Information Security Policy

Ministry of Central Services
Information Technology Division
Information Security Branch

Last revised: December 2016
Last reviewed: December 2016
Next review: July 2017

Government of Saskatchewan

Version Control			
Ver.	**Date**	**Changes**	**Authorization**
1.0	October 01, 2015	Original Version	Chief Information Officer
1.1	March 10, 2016	Sec. 5.3.1 Password Standards: lockout attempts changed to five;	Chief Information Officer
1.2	July 04, 2016	Sec. 2.1.1 p. 17 removed two bullets from Information Owners responsibilities;	Chief Information Officer
1.3	July 13, 2016	Sec. 1.1.1 Standards paragraph amended; Sec. 10.1.1 one bullet amended; Sec. 10.1.3 amended; Sec. 12.1.2 added one bullet to list;	CIO Director, ISB CIO Director, ISB
1.4	July 21, 2016	Sec. 5.2.3 added local admin standard; Sec. 6.1.1 SSH/sFTP standard: one bullet amended;	Director, ISB
1.5	December 8, 2016	Sec. 5.4.2 added standard for GMSAs;	Director, ISB

Table of Contents

Government of Saskatchewan

Information Security Policy

Introduction

Introduction

The Information Security Policy is intended to help safeguard the confidentiality, integrity and availability of the government's information assets. It forms part of the government's Information Security Program whose objectives are to:

- establish a coordinated, enterprise approach to IT security across government;
- implement modern, fit-for-use security and information protection technologies;
- ensure that data under the care of government is safeguarded appropriately; and
- reduce the government's risk profile.

These policies and standards are issued pursuant to Section 3(k) of *The Ministry of Central Services Regulations.* In accordance with that section Information Technology Division has the responsibility:

> *"to develop, implement, monitor and enforce security policies and standards of the Government of Saskatchewan respecting information technology, information management and records management;"*

This policy applies to Ministries and "prescribed public agencies" supported by the Ministry of Central Services pursuant to *The Information Technology Office Service Regulations.* When the term "Ministry" is used in the text it means "ministry" as defined by *The Executive Government Administration Act.* (see glossary)

This policy is based on the international standard known as "ISO/IEC 27002:2013."[1] We would also like to acknowledge the contributions from the Government of British Columbia and the Government of Alberta.

[1] Information technology – security techniques – Code of practice for information security controls, International Standard ISO/IEC 27002, Second edition 2013-10-01.

Government of Saskatchewan

Information Security Policy

Chapter 1

Management Directive

Chapter 1 – Management Directive		
1.1 Management Direction for Information Security		
1.1.1	Policies for Information Security	The Chief Information Officer is responsible for establishing, issuing and monitoring the compliance of information security policies.
1.1.2	Review of the Policies for Information Security	The information security policy must be reviewed at least every two years and updated when required.

1.1 Management Direction for Information Security

Objective:

To provide management direction and support for information security in accordance with the government's business requirements and relevant laws and regulations.

1.1.1 Policies for Information Security

The Chief Information Officer is responsible for establishing, issuing and monitoring the compliance of information security policies.

The Information Security Policy contains operational policies and standards intended to safeguard the confidentiality, integrity and availability of government information and information systems. It establishes the minimum requirements for the secure delivery of government services through:

- management and business processes that include and enable security processes;
- ongoing security awareness for personnel;
- physical security for sensitive information assets;
- governance processes for information technology;
- reporting of information security incidents;
- including information security in business continuity planning; and
- monitoring for compliance.

The Chief Information Officer (CIO) recognizes that information security is a process. In order to be effective, it requires management commitment and continuing security awareness efforts. Other principles that guide the government's directions are:

- information security requires a multi-layered defense strategy, and
- security is everyone's responsibility.

The Information Security Policies establish a baseline level of security that applies throughout government. Ministries may develop and implement additional policies, standards and guidelines for use within their organization or for a specific information system or program. Those additional policies may exceed but must not conflict with this policy.

