functionality.
- "Evergreen" refers to any and all equipment that has reached the end of the leasing contract life and/or that which no longer meets requisite functionality.
- "Surplus" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.
- "Beyond reasonable repair" refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

This policy applies to all IT assets: server, hard disk arrays, server clusters, workstations, laptops, notebooks, PDA, Blackberry's, cellular phones, photocopiers, fax machines, and printers.

Detailed Policy – eHealth Owned

Disposal and disposal procedures of all eHealth owned IT assets and equipment will be centrally managed and coordinated by Operations. Operations is also responsible for backing up and then wiping clean company data on owned IT assets slated for disposal, as well as the removal of eHealth tags and/or identifying labels. Operations must use the Government of Saskatchewan approved external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills. Operations is also responsible for acquiring credible documentation from the external agents that are contracted to conduct the data wiping, tag or label removal, or any other part of the disposal process.

Practices

Acceptable methods for the disposal of IT assets are as follows:

- Used as a trade-in against cost of replacement item.
- Reassigned to a less-critical business operation function.
- Donated through the Saskatchewan Community Donations program to schools, charities, and other non-profit organizations.
- Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
- Discarded as rubbish in a landfill after sanitized of toxic materials by approved service provider.

Responsibility

It is the responsibility of any individual working in Operations with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above. It is imperative that any disposals performed by eHealth are done appropriately, responsibly, and ethically, as well as with company resource planning in mind. The following rules must therefore be observed:

1. Obsolete IT Assets: As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over five (5) years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of Operations. Decisions on this matter will be made according to eHealth's purchasing/procurement policies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).
2. Reassignment of Retired Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of Operations. It is, however, the goal of eHealth to – whenever possible – reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.
3. Trade-Ins: Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. eHealth's Purchasing and Procurement manager or IT Asset manager will assume this responsibility.
4. Cannibalization and Assets Beyond Reasonable Repair: eHealth's Director of Operations is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as much should be cannibalized for any spare and/or working parts that can still be put to sufficient use within the corporation. Operations will inventory and stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved scrap dealer or salvaging company.
5. Decommissioning of Assets: All hardware slated for disposal by any means must be fully wiped clean of all company data. Operations will assume responsibility for decommissioning this

equipment by deleting all files, company-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must completely overwrite each and every disk sector of the machine with zero-filled blocks in accordance to the eHealth Guidelines – Hardware Sanitization. In addition, any property tags or identifying labels must also be removed from the retired equipment.

6. Harmful Substances: Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill as rubbish. Security Operations may perform this action itself using a Government Services-approved disposal methods, or hire an accredited disposal company specializing in this service. No matter what the route taken, the removal and discarding of toxins from [company name] equipment must be in full compliance with local and federal laws.
7. Donations: IT assets with a net residual value that are not assigned for reuse, discarding, or sale to individuals within eHealth or external buyers, may be donated through the Saskatchewan Community Donations program to an approved school, charity, or other non-profit organization (i.e. a distributor of free machines to developing nations). All donations must be authorized by eHealth.

Detailed Policy – eHealth Leased

Disposal and disposal procedures of all eHealth leased IT assets and equipment will be centrally managed and coordinated by Operations. Operations is also responsible for backing up and then wiping clean company data on leased IT assets slated for disposal, as well as the removal of eHealth tags and/or identifying labels. Operations will coordinate with the leasing agent for removal of hardware and/or sanitizing hardware before shipment. Operations is also responsible for acquiring credible documentation from the leasing agents that are contracted to conduct the data wiping, tag or label removal, or any other part of the disposal process.

Responsibility

It is the responsibility of any individual working in Operations with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed. It is imperative that any disposals performed by eHealth are done appropriately, responsibly, and ethically, as well as with company resource planning in mind. The following rules must therefore be observed:

1. Evergreen IT Assets: As prescribed above, “Evergreen” refers to any and all computer or computer-related equipment that has reached the defined leasing contract life and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as evergreen is the combined responsibility of the leasing agent and Operations. Decisions on this matter will be made according to eHealth’s purchasing/procurement policies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).
2. Reassignment of Leased Assets: Reassignment of computer hardware to a less-critical role is made at the sole discretion of Operations. It is, however, the goal of eHealth to – whenever possible – reassign leased IT assets in order to achieve full lease life from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.
3. Trade-Ins: Where applicable, cases in which a piece of equipment can be replaced by a newer model, reasonable actions must be taken to ensure that a fair leased value credit is obtained for the old leased IT asset against the cost of the replacement. eHealth’s Purchasing and Procurement manager or IT Asset manager will assume this responsibility.

10 Communications and Operations Management

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To ensure that correct and secure operation of eHealth data centers.

Responsibilities and procedures for the management and operations of all eHealth data centers are established through these policies. This includes the development of appropriate operating instructions and incident response procedures.

Objective 2.) To minimize the risk of system failures.

Advanced planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirement should be made, to reduce the risk of system stress.

The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

Objective 3.) To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious software. Software and computing systems are vulnerable to the introduction of malicious software, such as computer viruses, spy ware, network worms, Trojan horses and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and mangers should, where appropriate, introduce special controls to detect or prevent its introduction. It is essential that precautions be taken to detect and prevent computer viruses and spy ware on workstation/server systems.

Objective 4.) To maintain the integrity and availability of computing and communications services.

Routine procedures should be established for carrying out the agreed back-up strategy, taking backup copies of data and rehearsing their timely restoration, logging events and faults and monitoring the equipment environment.

Objective 5.) To ensure the safeguarding of information assets in networks and the supporting infrastructure.

The security management of networks which spans geographical boundaries requires additional controls to protect the confidentiality or sensitive data passing over un-trusted networks.

Objective 6.) To prevent damage to information assets and interruptions to business activities, media should be controlled and physically protected.

Appropriate operating procedures should be established to protect document, computer media, data and system documentation from damage, theft and unauthorized access.

Objective 7.) To prevent loss, modification or misuse of information exchanged between organizations.

Exchanges of information and software between the corporation and other organizations should be controlled, and should be compliant with any relevant legislation. Procedures and standards to protect information and media in transit should be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

10.1 IT Operations Policy
eHealth Saskatchewan

Subject/Title: *IT Operations Policy*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate Information technology operational standards, processes and procedures in compliance with legislation.

Scope/ Purpose

Any change to the eHealth Data Centre operations schedule introduces risk. It is important that proper planning takes place to avoid undesirable results.

eHealth Data Centre operations schedules are to be formally planned, authorized and documented.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Documented Operating Procedures Policy

Operating procedures identified by the security policy should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.

These procedures specify the instructions for the detailed execution of each job the operating teams are responsible for, including but not limited to;

- processing and handling of information;
- scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;
- instructions for handling errors or other exceptional conditions, which might arise during job execution;
- support contacts in the event of unexpected operational or technical difficulties;
- special output handling instructions such as the management of confidential output, including procedures for secure disposal of output from failed jobs;
- system restart and recover procedures for use in the event of system failure;

- scheduling and optimizing back-up processes to most effectively utilize resources
- testing, scheduling and applying system patches and upgrades.

Documentation is also to be prepared for datacenter maintenance and communications activities. This documentation will include up to date network and communications diagrams are readily available for referencing and troubleshooting. These diagrams will include current system model/product numbers with installed firmware or operating system revision numbers.

It is also the operations teams' responsibility to install, maintain and ensure that all information handling systems have the most current firmware or operating system patches installed.

Operational Change Control

Alterations that require changes to routine computer systems operations at eHealth introduce risk. Such changes are likely to be necessitated by enhancements to either hardware or software, or may simply be a reflection of revised schedules required by end users.

The administration of the security related aspects of eHealth's systems software will be conducted in a controlled fashion and documented. As well, provisions for dedicated hardware controls and software recovery mechanisms will be implemented and documented.

Change control shall follow the Information Technology Infrastructure Library (ITIL®) guidelines which include but are not limited to:

- changes to systems are applied in a controlled manner so that the stability and security of systems is not compromised;
- changes to systems are only implemented on the basis of formal requests and appropriate documented procedures that are appropriate to the task and continued compatibility of all software and hardware components; and
- adequate segregation of duties and approval of all changes has been received.

eHealth will establish and maintain a formal change control procedure for software and systems within its control to address any changes to the system hardware, software, or communications network. These procedures will include mechanisms for, but not be limited to;

- requesting changes;
- recording and tracking outstanding requests;
- assessment of the potential impact of such changes;
- communication of change details to all relevant persons;
- approval of requests;
- testing and documenting changes;
- incorporation of the changes;
- identifying responsibilities for aborting and recovering from unsuccessful changes.

The User Organizations and Application Providers will be responsible for putting in place reasonable change control procedures for software and systems within their control to meet the requirements outlined above.

Segregation of Duties

eHealth should use segregation of duty controls to ensure that the corporation is not unduly reliant on that user access is appropriate for each job. eHealth must distribute security responsibilities and should conduct regular management reviews to mitigate risks. The distribution of security responsibilities should be designed so that no individual is capable of compromising the overall security of eHealth. This is done by utilizing appropriate organizational structures that distribute responsibilities.

Segregation of Production Environments from Other Environments

The inappropriate introduction of modified software could have potentially disastrous effects on the eHealth production network. For that reason strict procedures are in place to ensure that changes or upgrades to the production environment go through a rigorous change control process.

Individuals working on behalf of eHealth that test new software provide documentation and assistance to eHealth operations responsible for the installation of new services in the production environment. This recommendation is made to mitigate the risk of individuals working on behalf of eHealth unintentionally or inadvertently issuing system commands on the wrong system.

Risk Assessment and Management
Refer to eHealth **SP 12.1 Security in Application Systems – Threat Risk Assessment.**

10.3 Capacity Planning and System Acceptance
eHealth Saskatchewan

Subject/Title: *Capacity Planning and System Acceptance Policy*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure that new systems plan for and are tested for capacity abilities to ensure confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

New systems must be tested for capacity, peak loading, stress testing, user acceptance and security. This is done to demonstrate a level of performance and resilience which meets or exceeds the technical and business requirements for eHealth.

By implementing adequate monitoring and auditing systems, projections of future capacity requirements can be made.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Capacity Planning

In order to account for new business and technology requirements adequate capacity planning techniques need to be in place. These techniques are used to create projections for future capacity requirements required by new and existing systems within the eHealth data center.

eHealth shall have capacity planning exercises in place to monitor and project capacity demands for adequate processing power and storage.

It is extremely important to monitor large capacity data handling systems such as transactional or reporting databases. Examples of key system resources to monitor in order to develop a proper trend analysis are: processor usage, memory storage, file storage and network utilization.

By monitoring these system resources at the point of implementation a baseline of the system can be created. Future resources utilization reports can be compared to the baseline to develop a useful trend analysis. This trend analysis provides a tool for managers to identify and avoid potential bottlenecks that present possible threats to system security and user services.

System performance shall be routinely monitored by eHealth in order to ensure excess capacity. Utilization Monitoring shall be as often as determined by workload and resource demand.

System Acceptance

eHealth has adopted test procedures that lead to a formal 'acceptance' of new or changed systems. Acceptance testing is a critical phase of any project and requires significant participation by the end users. The system acceptance tests should be developed in order to plan precisely, and in detail, the means by which 'Acceptance' will be achieved.

The system acceptance test plans will vary from system to system but the testing should be planned in order to provide a realistic and adequate exposure of the system to all reasonably expected events. Part of the system acceptance process will include the completion of the eHealth Application Verification Toolkit (AVERT) process, which will deliver insights into the security vulnerabilities of new and changing systems.

Prior to testing, the end users, as well as the Security and Project teams need to develop and agree a range of severity levels. These levels will range from 1 to 6 and will represent the relative severity of a problem with a system that was determined during testing.

1.) **STOP** – it is impossible to continue with the testing because of the severity of the error/bug
2.) **CRITICAL PROBLEM** – testing can continue but we cannot go into production with this problem.
3.) **MAJOR PROBLEM** – testing can continue but live this feature will cause severe disruption to business processes currently in production.
4.) **MEDUIM PROBLEM** – testing can continue and the system is likely to go into production with only minimal departure from agreed business processes.
5.) **MINOR PROBLEM** – both testing and live operations may progress. This problem should be corrected, but little or no changes to business processes are foreseen.
6.) **COSMETIC PROBLEM** – personal preference issues have arisen such as colors and fonts. However, if such features are key to business requirements and application adoption they will warrant a higher severity level!

The users of the system, the security auditors, and the executive sponsor of the project must then agree upon the responsibilities and required actions for each category of problem.

Finally, it is crucial to agree on the Criteria for Acceptance because no system is entirely fault free. The maximum number of acceptable 'out standings' in any severity category must be agreed upon.

10.4 Controls Against Malicious Software
eHealth Saskatchewan

Subject/Title: *Controls Against Malicious Software*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate controls and protection against viruses, trojans, malicious code, worms and other programmatic objects in order to ensure the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

System hardware, operating and application software, the networks and communications systems must all be adequately configured and safeguarded against both physical attack and unauthorized network intrusion. Measures must be taken to defend computer hardware and software from unauthorized usage.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Controls against Malicious Software

Responsibilities with respect to malicious software are as follows:

- eHealth is responsible for ensuring reasonable procedures are in place to check for viruses on hardware and software within its control.
- eHealth is responsible for ensuring reasonable procedures are in place to check for malicious software on systems within its control.
- eHealth is responsible for a contingency procedure detailing the course of action to be followed when a virus attack is suspected.
- Each User is responsible for ensuring reasonable procedures are in place to check for malicious software on hardware and software within its control (e.g. the workstation (PC) and software located on that workstation). Specifically Users are requested to periodically check their machines for viruses using eHealth approved malicious code detection and removal package with the most current working signatures.

If malicious code is thought to exist it is important to contact the service desk as described in **SP 6.3.1 Reporting Security Incidents.**

10.6 Network Management
eHealth Saskatchewan

Subject/Title: *Network Management*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate network management controls, processes and procedures that ensure the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

Health Information Solutions Centre Operational Support Services (OSS) is responsible for the overall security of the eHealth network.

eHealth should put in place reasonable operating procedures for the eHealth Network including the protection of data within eHealth's control.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Network Security Management

eHealth security infrastructure shall safeguard all Information stored on networks and protect the supporting infrastructure. eHealth shall perform a Risk Assessment to determine the need for message authentication in applications. The following controls shall be implemented, but not limited to, on eHealth hardware and software.

Hardware

1. An inventory of all system components will be maintained indicating model numbers, serial numbers and other unique identification numbers and will include the location of system components.
2. A hardware configuration list and supporting documentation will be developed and maintained.
3. Hardware maintenance personnel must be supervised by a representative of eHealth.

4. Where equipment maintenance requires the exchange or release of components (tapes, disks, diskettes, memory, EPROMS, etc.), which may contain sensitive Information, those components should not be released to the vendor unless the sensitive Information has been erased, encrypted or rendered inoperable.
5. Records of all hardware modifications, configuration changes and maintenance activities should be retained for a reasonable period.
6. Network monitoring of internal and external or public network connections, and early detection of malicious network activity.

Software

1. All acquired software must be examined for viruses, logic bombs or other extraneous malicious features.
2. Procedures should be put in place to strictly enforce the conditions of software licenses and respect software copyright requirements.
3. A current inventory will be maintained of all software (copy-righted/licensed/developed).
4. Where the User identification is authenticated, the User authentication information will not be displayed and will be protected from unauthorized access.
5. A system development life cycle (SDLC) methodology will be implemented where custom software or modifications to commercial software packages are developed for eHealth. The SDLC will ensure as a minimum that: security concerns are addressed, test criteria are met prior to implementation of operational software, change control procedures for operational software are implemented, and discrepancies for all data and software are reported, monitored and resolved.

When initiating access to the eHealth Network, all systems must display a banner indicating that the User has accessed a private and restricted system. The banner should identify the location of eHealth Security Policies for reference and compliance.

eHealth shall have network controls in place to ensure correct and cautious execution of System Utilities. Specific controls, such as enforced path controls, shall be provided to individuals that are working on behalf of eHealth as necessary.

Remote Access to Health Information is in accordance with the eHealth **SP 11,7,2 Granting Remote Access to Information Systems.**

The network shall be separated into zones with associated security controls. The Security Office shall determine the network zones and associated security controls, and undertake periodic reviews to ensure relevance and applicability.

Synchronized Network Time

All network devices and services must have a synchronized date and time to facilitate cross-referencing of logs.

Operator Logs

eHealth will use logging and reporting facilities that record appropriate activities, security violations and privileged use functions. These logs must be secured from tampering by restricting access to them. Adequate log administration, monitoring and follow-up procedures must also be implemented.

Logs should include, as appropriate:

1. system starting and finishing times;
2. system errors or warnings identified and corrective actions taken;
3. when automated paging of errors is used, a record of the time an error occurred, when the page was sent, and the pager/cell phone number;
4. confirmation of the correct handling and classification of data files and computer output; and
5. the name or user-id of the individual making the log entry.

Operator logs are to be subject to regular, independent checks against operating procedures.

Fault Logging

All system faults need to be recorded and reported to the appropriate trained individuals working on behalf of eHealth or maintenance firms for corrective action.