Ministries must provide the Chief Information Officer with copies of any locally developed information security policies, standards or guidelines.

The Chief Information Officer must maintain a central repository for the collection of Ministry-developed policies, standards or guidelines.

Standards

Standards, where they exist, are included in the corresponding policy chapter. The Director, Information Security Branch, will issue and revise government standards as needed.

Risk Management Decision Item

When information security polices or standards cannot be complied with, the details must be documented in a Risk Management Decision Item (RMDI). The RMDI must record the policies violated and the risks associated with the non-compliance. When the request involves a Ministry application or system, the risks must be jointly accepted by the Ministry Security Officer and the Director, Information Security Branch (on behalf of the CIO). When the issue involves Information Technology Division only then the Director, Information Security Branch (acting on behalf of the CIO), must sign and accept the risk before the non-compliant request is implemented.

1.1.2 Review of the Policies for Information Security

The information security policy must be reviewed at least every two years and updated when required.

The Chief Information Officer must, at least every two years, review the information security policies, standards and guidelines in an effort to ensure their continuing adequacy and effectiveness. Reviews must consider:

- feedback from stakeholders;
- legislative, regulatory or policy changes that impact information security and/or information management;
- the planning and implementation of new or significantly changed technology;
- major initiatives (e.g. new information systems or contracting arrangements);
- audit reports or reviews of security controls that identify high risk vulnerabilities;
- threat or vulnerability trends produced from automated monitoring processes that indicate an increased risk to information assets;
- reports from security incident investigations;
- the renewal of supplier access agreements which involve major government programs or services;
- the introduction or revision of national, international or industry standards for information security that address emerging technology issues; and
- reports from associated external agencies (e.g. Privacy Commissioner, Police) that identify emerging trends related to information security.

Where Ministries have developed specific policies they must review them at least every two years and provide the Chief Information Officer with updated versions.

Government of Saskatchewan

Information Security Policy

Chapter 2

Organization of Information Security

Chapter 2 – Organization of Information Security		
2.1 Internal Organization		
2.1.1	Information Security Roles and Responsibilities	All information security responsibilities must be defined and allocated.
2.1.2	Segregation of Duties	Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of information systems.
2.1.3	Contact with Authorities	Appropriate contact with Local, Provincial and Federal Authorities must be maintained.
2.1.4	Contact with Special Interest Groups	Appropriate contacts must be maintained with information security forums and related professional associations.
2.1.5	Information Security in Project Management	Information security must be addressed in project management regardless of the type of the project.
2.2 Mobile Devices and Teleworking		
2.2.1	Mobile Device Policy	Appropriate security controls must be implemented to mitigate risks associated with the use of mobile devices.
2.2.2	Teleworking	Appropriate security controls must be implemented to mitigate risks associated with teleworking.

2.1 Internal Organization

Objective:

To establish a framework to initiate and control the implementation and operation of information security within the government.

2.1.1 Information Security Roles and Responsibilities

All information security responsibilities must be defined and allocated.

The following outlines the organization of information security in the Government of Saskatchewan. Roles, responsibilities and accountabilities for key positions are described.

Chief Information Officer (CIO)

The Chief Information Officer is responsible for:

- advising the Minister of Central Services and the Deputy Minister of Central Services on Government of Saskatchewan information security policy;
- setting government-wide security objectives, standards and guidelines;
- monitoring compliance at a government-wide level and managing a process for exceptions; and
- managing policy instruments according to the principles laid out by the Information Security Branch.

Director, Information Security Branch

The Director, Information Security Branch, is responsible for:

- developing the Information Security Program;
- implementing government-wide information security policies;
- coordinating regular reviews of policies for effectiveness and relevancy;
- ensuring policies are consistent with current technology and security requirements; and
- representing the CIO and Ministry of Central Services on matters pertaining to security.