All individuals working on behalf of eHealth are asked to contact the eHealth service desk at with any information regarding software malfunctions or support issues. For further information refer to the eHealth **SP 13.1 Reporting IT Security Incidents.**

Monitoring

eHealth will put reasonable procedures in place to monitor use, access and health of the network. Specific monitoring practices will be put in place for each application or service dependant on the data classification contained within the application as well as the service level requirements defined within the "Prepared to Support" documentation. Refer to **eHealth SP 10.10.1 Monitoring System Access and Use.**

10.6.1.1 Wireless Access Policy
eHealth Saskatchewan

Subject/Title: *Wireless Access Policy*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate controls to protect the eHealth network from unauthorized or unsecure wireless access in order to ensure the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

The purpose of this policy is to define standards, procedures, and restrictions for connecting to eHealth's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

a. External hosts via remote access technology (for example, using a wireless router at home to connect to the corporate Virtual Private Network).
b. Wireless gateways on corporate premises.
c. Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access corporate resources, even if said equipment is not corporately-sanctioned, owned, or supplied. For example, use of a public library's wireless network to access the corporate network would fall under the scope of this policy.

The overriding goal of this policy is to protect eHealth's technology-based resources (such as corporate data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image from any users utilizing wireless networking technology.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students and other persons acting on behalf of the corporation who utilize wireless technologies to access eHealth networking systems. Wireless access to enterprise network resources is a privilege, not a right. Consequently, commencement of service to eHealth does not automatically guarantee the granting of wireless access privileges.

Detailed Policy

All wireless access points within eHealth will be centrally managed by Operations and will utilize encryption, strong authentication, and other security methods at eHealth's discretion. End-users are expected to adhere to the same security protocols while utilizing wireless access as they would if on the LAN. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

It is the responsibility of any individual working on behalf of eHealth who is connecting to the corporate network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct eHealth business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- Eligibility to have wireless access must follow an access request process to gain access to the LAN network.
- Any wireless equipment that would be used to access corporate resources. Devices must adhere to the minimum requirements as define in the wireless device guidelines document.
- General access to the corporate network through the Internet by residential remote users through eHealth's network is permitted.
- Individuals using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through encrypted strong passwords in accordance with eHealth's password policy. Individuals agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
- All access points inside the regional facilities must be sanctioned by Security Operations.
- The wireless access user also agrees to and accepts that his or her access and/or connection to eHealth's networks may be monitored to record dates, times, duration of access, data types and volumes, [add any additional monitored activities, as appropriate] etc., in order to identify unusual usage patterns or other suspicious activity [add any additional monitored activities, as appropriate]. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- Any questions relating to this policy should be directed to Service Desk
- eHealth reserves the right to turn off without notice any access port to the network that puts the company's systems, data, users, and clients at risk.

Wireless networks are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive corporate data.

Addition of new wireless access points within corporate facilities will be managed at the sole discretion of IT. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the corporate facilities, are strictly forbidden.

Additional References
Standards and Guidelines - Wireless Local Area Network Checklist.doc

10.8.4 Security of Electronic Mail
eHealth Saskatchewan

Subject/Title: *Security of Electronic Mail*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate use and management of electronic mail systems to ensure the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

The purpose of this policy is to ensure proper secure use of eHealth's Email services. Any infringement of this policy will be treated as misconduct of the most serious nature and may result in disciplinary action, which can result in dismissal.

It is the duty of all individuals working on behalf of eHealth to comply with this policy when using electronic mail on any eHealth computer either within the workplace or away from eHealth premises.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Legal Considerations

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Email and all the content and attachments contained with in each message are the property of the corporation. This includes:

a) Text messages;
b) Calendaring;
c) Notes;
d) Task assignments;
e) Attached files;
f) Printed versions of Email; and
g) Archived Email messages

eHealth reserves the right to override users' passwords and access the email at any time for valid business purposes such as business continuity, system maintenance, and investigations.

Access
Email account access will be provided to users of eHealth IT systems when a user account application with a request for email access has been submitted to the Service Desk. See eHealth SP 11.1.1 – Electronic Information Access Control

Retention
Six (6) months of email shall be retained on the email server. Archiving of e-mail can be made available based upon the Administrative Records Management System or Operational Records Management System retention requirements.

Mailbox Size
Users will make every effort to keep their electronic mailbox to a manageable size containing a six (6) month history from the current calendar date.

Retention of Email for longer periods is a business driven requirement and may be subject to the Administrative Records Management System (ARMS) or Operational Records Management System (ORMS) requirements. To reduce the electronic mailbox and satisfy the ARMS or ORMS requirements a hardcopy of the Email should be produced and put on file.

Technical Email transmission and mailbox storage size limitations are defined in the **Electronic Mail Management Guidelines.**

A request detailing the business requirements can be submitted to the Service Desk for Operations to adjust technical mailbox size to allow for larger electronic storage capacity.

Archiving
Archiving of email must be securely stored on networking devices and shall not be located on local workstations, laptops or removable media.

Local Storage of email
Email must be securely stored on local devices using a Security Office approved encryption method.

Exception Management
Exceptions will be note in the eHealth Exception Management Register, following the eHealth Risk Assessment Guidelines

User Responsibilities
All Email messages and content is the responsibility of the user. For detailed user responsibilities, refer to the eHealth SP 7.1.3 Acceptable Use of Assets

Transmission of eHealth Data via Electronic Mail
Transmission of eHealth Data is allowable via e-mail as prescribed by the classification of the data.

For more detail on data transmission, refer to **Chart – Information Security Classification and Standards Chart.**

Corporate Image and Confidentiality Notice
Users must conform to the corporate communications policy for visual presentation of Email communications. Users must include the corporate confidentiality notice on all Email communications. Users should not include a scanned copy of their handwritten signature in Email communications.

Mass Distribution
Only authorized users may have permission to use distribution groups that include all users. Users may create and use personal distribution groups which contain limited number of Email addresses to accommodate the special interests of their project or services.

10.10.1 Monitoring System Access and Use

eHealth Saskatchewan

Subject/Title: ***Monitoring Systems Access and Use***	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate monitoring controls, processes and procedures that ensure that access of confidentiality of personal, health and business information in its care and custody has been done in an appropriate and authorized means, in compliance with legislation.

Scope/ Purpose

Access to as well as the use of eHealth data processing facilities shall be subject to auditing, monitoring, and reviewing controls. These controls shall be used to help eHealth protect and maintain the security of Information and IT Resources, and aid in determining compliance with and measuring the effectiveness of eHealth's Privacy and Security policies and processes, and the IT Security Standards.

The purpose of this policy is to:

- articulate eHealth Auditing, Monitoring, and Reviewing controls for Information Technology (IT) Resources.
- comply with the Freedom of Information and Protection of Privacy Act (FOIP), the Health Information Protection Act (HIPA).

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

MONITORING

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions will record and retain audit-logging information sufficient to determine:

- the activity that was performed;
- the account or system that performed the activity, including where or on what system the activity was performed;
- the system the activity was performed on;
- the time that the activity was performed;

- the tools that were used to perform the activity;
- the status (such as success vs. failure), outcome, or result of the activity.

Security controls, audit trails, and activity logs will be used for IT resources during automated and manual processes. Monitoring of IT resources shall include, but is not limited to:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
4. controlled access to software that monitors or modifies network configurations or devices;
5. equipment maintenance records of suspected or actual equipment faults and maintenance activities;
6. fault logs and reports;
7. internet use;
8. external network connections and remote access networks;
9. entry control logs recording entry statistics (e.g., name, affiliation, date, and time, et cetera) to eHealth IT Resources and data processing facilities;
10. internet audit trails (where required); and
11. the maintenance of synchronized clock settings.
12. Initiate a network connection;
13. Accept a network connection;
14. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
15. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
16. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
17. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or antispyware system.

To maintain the integrity and availability of Information Systems, Operations personnel will maintain either manual or automated system logs of their activities. Personnel logs shall be subject to regular independent checks against operating procedures to ensure that adequate processes are logged and that the procedures are being followed. Logs shall include, but are not limited to:

1. system starting and finishing times;
2. system errors or warnings identified and corrective actions taken;
3. when automated paging of errors is used, a record of the time an error occurred, when the page was sent, and the pager/cell phone number;
4. confirmation of the correct handling and classification of data files and computer output; and
5. the name or user-id of the individual making the log entry.

Electronic access controls shall be employed to protect IT Resources in accordance with the eHealth SP **11.1.1 Electronic Information Access Control** and Security Standards. Electronic access privileges are monitored and audited to detect potential vulnerabilities or access privilege abuse.

Security Operations will ensure that controls are in place for the monitoring and early detection of malicious network activity.

Formatting and storage

The logging and auditing system will ensure the integrity of the logs and to support enterprise-level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

1. Event Logs collected by a centralized log management system;
2. Logs in a well documented format sent via syslog, syslog-ng, or syslog reliable network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements such as but not limited to those based on Checkpoint OpSec, ArcSight CEF, and IDMEF.

AUDITING

All audit tools will be protected to safeguard integrity and to prevent misuse. The Security Office will develop system audit controls, including maintenance of audit trails for user access attempts to intranet, internet, applications, browsing, and directories.

Contractors shall maintain a log of all successful and unsuccessful requests for physical, environmental, or electronic access to eHealth information and IT resources. The log shall be available, upon request, to the Security Office for auditing purposes.

The Security Office will maintain centralized audit trails of eHealth checks and controls, including those that are in place for Information accesses, changes, additions, and deletions.

Desktop Operations will perform periodic computer audits to ensure that software is licensed. Non-approved software shall be removed and reported to the Security Office.

At the request of the Security Office, Information System Owners shall perform audits of the systems for which they are responsible.

REVIEWING

Logs will be protected to maintain integrity and to prevent unauthorized access. Logged Information may be filtered by Security Office to ensure that only relevant Information is reviewed. **The individual(s) reviewing the Log shall have a segregation of duties from the activities being monitored**.

Fault Logs will be reviewed to ensure faults have been satisfactorily resolved and corrective actions taken.

THREAT-RISK ASSESSMENT

Refer to eHealth **SP 12.1 Security in Application Systems – Threat Risk Assessment.**

Security Response

eHealth has established security response processes to minimize damage from Information Security Incidents (see eHealth SP 13.1 Reporting IT Security Incidents). To monitor responses to Information Security Incidents and learn from such Incidents, audit trails and relevant Information will be collected for:

- problem analysis;
- use in arbitration, civil or criminal proceedings; and
- negotiating for compensation from software and service providers, and other Contractors.

DATABASE MANAGEMENT

All database discrepancies such as lost records or potential security exposures will be reported to the Security Office immediately.

Database audit checks shall be conducted periodically by the Security Office to verify logical and physical database consistency. Where feasible, a backup strategy shall be employed to restore lost records. (Refer to **PROCEDURES – eHealth Database Backup Strategy**)

A Log will be kept for the use of all enterprise database(s), including database administration utilities, which will include recording the accessing application, date, time, and user-id. Whenever possible, the type of access (e.g., read, update, delete) to an enterprise database and the record accessed is recorded. Changes made to all enterprise databases shall be tracked in accordance with the eHealth Change Management Process (see eHealth **SP 10.1 IT Operations - Operational Change Control**).

11 Access Control

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To control access to information.

Access to information, and business processes should be controlled on the basis of business and security requirements. This needs to take into account any policies for information dissemination and authorization.

Objective 2.) To prevent unauthorized access to information systems.

Formal procedures need to be in place to control the allocation of access rights to information systems and services.

This process covers all stages of the 'life-cycle' of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention is given to control the allocation of privileged access rights which allow users to override system controls.

Objective 3.) To prevent unauthorized access.

The co-operation of authorized users is encouraged and necessary of effective security.

Users are made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords, data access and the security of user's equipment.

Objective 4.) Protection of networked services

Access to both internal and external networked services is controlled.

This is done to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:
: appropriate interfaces between the corporation's network and the networks owned by other jurisdictions, government ministries, health organizations or public networks;
: appropriate authentication mechanisms for users and equipment;
: control of user's access to information services.

Objective 5.) To prevent unauthorized computer access.

Security mechanisms are used at the operation system level to restrict access to computer resources. These mechanisms are capable of the following:
: identifying and verifying the identity, and if necessary the terminal and location of each authorized user;
: recording successful and failed system accesses;
: providing appropriate means for authentication and ensures quality password standards are met.
: where appropriate, restrict the connection times of the users.

Objective 6.) To prevent unauthorized access to information held in information systems.

Security mechanisms are used to restrict access within application systems. Logical access to software and information is restricted to authorized users.

Application systems must do the following:

- control users access to information and application system functions, in accordance with a defined business access control policy;
- provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;
- not compromise the security of other systems with which information resources are shared;
- be able to provide access to information to the owner only, other authorized individuals or defined groups of users.

Objective 7.) To deter unauthorized activities.

Systems are monitored to detect deviation from the access control policy and record events to provide evidence in the case of security incidents.

This monitoring also allows the effectiveness of the controls adopted to be checked and verified against the access policy model (refer: eHealth SP 11.1.1 – Electronic Information Access Control)

Objective 8.) To ensure information security when using mobile computing and teleworking facilities.

The protection applied is commensurate with the risks these specific ways of working cause. Mobile computing carries the risks of working in an unprotected environment and these risks need to be considered and appropriate protection applied. In the case of teleworking, eHealth must apply protection to the teleworking site and ensure that suitable arrangements are in place for this method of working.

11.1.1 Electronic Information Access Control Policy
eHealth Saskatchewan

Subject/Title: *Electronic Information Access Control Policy*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate access controls, processes and procedures that ensure that only authorized users gain access to confidentiality of personal, health and business information that is in its care and custody, in compliance with legislation.

Scope/ Purpose

Access control standards for electronic information systems must be established by eHealth and must incorporate the need to balance restrictions to prevent unauthorized access against the need to provide unhindered access to meet business needs.

eHealth applies access control standards in order to control access to its information assets. These standards must be appropriate for eHealth's business and security needs. The dangers of inadequate access control standards range from inconvenience to critical loss or corruption of data.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

User Access

Access is limited and granted only to individuals in accordance with the level of access required for the performance of specified duties. A record of all users with access privileges to eHealth Information System Resources shall be maintained.

At the time of access to the eHealth Electronic Information System Resources, all systems must display a banner indicating that the User has accessed a private and restricted system. The banner should identify the location of the Privacy and Security Policies for reference and compliance.

Logging and Auditing

Logging and auditing are also critical to meet other operational needs such as system administration and transaction monitoring.

Electronic mail (e-mail), file, database and other information systems may be monitored for the following reasons, but is not limited to:

- as a result of an Information Security Incident, or;
- if requested to do so by the user's Manager/Director because unacceptable use is suspected (see eHealth **SP 7.1.3 Appropriate Use of Assets**), or;
- as a part of a regular audit performed on set number of random users, or;

Electronic mail (e-mail), file, database and other information systems may be monitored without notification to the account holder.

Audit logs that record data access events shall be maintained and available for review as required by the Security Office. Refer to eHealth **SP 10.10.1 – Monitoring System Access and Use.**

User Registration

The Security Office shall ensure a formal user registration procedure is in place, including **Account Request** and **Workstation-Network Access Forms**. These forms must be signed by the appropriate authority and submitted to eHealth Support Desk five (5) business days prior to the date access is required.

Refer to eHealth **SP 11.3.1 - Password Management**

Leave of Absence or Change of Access Requirements

The Security Office shall ensure a formal user account access change or de-registration procedure is in place, including **Account Request** and **Workstation-Network Access Forms**. This form must be signed by the appropriate authority and submitted to eHealth Support Desk five (5) business days prior to the date access is required.

User Termination

All access privileges will be revoked immediately upon expiration or termination of duties, agreement, contract, or appointment with eHealth. eHealth Corporate Services will fill out the **Account Request Form** and contact eHealth Support Desk five (5) for the removal of user access privileges.

Privilege Management

The appropriate authority shall ensure that Users with access privileges review the applicable policies, indicate understanding and sign the user agreements. (See applicable policies)

Account Identification

In reference to the security controls identified in the data classification guidelines, authentication will be made at the appropriate level for identification and accountability

User Authentication

Unique user id's will be created.

System Authentication

Service accounts will be created for access to a specific administrative system or service. Terminal identification may be used to limit access to specific information resources.

Generic User ID Authentication

Generic User id's may be created to access non-sensitive, de-identified or general corporate information.

Review of User Access

Inactive accounts will be disabled after six (7) months and deleted after thirteen (13) months.

User Responsibility

Users will follow the eHealth **SP 8.1.1 - Including Security in Job Responsibilities**.

Group Access Restrictions

Where possible, access to information services will be controlled through group permissions, not individual account permissions.

In the event that any electronic access control is compromised, users will follow the eHealth **SP 13.1 - Reporting Security Incidents.**

User Authentication for External Connections

Users will follow the eHealth **SP 11.7.2 - Granting of Remote Access to Information Systems.**

Review of User Access Rights

The Security Office shall review user access rights, either as part of a regular security review or more frequently (as required), and may revoke privileges when necessary.

Access rights of privileged accounts will be reviewed every three (3) months and basic accounts every six (6) months.

Inactive accounts will be disabled after six (7) months and deleted after thirteen (13) months.

11.3 User Responsibilities Policy
eHealth Saskatchewan

Subject/Title: *User Responsibilities Policy*	Revision Number: 1.0
Approving Authority: eHealth Corporate Services Name: Title: Director Corporate Services	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate processes and procedures to inform the users of eHealth services and applications of their responsibilities when accessing information in its care and custody, in compliance with legislation.