Information Security Branch

Information Security Branch, Information Technology Division, Ministry of Central Services, is responsible for:

- identifying and mitigating risks to information and information systems within the Government of Saskatchewan;
- providing government with timely and accurate information regarding current and future information security risks as they relate to government service delivery;
- endorsing a service delivery model which focuses on relationship management, security investment planning, compliance, awareness and training;
- policy development, coordination of security standards and management of the information security portfolio; and
- procuring external suppliers for various information security services.

Security specialists in Information Security Branch are responsible for:

- interpreting the Information Security Policy to assist in the delivery of business functions;
- evaluating information security implications of new government initiatives;
- performing information system security risk analysis activities;
- performing information security assessments and reviews;
- evaluating new threats and vulnerabilities;
- investigating information security incidents;
- advising on the information security requirements for documented agreements;
- analyzing and providing advice on emerging information security standards; and,
- providing information security advice to supported Ministries and agencies.

Ministry Security Officer

Each Ministry must have a designated Security Officer who is responsible for:

- ensuring that standards/procedures to support day-to-day security activities are documented in compliance with the Information Security Policy;
- co-ordinating information security awareness and education;
- investigating reported information security events to determine if further investigation is warranted;
- providing up-to-date information on issues related to information security;
- assisting business areas in conducting Threat and Risk Assessments (Section 10.1.1);
- providing advice on security requirements for information systems development or enhancements;
- co-ordinating ministry information security initiatives with cross-government information security initiatives;
- providing advice on emerging information security standards relating to ministry specific lines of business; and,
- raising ministry security issues to the cross-government Security Officers' Committee.

Security Officers' Committee

The Security Officers Committee (SOC) must have representation from each Executive Government Ministry. Agencies must also be represented when their IT infrastructure is supported by Information Technology Division. The SOC is responsible for:

- enhancing the overall security posture of the government;
- advising government on security as a business process;
- guiding the development of a security governance framework that incorporates strategies, reporting, policies, training, enforcement and compliance;
- working with Information Security Branch in the development, review and approval of policies, standards and guidelines;
- striving to ensure the highest standard of information protection; and
- the communication and awareness of information security policy.

Information Owners

Information Owners have the responsibility and decision-making authority for information throughout its life cycle including creating, regulating, restricting and administering its use and disclosure. Information owners must:

- determine business requirements including information security needs;
- ensure information and information systems are protected commensurate with their value and level of sensitivity;
- define security requirements during the planning stage of any new or significantly changed information system;
- provide and manage security for information assets throughout their lifecycle;
- determine authorization requirements for access to information and information systems;
- approve access privileges for each user or set of users;
- document information exchange agreements;
- develop service level agreements for information systems under their custody or control;
- implement processes to ensure users are aware of their security responsibilities;
- monitor that users are fulfilling their security responsibilities; and
- participate in security reviews and/or audits.

Service Owners

Information Technology Division (ITD) manages the government's information technology network including its architecture, security, file systems, and physical infrastructure such as computers, storage systems and mobile devices. ITD also assists clients with the procurement, operation, management and upgrading of applications. Service owners have the responsibility and decision-making authority for:

- Application Management Services
- Operations
- Project Management
- Data Centre Services
- Network Services
- Information Security Branch
- Client Request Services
- Deployment Services
- Regional Support Services
- Remote Support Services
- Account Management
- Problem Management
- Service Desk

Service Owners must:

- ensure information and information systems are safeguarded in accordance with their value and level of sensitivity;
- provide and manage security for information assets throughout their lifecycle;
- maintain and operate the technical infrastructure on which information systems reside;
- maintain and operate the security infrastructure that safeguards information systems; and
- develop service level agreements for information technology assets under their custody or control.

2.1.2 Segregation of Duties

Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of information systems.