Scope/ Purpose

The cooperation of authorized users is essential for effective security. Users will be made aware of their responsibilities for maintaining effective access controls.

All individuals play a role in the protection of the privacy, confidentiality, and security of personal health information.

eHealth applies access control standards in order to control access to its information assets. These standards must be appropriate for the corporations business and security needs. The dangers of inadequate access control standards range from inconvenience to critical loss or corruption of data.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

User Responsibilities

Users who access IT Resources will:

- read the eHealth Security Policy and other relevant eHealth security standards and guidelines;
- Individuals working on behalf of eHealth should check with their supervisor/manager or the Security Office if they have questions about which policies and procedures apply to them.
- complete any required IT security training, and the Information Security Education and Awareness Training as provided by the corporation;
- sign a Confidentiality Agreement and applicable user agreements acknowledging understanding and agreement to comply with the Information Security and Privacy policies and applicable legislation;

- be responsible for the security of his or her own Workstation (PC) and other hardware, software and data within his or her control, the use of his or her User ID and Passwords;
- only use IT Resources for eHealth business purposes;
- Practise security conscious behaviour at all times such as attending regular security educational awareness sessions, discussing personal health information only in private locations (where it cannot be overheard), and not sharing passwords or posting passwords where they are visible.
- report all information security incidents promptly **(See eHealth SP 13.1 – Reporting Security Incidents)**;
- access only the minimum identifiable patient or personal Information necessary to perform job functions; and
- return all IT Resources upon termination of duties, agreement, contract, or appointment with eHealth.

Each individual will be accountable for their actions and have a duty of care to ensure due diligence is afforded to comply with eHealth security policies. Accountability cannot be delegated.

Consultants, Contracted Personnel and Information Sharing Partners

As with others the role of consultants, contracted personnel and data-sharing partners is to protect the privacy, confidentiality, and security of personal health information. In addition to the standard user responsibilities, consultants, contracted personnel and information sharing partners will include:

- In the case of personal services contracts, signing a confidentiality contract addendum for consultants, contracted personnel and information sharing partners.
- When a consultants, contracted personnel and information sharing partners are brought in through a vendor company contract, the signing officer for the vendor company will sign the confidentiality contract.
- Following the outlined information protection steps of contractual agreements. The agreements will outline the name of the user(s), specific access privileges and the expiration date, the user(s) commitment to protect the privacy, confidentiality, and security of the information, the name of a contact person who will handle client complaints and inquiries, and the legal jurisdiction under which litigation will be resolved.

Password Use

Passwords shall not be shared or transferred by any User. Users are individually responsible for updating and safeguarding their passwords and must abide by the eHealth Security Policies regarding Password management **(See eHealth SP 11.3.1 Password Management).** Any threat to the integrity of a password shall be reported immediately **(See eHealth 13.1 – Reporting IT Security Incidents)**.

Monitoring

Managers/supervisors (or designates) shall ensure that new or inexperienced individuals are adequately supervised to ensure that IT security is enforced.

In conjunction with applicable collective agreements and the management terms and conditions of assigned duties, a formal discipline process is in place for individuals who violate security policies and procedures.

Directing Media Inquiries

All individuals working on behalf of eHEALTH shall direct all media inquiries relating to eHealth, clients or any public health issue to the Saskatchewan Ministry of Health Communications Branch. (Refer to eHealth **SP 8.1.1 Including Security in Job Responsibilities – Communications with the Media.)**

11.3.1 Password Management Policy
eHealth Saskatchewan

Subject/Title: *Password Management Policy*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure that user passwords are appropriate to protect the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

Passwords provide a means of validating a user's identity and thus to establish access rights to eHealth information assets. Passwords are the first line of defence for the protection of eHealth information resources.

To assist in the prevention of unauthorized user access.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Password Management

All individuals working on behalf of eHealth; individuals, volunteers, students, contractors, business associates, suppliers, and vendors shall adhere to the following policy concerning passwords:

- Passwords shall not be a proper name, the user's logon name, a first or last name in any form, or any family member's name.
- Passwords shall not use other information easily discovered about the user such as the user's license plate number, phone number, birth date, street name, etc.
- Passwords shall not be all the same character or digit (e.g., xxxxx or 99999), or be in another commonly-used or easily-guessed format so that the password can't be easily cracked using an automated tool.
- Passwords shall not be shared.
- Passwords for logon IDs shall be aged and changed at least every ninety (90) days.
- Passwords for logon IDs considered sensitive (i.e., system administrator's privileged account IDs) shall be changed at least every sixty (60) days.

Access to eHealth information resources shall require the use of a unique password consisting of at least eight (8) mixed alphanumeric characters using both uppercase and lowercase characters. All eHealth systems shall require a valid user ID and password for authentication. And adopt the following password rules:

1. **Default Passwords.** The initial password issued by a security administrator must be valid only for the user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.
2. **Minimum Length.** The minimum length of passwords shall be eight (8), system accounts will be required to be a minimum of ten (10). Both shall use alphanumeric characters using both uppercase and lowercase characters consisting of a minimum of two (2) numeric and one (1) special character.
3. **Minimum Password Age.** The minimum age a password must be before it can be changed is one (1) day.
4. **Password Change.** All users will automatically be forced to change their passwords at least once every ninety (90) days.
5. **Password Incidents.** If a system has been compromised by unauthorized personnel gaining access to it, system administrators shall take the appropriate actions (s) necessary to secure the system. This may result in every password being changed on a system. Likewise, if a user suspects their password might have been compromised, contact the eHealth service desk immediately **(See eHealth SP 13.1 Reporting Security Incidents).**
6. **Password Storage.** Passwords shall not be stored in readable form or placed in locations where unauthorized persons might discover them.
7. **Password Reminders.** All individuals working on behalf of eHealth that have been given a corporate user account and password shall not write down any passwords.
8. **Embedded Passwords.** All individuals working on behalf of eHealth that have been given a corporate user account shall not store passwords in readable batch files, automatic login scripts, software macros, keyboard functions keys, or in any location where an unauthorized person might discover them
9. **Privileged Accounts.** Privileged user IDs, such as system administrators, shall have their passwords changed at least every sixty (60) days.
10. **System Accounts.** Accounts used to manage system services and nodes will not be required to expire passwords automatically. A manual process will be used to renew passwords for these accounts every twelve (12) to eighteen (18) months. These passwords are subject to more stringent auditing and will be required to be a minimum of 12 *mixed alphanumeric characters using both uppercase and lowercase characters*
11. **Password History File**. On all eHealth information processing systems, a history file must be used to prevent users from reusing passwords. The history file must minimally contain the last ten (10) passwords for each user-ID.
12. **Encryption of Passwords.** To prevent passwords from being disclosed, passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications systems.
13. **Password Sharing Prohibition.** To ensure accountability, passwords must remain confidential and never shared.
14. **Password Constraints.** The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorized parties shall not be able to observe them.

11.7.1 Mobile Computing
eHealth Saskatchewan

Subject/Title: *Mobile Computing*	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date: March 1, 2011** **Revision Date: February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate mobile computing controls, processes and procedures that ensure the protection and confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

The protection applied is appropriate to the risks these specific ways of working beyond the protection of the internal network. Mobile computing carries the risks of working in an unprotected environment and these risks need to be considered and appropriate protection applied. In the case of teleworking, eHealth must apply protection to the teleworking site and ensure that suitable arrangements are in place for this method of working.

The guidance and standards outlined below are designed to ensure that the information and equipment belonging to eHealth is used outside the office environment is afforded similar levels of protection as that equipment and information that is used exclusively within the office environment. This also extends to information processed exclusively within an individual's, who is working on behalf of eHealth, home.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the Security Office. General points to be used for corporate notebooks and tablet devices are included, but not limited to the following lists:

- All individuals working on behalf of eHealth will be required to attend HIPA (Health Information Protection Act) education sessions. This can be arranged by contacting the Privacy Office.
- Warranty must be maintained on notebooks and tablet devices.
- Unique usage and security awareness needs must be addressed for notebook and tablet

- Users must take good care of notebooks and tablet devices to prevent accidental damage, e.g. from rough handling, accidentally spilling drinks on the equipment, or being in close proximity to extreme temperature;
- Personal health information or corporate information on local storage of notebook and tablet devices must be encrypted.
- The least amount of personal health information necessary to perform the task is to be downloaded. I.e. only information for personal health information to be provided service on a given day. Where possible, the amount of information for specific personal health information should also be limited to what is required for required function or service.
- Personal health information downloaded to mobile devices must be deleted as soon after the completion of the task as possible.
- users must not install any software on notebooks and tablet devices without prior authorization; (
- all third party software installed on notebooks and tablet devices will be licensed for such usage;
- users who tamper with the standard hardware and software configurations on notebooks and tablet devices could face disciplinary action and have the equipment withdrawn;
- users must not disable any element of the standard notebooks and tablet devices configuration, including data encryption, screen-saver password and anti-virus software;
- passwords will be managed in accordance with the eHealth **SP 11.3.1 Password Management**;
- all external email, software or documents will be checked for viruses before loading onto notebooks and tablet devices;
- Corporate information may be stored locally on the notebook or tablet device for temporary usage. This information must be placed in corporate network storage and permanently removed from the notebook or tablet device as business processes are required.
- notebooks and tablet devices will be held in a secure, locked enclosure or physical control when not in use;
- IT will keep a register of notebooks and tablet devices in use with details of owners and installed software;
- the standard notebooks and tablet device configuration will be maintained, updated and applied to individual equipment to provide up-to-date protection features to secure local information.

On the Move (User)

- Ensure that notebooks and tablet devices are not left unattended when traveling, being particularly vigilant on public transport and in public places such as stations, airports, restaurants and hotels.
- If using a security token to permit authenticated access to a particular application, then these devices must also be carried separately from the laptop.
- If you must use your laptop in a public place, make sure that others cannot see your work, and never process sensitive material under these circumstances.

Using Your Mobile Computer Securely (User)

- Ensure that either the supervisor system (BIOS) password has been set or a centrally managed hard drive encryption is used to secure boot sector as well as data partitions.
- Ensure that notebooks and tablet devices operating systems must be locked when not in use.
- All notebook and tablet devices are provided for corporate use. Refer to acceptable use policy for more information.

Taking Your Mobile Computer out of Country

Before taking your notebook or tablet device out of country you should seek advice from the IT designate or relevant line manager. (e.g.; remote access, patch management, etc.)

If Corporate Notebooks or Tablets in Your Care is Lost or Stolen

Report the incident immediately. Refer eHealth SP 13.1 Reporting IT Security Incidents

11.7.2 Granting of Remote Access to Information Systems
eHealth Saskatchewan

Subject/Title: ***Granting of Remote Access to Information Systems***	**Revision Number: 1.0**
Approving Authority: eHealth Security Office **Name:** **Title: Chief Security Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate processes and procedures that ensure that remote access to information maintains the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

eHealth shall grant remote access to information under its custodianship only to authorized persons, and only for authorized purposes in accordance with this policy. eHealth shall establish clear accountability structures supported by appropriate systems, policies and procedures to protect personal health information accessed remotely through computer connections and any other electronic means from any unauthorized use, disclosure or modification as required under *The Health Information Protection Act*.

This policy will:

1. To set out the requirements for the granting of remote access to information systems under the custodianship of the eHealth.
2. To establish criteria and safeguards pertaining to remote access to information systems.
3. To comply with the requirements of *The Health Information Protection Act*.

Applicability

This policy applies to all individuals within the corporation: individuals, providers, vendors, consultants, volunteers, students and other persons acting on behalf of the eHealth.

Detailed Policy

Granting Of Access to Health Information

Responsibilities of Users Granted Remote Access

Users who have been granted remote access to information shall:

- comply with all applicable contracts or agreements;

- protect the confidentiality and privacy of the information;
- use the personal health information responsibly and appropriately; and
- maintain the integrity and accuracy of the personal health information.

Users shall not use, modify, or disclose personal health information to non-authorized persons unless it is done in accordance with ***The Health Information Protection Act*** and eHealth's privacy and/or security Policies.

Access Security

All Remote Access by authorized users shall use two-factor authentication to validate the User's identity.

Application for Remote Access Privileges

Individuals working on behalf of eHealth

Remote access to information systems shall be granted on a limited basis to authorized persons who have a demonstrated need for access. An applicant requesting remote access shall seek approval from either the eHealth designated access administrator or his/her supervisor, who has responsibility to approve such requests. Approved requests shall be forwarded to the eHealth*'s* network administrator or designated administrator to facilitate remote access.

Remote access to the eHealth network and resources will only be permitted providing that authorized users are specifically authenticated (no generic or anonymous access accounts), data is encrypted across the network (from client workstation to eHealth network), and privileges are restricted to the appropriate information and systems. Refer to Process – **Acceptance Criteria for Remote Access Connection.**

Healthcare Providers

Remote access to information systems shall be granted on a limited basis to authorized providers who have a demonstrated need for access. An applicant requesting remote access shall seek approval from the eHealth designated access administrator, who has responsibility to approve such requests. Approved requests shall be forwarded to the eHealth*'s* network administrator or designated administrator to facilitate remote access.

Remote access to the eHealth network and resources will only be permitted providing that authorized providers that are specifically authenticated (no generic or anonymous access accounts), data is encrypted across the network (from client workstation to eHealth network), and privileges are restricted to the appropriate information and systems. Refer to Process – **Provider Acceptance Criteria for Remote Access Connection.**

"Business To Business" (EMR to EHR)

Requests for "Business To Business" access (i.e., connection between a distinct network infrastructure and that of eHealth) shall be submitted, in writing, to the Security Office. Such connections shall require authorization of the eHealth CIO (or designate). A Service Level Agreement shall outline the level of IT support to be provided by eHealth.

Assessments

Privacy Impact Assessment (PIA)

The need for a PIA shall be determined by the Privacy Office. In the event that a PIA is required, it shall be carried out under the direction of the Privacy Office.

Threat Risk Assessment (TRA)

For each application, a Threat Risk Assessment followed up with a Security Assessment will also be carried out under the direction of eHealth's Security Office.

Any decision with respect to the application for remote access shall be subject to the findings and recommendations of these assessments.

Vendor Support

In the event that a vendor requires remote access to eHealth network applications that contain personal health information for the purposes of providing system and/or application support, eHealth shall enter into a contractual relationship with the vendor. The contract shall clearly outline the terms and conditions for the granting of remote access privileges.

Threat Risk Assessment (TRA)

For each vendor, a Threat Risk Assessment will be carried out under the direction of the eHealth Security Office.

Any decision with respect to the application for remote access shall be subject to the findings and recommendations of these assessments.

Costs

Any costs incurred by eHealth in the provision of Remote Access shall be payable by the applicant. Costs, as determined by fee schedules established by eHealth, may include expenses for computer hardware, software requirements, or costs of ongoing technical support.

Training

The applicant shall be required to undergo training for the application(s) to which he/she has requested remote access. Training shall be provided by eHealth. The applicant shall be responsible to contact the appropriate application "owner(s)" and attend all required training sessions before the remote connection is established.

The applicant shall be required to undergo security and privacy awareness training as provided by eHealth prior to gaining access to remote systems.

Surveillance and Monitoring

The Security Office and Privacy Office reserve the right to monitor and audit any and all access to personal health information. The surveillance and auditing may include: periodic reviews, random audits, and pattern recognition of individual usage to personal health information to ensure compliance with the protection of privacy guidelines.

FOIP

The Security Office and Privacy Office may be required to provide audit and log reports of access to personal health information in support of Freedom of Information requests (FOIP). The reports will include: who accessed the information, when the access was done and what personal health information was accessed.

Withdrawal of Remote Access Privileges

Inappropriate access, use or disclosure of information under the custodianship of eHEALTH shall result in the immediate withdrawal of remote access privileges and the filing of a Security Incident with the Security Office and Privacy Office in accordance with the Security Incident Response Policy.

Privileges will also be withdrawn in the event that computer infrastructure for the remote access fails to meet eHealth's security standards.

Additional References

Process – Acceptance Criteria for Remote Access Connection
Process - Provider Acceptance Criteria for Remote Access Connection
Policy - Security Incident Response Policy

12 System Development and Maintenance

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To ensure that security is built into information systems.

This includes infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting application or service can be crucial fro security. Security requirements are identified and agreed upon prior to the development of information systems.

It is our goal to identify as many of the security requirements during the requirements phase of a project and to ensure they are justified, agreed and documented as part of the overall business case for any new systems.

Objective 2.) To prevent loss, modification or misuse of user data in application systems.

Appropriate controls and audit trails or activity logs are designed into application systems, including user in-house developed applications. These controls include validation of input data, internal processing and output data.

Objective 3.) To protect the confidentiality, authenticity or integrity of information.

Cryptographic systems and techniques are used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

Objective 4.) To ensure that IT projects and support activities are conducted in a secure manner.

Access to system files is controlled.

Maintaining system integrity is the responsibility of the user function, development group or program area to whom the application system or software belongs.

Objective 5.) To maintain the security of application system software and information.

Project and support environments are strictly controlled.

Managers responsible for application systems are also responsible for the security of the project or support environment. They are required to ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operation environment.

12.1 Security in Application Systems
eHealth Saskatchewan

Subject/Title: *Security in Application Systems*	Revision Number: 1.0
Approving Authority: eHealth Security Office Name: Title: Chief Security Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, controls and architecture that ensure applications are able to maintain the confidentiality of personal, health and business information in its care and custody, in compliance with legislation.