Information Owners must reduce the risk of a disruption of information systems by:

- requiring complete and accurate documentation for all information systems;
- requiring that no single individual has access to all operational functions of an information system;
- rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on critical systems;
- automating functions to reduce the reliance on human intervention;
- requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- requiring that individuals responsible for initiating an action are not responsible for authorizing that action, and:
- implementing security controls to minimize opportunities for collusion.

Information Technology Division must ensure that:

- creating accounts with elevated privileges is documented and approved by an appropriate officer;
- system, service and application administration duties are segregated;
- application development and database administration are segregated;
- the person who uses an account is not the person who created the account;
- no one single person has control over a business process from inception to completion.

2.1.3 Contact with Authorities

Appropriate contact with Local, Provincial and Federal Authorities must be maintained.

The Director, Information Security Branch, must ensure that external authorities, emergency support staff and service providers can be contacted by:

- maintaining and distributing a list of internal and external authorities and service providers; and
- documenting emergency and non-emergency procedures for contacting authorities as required during information security incidents or investigations.

2.1.4 Contact with Special Interest Groups

Appropriate contacts must be maintained with information security forums and related professional associations.

The Government must promote and enhance employee knowledge of industry trends in information security, best practices, new technologies and emerging threats and vulnerabilities.

Personnel with information security responsibilities must maintain currency by:

- participating in information exchange forums regarding best practices, development of industry standards, new technologies, threats, vulnerabilities, early notice of attacks, and advisories;
- maintaining and improving knowledge of information security topics; and
- creating a support network with other security specialists.

The Director, Information Security Branch, must promote professional certification and membership in professional associations for personnel throughout government that have information security responsibilities.

2.1.5 Information Security in Project Management

Information security must be addressed in project management regardless of the type of the project.

Information Owners and Project Managers must ensure that information security risks are identified and addressed as part of a project. This applies to any project regardless of its character, e.g. a project for a core business process, Information Technology or other supporting processes. The project management methods in use must require that:

- information security objectives are included in project objectives;
- an information security risk assessment is conducted at an early stage of the project to identify controls;
- information security is part of all phases of the applied project methodology.

Information security implications must be addressed and reviewed regularly in all projects. Responsibilities for information security must be defined and allocated to specified roles defined in the project management methods.

2.2 Mobile Devices and Teleworking

Objective:

To mitigate risks associated with the use of mobile devices and teleworking.

2.2.1 Mobile Device Policy

Appropriate security controls must be implemented to mitigate risks associated with the use of mobile devices.

Information Owners must consider the risks associated with the use of mobile devices in unprotected environments. The following are the minimum controls that must be implemented.

The Information Owner must:

- develop, document and implement procedures on the issuance, usage and return of mobile devices;
- ensure that only government-owned or government-managed mobile devices are used on the government network and to store government information;
- ensure all mobile devices are inventoried in accordance with Section 4.1.1;
- ensure mobile devices are returned in accordance with Section 4.1.4 and, where applicable, disposed of in accordance with Section 4.3.2;
- ensure that sensitive data on mobile devices is encrypted with approved methods;
- ensure that mobile devices are password-protected and lock automatically after a predetermined number of unsuccessful login attempts or period of inactivity;
- only allow access and storage of information that has a Security Classification of Level A on mobile devices when there is a distinct business requirement;
- ensure software to protect against malicious software is installed and maintained (Section 8.2.1);

- authorize the use of mobile devices during out-of-country travel;
- ensure users are trained on the proper use of mobile devices, associated software and services, and security incident reporting;
- ensure users are informed of and accept the terms and conditions of this policy and supporting policies; and
- ensure all consultants and IT service provider contracts and agreements include clauses which reference this and other security policies.