Scope/ Purpose

eHealth is committed to ensuring the integrity and security of Information Technology (IT) Resources used to generate, process, transmit, store, or access information. Therefore, all IT Resources shall be used in a secure manner and are subject to access and security controls.

To prevent loss, modification or misuse of user data in application systems.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Security Requirements in Application Systems

An eHealth approved system life cycle methodology, including the Application Verification Toolkit (AVERT) security review, is required for the development of any application internally developed by eHealth, commercial off the shelf or externally developed applications.

Security in Application Systems

eHealth shall incorporate validation checks into applications to detect any Information corruption through processing errors or deliberate acts. Both input and output data shall be validated where possible. Information Systems shall be checked regularly by eHealth for compliance.

Access Control to Program Source Library

Access to program source code and associated items such as documentation describing the functionality of an application will be controlled following the information classification guidelines described in the **Security Classification for Information Version 1.5 - Security Framework Strategy**

Segregation of Duties

Prior to the development and implementation of a new information system, or an enhancement to an existing Information System, security control requirements are specified and integrated into the project during the feasibility stage. eHealth shall ensure a separation of duties exists between the groups responsible for the development, operation, audits, and administration of Information Systems through regular management reviews.

System Acceptance

Operational requirements of any new Information System or any enhancement to an existing Information System, shall be established, documented, and tested prior to acceptance for production.

Segregation of Production and Other System Environments

All individuals that work on behalf of eHealth that run test new software provide documentation and assistance to eHealth operations responsible for the installation of new services in the production environment. This recommendation is made to mitigate the risk of individuals unintentionally or inadvertently issuing system commands on the wrong system.

THREAT-RISK ASSESSMENT

The Security Office shall conduct a Threat-Risk Assessment using the eHealth Application Verification Toolkit (AVERT) on any new applications or modifications to existing high-risk systems. The results of the Threat-Risk Assessment shall be used to determine the Information Asset Classification, the level of Threat-Risk to the Information Asset, and any recommendations necessary to mitigate the Threat-Risk to make it acceptable. The Threat-Risk Assessment at a minimum shall include:

- a high level AVERT process performed at the beginning of a Project;
- a detailed level AVERT process performed at the User Acceptance and Testing phase of a project;
- an AVERT automated Vulnerability Assessment (VA) ran against the application, following the automated tools best practises;
- a detailed report containing the findings of the detailed level AVERT, the results of the automated vulnerability assessment, and the recommendations from the Security Office as to whether the project can proceed or if there is an unacceptable amount of risk to continue.

Operational and Clinical Databases

The use of operational and clinical databases containing confidential and restricted information for testing and training purposes shall be avoided.

Encryption

The Security Office shall develop standards for the use of cryptographic controls, to protect the confidentiality, authenticity, and integrity of electronic Information. Data Classification shall be performed to identify the required level of encrypted protection for electronic Information (e.g., confidentiality, integrity/authenticity, non-repudiation). Refer to the **Security Classification for Information V 1.5.1 - Security Framework Strategy** and **Chart – Information Security Classification and Standards**.

When designing and implementing cryptographic controls, The Security Office shall ensure that controls comply with applicable legislation, regulations, and Collective Agreements.

All cryptographic keys shall be protected against modification, loss, destruction, and unauthorized disclosure. eHealth Resources used to generate, store, and archive cryptographic keys shall be physically and logically protected.

13 Information Security Incident Management

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Objective 2.) To ensure a consistent and effective approach is applied to the management of information security incidents.

13.1 Reporting Privacy and Security Incidents
eHealth Saskatchewan

Subject/Title: ***Reporting Privacy and Security Incidents***	**Revision Number: 1.0**
Approving Authority: eHealth Privacy Office and the eHealth Security Office **Name:** **Title: Chief Security Officer and Chief Privacy Officer**	**Effective Date:** **March 1, 2011** **Revision Date:** **February 28, 2013** **Toolkit Reference:**

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate processes and procedures to capture and report privacy and security incidents and breaches to all levels of management, in compliance with legislation.

Scope/ Purpose

It is the responsibility of all individuals within the corporation to report all privacy and security incidents and breaches when they are discovered.

The intention of this policy is to minimize the damage from privacy and security incidents and breaches, and to monitor and learn from such incidents.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

All individuals working on behalf of eHealth that become aware of possible privacy or security incidents or breaches shall report them to their own supervisor, or to the supervisor of the individual who may have been involved with the incident. It is then the supervisor's responsibility to assess whether a violation has occurred.

Reporting Security Breaches/Incidents

Examples of activities that constitute security breach/incident include, but are not limited to:

- **Password compromised** – you discover that someone else has access to your account using your password, or others are misusing passwords.
- **Hacking attempt** – certain systems may disable accounts where the wrong password was entered three times. If your account was disabled because someone else was attempting to access it, then a security incident has occurred.

- **Computer virus infection** – virus infection that was not detected and cleaned automatically.
- **Computer files missing** – unexplained deletion of any file.
- **Unexplained changes to system data/configuration** – any unexplained change to data.
- **Theft/loss of IT equipment** – a theft or loss is an information security incident if it means that information is lost or made available to others.
- **Unauthorized people using** or attempting to use IT equipment.
- **Unauthorized people gaining access** to protected areas.
- **Violations** to eHealth **SP 7.1.3 Acceptable Use of Assets.**
- **Violations to the eHealth Privacy and/or Security Policies**
- **New vulnerabilities and exploits** discovered in existing IT systems. Security Operations analysts are exempt from this requirement as this is part of their existing duties.

Reporting Privacy Breaches/Incidents

Examples of activities that constitute privacy breach/incident include, but are not limited to:

- **Disclosure** – you discover that someone has been given or sent information that was not intended for their use.
- **Inappropriate Access** – Access to information is part of operational requirements for certain jobs. Inappropriate access is when an authorized user gains access to information that was not specifically for the purpose of their job.
- **Limiting Collection** – you find out that more information is being collected and retained then what is necessary to provide service.
- **Safeguards** – safeguards that are either technical or non-technical have been circumvented or ignored when accessing or collecting information.
- **Consent** – that consent directives are not being captured or that consent directives are being circumvented or ignored.
- **Limiting Use** – that the information collected has been used for purposes that were not identified when it was originally collected.
- **Unauthorized Access** – that someone as attempted to gain access to information that they were not authorized for, electronically or paper based.
- **Accuracy –** it was found that information is knowingly or unknowingly incorrect which could lead to a misrepresentation or adverse outcome.
- **Violations** to eHealth **SP 7.1.3 Acceptable Use of Assets** that would involve information.
- **Violations to the eHealth Privacy Policies**

Supervisors can consult with the following on their decision:
: the Human Resources consultant;
: the Chief Security Officer;
: the Chief Privacy Officer;

eHealth Corporate Services can assist with interpretation and application of the policies and processes relating to investigating and addressing behaviour or work performance issues. Violations of the eHealth policies shall be addressed in a manner similar to other types of unacceptable behaviour or work performance issues.

The managers of eHealth can assist with interpretation of eHealth policies as they relate to privacy and security of information and technical resources. A privacy or security representative can provide technical support to confirm if an IT resource has been inappropriately accessed, and assist in identifying and implementing technical options to prevent subsequent violations and security exposures.

The Privacy Office and Security Office shall collaboratively prepare procedures for reporting privacy and security breaches and incidents (see **Process - Privacy and Security Breach Management Guidelines)**. The privacy or security representative will complete a Privacy and Security Incident Reporting form outlining details of the incident and their suggestions to mitigate future risk. Once complete, this form will be signed by the appropriate senior manager along with the Chief Privacy and Chief Security Officer. The form will then be filed with the Security Office for future reference.

Copies of the Privacy and Security Policies are available on the eHealth Intranet.

Other policies that apply to individuals who provide services to eHealth and who have access to eHealth's IT resources include:

: Freedom on Information and Protection of Privacy
: Health Information and Privacy Act
: Harassment
: Performance Improvement
: Corrective Discipline
: Conflict of Interest

Reporting IT Privacy or Security Weaknesses

All individuals working on behalf of eHealth are asked to inform their immediate managers of any observed or suspected privacy or security weaknesses in, or threats to systems or services provided by eHealth as quickly as possible. If management is not available please contact the service desk with this information.

eHealth asks that, under no circumstances, you attempt to prove a suspected weakness as this could result in potential misuse of the system.

Reporting Software Malfunctions

All individuals working on behalf of eHealth are asked to contact the service desk with any information regarding software malfunctions or support issues.

14 Business Continuity Management

Policies within this section of the framework require the approval from the Security Office or co-approval from units within eHealth that currently have ownership of that responsibility. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To counteract interruptions to business activities and to protect critical business processes from effects of major failures or disasters.