Users must:

- have authorization from the Ministry or agency to use mobile device(s);
- ensure that mobile devices in his or her care are only accessed by those authorized to do so;
- ensure that mobile devices are password-protected and the password applied in accordance with Section 5.3.1;
- ensure that mobile devices are not left unattended;
- protect mobile devices from loss, theft, damage and unauthorized access;
- ensure that information that has a sensitivity of Level A is not accessed by or stored on mobile devices unless s/he has received explicit authorization from the Ministry and the Information Owner to do so;
- ensure that all sensitive information transmitted by or stored on mobile devices is encrypted by approved methods;
- backup information stored on all mobile devices in accordance with Ministry policies;
- ensure that information that cannot be stored on the Ministry shared network drive must be saved to media, encrypted by an approved method and transported and stored securely;
- ensure that data on mobile devices are not the only copies that exist;
- ensure that only software authorized for use on the government network is installed;
- ensure that software is installed only by those authorized to do so;
- ensure that sensitive information is not accessed while using mobile devices in a public place (e.g. coffee shop, airport, park); and
- immediately report the loss or theft of a mobile device to the user's supervisor and the Information Technology Division Service Desk (Section 12.1.2).

2.2.2 Teleworking

Appropriate security controls must be implemented to mitigate risks associated with teleworking.

Telework arrangements must be in compliance with the Government of Saskatchewan Telework Policy (Human Resource Manual 1104).

Before granting permission to enter into a telework arrangement the Ministry must consider:

- the sensitivity of information accessed or stored at the location;
- the physical security at the teleworking location;
- likelihood of unauthorized access at the teleworking location;
- the security of home wired and wireless networks; and
- remote access threats.

Mandatory controls are:

- sensitive government information in electronic format cannot be stored at a teleworking site unless it is encrypted with approved methods;
- sensitive government information in hard copy format cannot be stored at a teleworking site unless it is in a locked cabinet;
- teleworking sites where Classification Level A information is stored must be monitored by alarm when vacant;
- only government-issued computers can be used for the processing of government information;
- only approved remote access methods can be used to access the government network;
- at least monthly, computers must be brought to the primary work site, logged into the network and have patches and updates applied; and
- a home wireless network used to access the government network must be secured in accordance with Section 9.1.1.

Government of Saskatchewan

Information Security Policy

Chapter 3

Human Resource Security

Chapter 3 – Human Resource Security		
3.1 Prior to Employment		
3.1.1	Screening	Personnel screening must be performed prior to entering a working relationship with the Government of Saskatchewan.
3.1.2	Terms and Conditions of Employment	All personnel must be made aware of and agree to the Government of Saskatchewan's expectations related to information security.
3.2 During Employment		
3.2.1	Management Responsibilities	Management must ensure that personnel apply security in accordance with policies and procedures.
3.2.2	Information Security Awareness, Education and Training	Personnel must be given appropriate information security training and be informed of changes to policies and procedures.
3.2.3	Disciplinary Process	There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.
3.3 Termination and Change of Employment		
3.3.1	Termination or Change of Employment Responsibilities	Managers must advise personnel of their information security responsibilities when employment changes or is terminated.

3.1 Prior to Employment

Objective:

To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

3.1.1 Screening

Personnel screening must be performed prior to entering a working relationship with the Government of Saskatchewan.

All new employees and contractors must be screened. The screening must be conducted in accordance with relevant legislation and Human Resource Policies of the Government of Saskatchewan.

The screening must include verification of:

- identity;
- education, skills and experience;
- employment history;
- character references;

A criminal record check must be conducted in accordance with Section PS 816 of the Human Resource Manual.

3.1.2 Terms and Conditions of Employment

All personnel must be made aware of and agree to the Government of Saskatchewan's expectations related to information security.

The terms and conditions for employees of the Government of Saskatchewan are described in the Ethics and Conduct section of the Employee Services Portal. The Oath of Office includes an entry regarding the protection of sensitive information and must be signed by the employee.

The terms and conditions for contractors and external party users must include:

- a confidentiality or non-disclosure agreement in accordance with Section 9.2.4;
- legal responsibilities and rights;
- responsibilities for the classification of information and management of government assets;
- responsibilities for the handling of external party information; and
- responsibilities for the handling of personal information and personal health information.

Managers must ensure that the terms and conditions of employment are agreed to by all personnel.

3.2 During Employment

Objective:

To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

3.2.1 Management Responsibilities

Management must ensure that personnel apply security in accordance with policies and procedures.

Managers must support the Government's information security objectives by:

- briefing all personnel on their security roles and responsibilities prior to granting access to sensitive data and systems;
- ensuring all personnel have access to this Information Security Policy; and
- ensuring all personnel conform to the terms and conditions of employment.

Employees must be made aware of the protections provided by the Public Interest Disclosure Act (2011) regarding the reporting of wrongdoings.

3.2.2 Information Security Awareness, Education and Training

Personnel must be given appropriate information security training and be informed of changes to policies and procedures.

Managers must include an information security awareness component during orientation for new personnel.

Ongoing awareness training must be conducted. Among the topics that must be discussed are:

- safeguarding sensitive government information;
- known threats to information security;
- legal responsibilities;
- information security policies, directives and guidelines;
- how to report information security events;
- appropriate use of government information and assets;
- related disciplinary processes; and
- how to obtain security advice.

3.2.3 Disciplinary Process

There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

When it is determined that an employee or contractor was responsible for a security breach or policy violation, Information Security Branch must notify the appropriate Ministry Security Officer.

Appropriate personnel in the Ministry must review details of the incident, consider disciplinary action if warranted and arrange for permanent or temporary removal of access privileges when appropriate.

The Human Resource Manual Section 803 defines Corrective Discipline processes in the Government of Saskatchewan.

3.3 Termination and Change of Employment

Objective:

To protect the government's interests as part of the process of changing or terminating employment.

3.3.1 Termination or Change of Employment Responsibilities

Managers must advise personnel of their information security responsibilities when employment changes or is terminated.

Terminated employees and contractors must be made aware of:

- ongoing security requirements including the need to not disclose sensitive government information;
- legal responsibilities;
- responsibilities described in confidentiality or non-disclosure agreements; and
- any other applicable policy or contract.

Managers can find applicable instructions and forms on the Employee Services Centre site.

When users accept different job responsibilities within government the current Manager must ensure that Ministry information assets are turned over to the Ministry. Also ensure that access to systems and services in the current Ministry is revoked.

See Sections 4.1.4 and 5.2.6 for other security controls to apply when an employee is terminated.

Government of Saskatchewan

Information Security Policy

Chapter 4

Asset Management

Chapter 4 – Asset Management		
4.1 Responsibility for Assets		
4.1.1	Inventory of Assets	An inventory of all important assets associated with information systems must be documented and maintained.
4.1.2	Ownership of Assets	Information Owners or Service Owners must be designated for all assets and services associated with the government's information technology.
4.1.3	Acceptable Use of Assets	Rules for the acceptable use of information systems must be identified, documented and implemented.
4.1.4	Return of Assets	Personnel must return government assets upon termination or change of employment.
4.2 Information Classification		
4.2.1	Classification of Information	Information must be classified in accordance with its value, sensitivity and intended use.
4.2.2	Labelling of Information	Information must be appropriately labeled in accordance with the assigned level of sensitivity.
4.2.3	Handling of Assets	Information must be appropriately handled in accordance with its assigned level of sensitivity.
4.3 Media Handling		
4.3.1	Management of Removable Media	All removable computer media must be managed and appropriate controls applied considering the sensitivity of the data they store.
4.3.2	Disposal of Media	Media must be disposed of securely using formal procedures that consider the sensitivity of the information stored.
4.3.3	Physical Media Transfer	Media being physically transported must be appropriately protected.

4.1 Responsibility for assets

Objective:

To identify government information assets and define appropriate protection responsibilities.

4.1.1 Inventory of Assets

An inventory of all important assets associated with information systems must be documented and maintained.