A business continuity management process has been implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

The consequences of disaster, security failures and loss of service need to be analysed. Contingency plans are developed and implemented to ensure that business processes can be restored within the required time-scales. The business continuity plans need to be maintained and practised to become an integral part of all other management processes.

The business continuity management process includes controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

14.1.1 Business Continuity Management
eHealth Saskatchewan

Subject/Title: *Business Continuity Management*	Revision Number: 1.0
Approving Authority: eHealth Operations Name: Title: Chief Operating Officer	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure that the security controls and protections in place are not circumvented during the testing or execution of the business continuity / disaster recover plan, in compliance with legislation.

Scope/ Purpose

Business continuity Planning (BCP) is essential for the continuation of key business services, in the event of an unexpected occurrence which seriously disrupts the business process.

Through risk assessments, BCP analyses the nature of such unexpected occurrences, their potential impact, and the likelihood of these occurrences becoming serious incidents.

In order to succeed, a formal BCP project must be initiated, have adequate allocated funding and sufficient human resources

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

BUSINESS CONTINUITY PLANS

eHealth shall make every effort to minimize the impact of a disaster or other adverse event, while ensuring the timely resumption of essential operations. Business Continuity Plans (BCP) are required, as determined by the Security Office to protect against corporate vulnerabilities resulting from such an event. A single framework for BCPs shall be maintained to ensure consistency.

Each BCP shall have a specified owner based on the business resources or processes involved. The plan owner shall ensure procedures are in place for carrying out the continuity plan, including the training and education of individuals, and shall ensure that:

- BCPs identify all assets involved in critical business performance and address the Information Security requirements needed for business continuity. BCPs shall identify the training and

responsibilities of individuals working on behalf of eHealth, and identify acceptable Information and service loss.

- multiple copies of BCPS are stored in locations distant enough so as to not be in danger if a disaster occurs at a particular Facility. Business Continuity Plans shall be protected to maintain the security of corporate-specific details.
- BCPs shall be tested and updated regularly to ensure that they are timely and effective.
- The BCP is maintained and re-assessed on by having a regularly scheduled review process in place.

Information owners shall ensure regular back up of essential software and Information, to allow recovery following a disaster or system failure. Recovery of Information shall be tested periodically by the Information owner.

15 Compliance

Policies within this section of the framework require the approval from the Chief Executive Officer. This ownership is identified within the Approving Authority area of the sub-policies below.

Objective 1.) To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The design, operation, use and management of information systems at eHealth are subject to statutory, regulatory and contractual security requirements.

Advice on specific legal requirements should be sought from eHealth's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from province to province and need to be taken into consideration when utilizing trans-border data flow.

Objective 2.) To ensure compliance of systems with corporate security policies and standards.

The security of information systems is regularly reviewed.

Such reviews will be performed against the appropriate security policies and the technical platforms and information systems will be audited for compliance with security implementation standards.

Objective 3.) To maximize the effectiveness of and to minimize interference with the audit process.

Controls will be put into place to safeguard operational systems and audit tools during system audits.

Protection is also in place to safeguard the integrity and prevent misuse of audit tools.

15.2.1 Compliance
eHealth Saskatchewan

Subject/Title: *Compliance*	Revision Number: 1.0
Approving Authority: eHealth Executive Management Name: Title: CHIEF EXECUTIVE OFFICER	Effective Date: March 1, 2011 Revision Date: February 28, 2013 Toolkit Reference:

Note: *It is the responsibility of all individuals within the corporation to ensure they are working to the most up to date and relevant policies and procedures. By so doing, the quality of the services offered will be maintained and the chances of individuals working on behalf of eHealth making erroneous decisions, which may affect patient, individuals working on behalf of eHealth or visitor safety and comfort, will be reduced.*

General Policy Statement

eHealth shall develop, implement and maintain appropriate standards, processes and procedures that ensure all aspects of the security controls are being followed and that appropriate disciplinary measures are applied, in compliance with legislation.

Scope/ Purpose

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements.

To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

Applicability

This policy applies to all individuals within the corporation: individuals, volunteers, students, contractors and other persons acting on behalf of eHealth.

Detailed Policy

Auditing

The Security Office will:

- establish processes for the monitoring of IT resources to ensure the integrity of such resources while providing protection from potential threats;
- assign a designate to monitor, track, and review the eHealth security standards;
- in consultation with the relevant Trustee (where applicable), shall perform a Threat-Risk Assessment to determine the required level and frequency of monitoring.
- perform audits and random system validations on database, application and networking systems within eHealth to verify logical and physical consistency.
- perform both planned and random audits on database, application, server, desktop and networking systems to validate compliance with legislative and Ministerial regulations and policies.

Collection of Evidence
The Security Office will provide processes for the proper collection of evidence as well as supervise any forensic analysis of the eHealth information processing systems.

Protection of Information Processing Systems
All system security audit tools including software, data and technical devices will be maintained and used by the Security Office personnel or under their direct supervision.

APPENDIX A – Mapping of eHealth Security Policy Framework

Old Policy to New (net new policies are not shown)

eHealth SP 2.0a		eHealth SP 2.6	
4.1.1	Organizational Information Security	6.1	Organizational Information Security
5.1	Information Assets	7.1.1	Information Assets
6.1.1	Including Security In Job Descriptions	8.1.1	Including Security In Job Descriptions
6.2.1	Appropriate Use of Technology	7.1.3	Appropriate Use of Assets
6.3.1	Reporting IT Security Incidents	13.1	Reporting IT Security Incidents
7.1	Physical Security of NON SPM Facilities	9.1.1	Physical Security of NON Government Services Facilities
7.2	Working in a Secure Environment	9.1.5	Working in a Secure Environment
8.1.1	IT Operations Policy	10.1	IT Operations Policy
8.2	Capacity Planning and System Acceptance	10.3	Capacity Planning and System Acceptance
8.3.1	Controls Against Malicious Software	10.4	Controls Against Malicious Software
8.5	Network Management	10.6	Network Management
8.6	Information labelling and Security	7.2.2	Information labelling and Security
8.7	Security of Electronic Mail	10.8.4	Security of Electronic Mail
8.7.7	Wireless Access	10.6.1.1	Wireless Access
9.1.1	Electronic Information Access Control	11.1.1	Electronic Information Access Control
9.3	User Responsibilities	11.3	User Responsibilities
9.3.1	Password Management	11.3.1	Password Management
9.7	Monitoring System Access and Use	10.10.1	Monitoring System Access and Use
9.8.1	Mobile Computing	11.7.1	Mobile Computing
9.8.2	Granting of Remote Access to Information System	11.7.2	Granting of Remote Access to Information System
10.2	Security in Application Systems	12.1	Security in Application Systems
11.1.1	Business Continuity Management	14.1.1	Business Continuity Management
12.1	Compliance	15.2.1	Compliance

New Policy to Old (net new policies shown)

eHealth SP 2.6		eHealth SP 2.0a	
6.1	Organizational Information Security	4.1.1	Organizational Information Security
7.1.1	Information Assets	5.1	Information Assets
7.1.2.1	Releasing Source Code		
7.1.3	Appropriate Use of Assets	6.2.1	Appropriate Use of Technology
7.2.1	Information Asset Classification		
7.2.2	Information labelling and Security	8.6	Information labelling and Security
8.1.1	Including Security In Job Descriptions	6.1.1	Including Security In Job Descriptions
9.1	Secure Area Classification		
9.1.1	Physical Security of NON Government Services Facilities	7.1	Physical Security of NON SPM Facilities
9.1.5	Working in a Secure Environment	7.2	Working in a Secure Environment
9.2.6	Information Technology Asset Disposal		
10.1	IT Operations Policy	8.1.1	IT Operations Policy
10.3	Capacity Planning and System Acceptance	8.2	Capacity Planning and System Acceptance
10.4	Controls Against Malicious Software	8.3.1	Controls Against Malicious Software
10.6	Network Management	8.5	Network Management
10.6.1.1	Wireless Access	8.7.7	Wireless Access
10.8.4	Security of Electronic Mail	8.7	Security of Electronic Mail
10.10.1	Monitoring System Access and Use	9.7	Monitoring System Access and Use
11.1.1	Electronic Information Access Control	9.1.1	Electronic Information Access Control
11.3	User Responsibilities	9.3	User Responsibilities
11.3.1	Password Management	9.3.1	Password Management
11.7.1	Mobile Computing	9.8.1	Mobile Computing
11.7.2	Granting of Remote Access to Information System	9.8.2	Granting of Remote Access to Information System
12.1	Security in Application Systems	10.2	Security in Application Systems
13.1	Reporting IT Security Incidents	6.3.1	Reporting IT Security Incidents
14.1.1	Business Continuity Management	11.1.1	Business Continuity Management
15.2.1	Compliance	12.1	Compliance