Information Owners and Service Owners must identify and document assets under their control including:

- software (e.g. applications, system software, development tools and utilities);
- hardware (e.g. computer and communications equipment, removable media, etc.);
- services (e.g. computer and communications services, general utilities); and
- information assets and their security classification.

Information assets include databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails and archived information.

The inventory must not duplicate other inventories unnecessarily but reference them where appropriate.

The following information must be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss or destruction:

- type of asset;
- ownership;
- format;
- location;
- assigned user (where applicable);
- backup information;
- license information;
- security requirements (confidentiality, integrity and availability); and
- consequence of loss.

The loss, theft or misappropriation of assets must be reported immediately to the Manager and the Information Technology Division Service Desk. When information is lost, stolen or misappropriated the procedures outlined in Section 12, “Information Security Incident Management,” must be followed.

4.1.2 Ownership of Assets

Information Owners or Service Owners must be designated for all assets and services associated with the governments' information technology.

Information Owners and Service Owners are responsible for:

- controlling the production, development, maintenance, use and security of information and information assets in their jurisdiction;
- ensuring that information and information assets are appropriately classified and safeguarded; and
- defining and regularly reviewing access restrictions and classifications in accordance with applicable policies.

The responsibilities of Information Owners and Service Owners are more thoroughly described in Section 2.1.1.

4.1.3 Acceptable Use of Assets

Rules for the acceptable use of information systems must be identified, documented and implemented.

All users of the government's information systems must take responsibility for and accept the duty to actively protect the government's information assets.

The requirements for core and incidental use are described in the "Information Technology Acceptable Usage Policy" found at Section PS 1103 of the Human Resource Manual.

4.1.4 Return of Assets

Personnel must return government assets upon termination or change of employment.

Managers must ensure the recovery of:

- documents, files, data, books and manuals in electronic and hard copy formats;
- information assets developed or prepared by an employee or contractor in the course of his/her duties;
- work-related email in the current and archived mailboxes;
- computer hardware, software and related equipment;
- mobile devices and portable media; and
- access cards, keys, key fobs, id cards and other government-issued devices.

The user must copy all **personal** electronic files to removable media and delete the originals from government systems.

Unreturned access devices must be documented and steps taken to ensure they cannot be used for unauthorized access to Government building, information systems and/or data.

The Employee Services Centre includes manager checklists to be used when an employee is terminated.

4.2 Information Classification

Objective :

To ensure that government information receives and appropriate level of protection in accordance with it sensitivity and value.

4.2.1 Classification of Information

Information must be classified in accordance with its value, sensitivity and intended use.

The Information Technology Division is responsible for developing an information classification system. The system must take into account the confidentiality, integrity, and availability requirements and the financial value of information assets.

The Government of Saskatchewan's information classification levels are:

- A: high sensitivity – unauthorized disclosure could cause extreme injury to government or a person;
- B: medium sensitivity – unauthorized disclosure could cause serious injury to the government or a person;
- C: low sensitivity – unauthorized disclosure could cause low injury to the government or a person;
- Public: non-sensitive – unauthorized disclosure will not result in injury to the government or a person.

Information owners must assign a level of sensitivity in accordance with the Guide for Information Protection Classification. The guide includes more details of the classification levels and examples. In determining the level of sensitivity information owners must consider that, in some cases, the aggregate of the information can be more sensitive than a smaller subset or individual record. In addition, some information is only sensitive for a certain period of time and the classification level may change accordingly.

4.2.2 Labeling of Information

Information must be appropriately labeled in accordance with the assigned level of sensitivity.

Information Owners must ensure that information, whether in physical or electronic format, is labeled with its information security classification. This communicates to information users the level of sensitivity and required safeguards.

Items for consideration include printed or electronic records, reports, files, on-screen displays, recorded media and messages.

Automated labeling must be used where available such as document templates, headers and footers, and selectable boxes in forms. Where labeling is not feasible an alternate method must be used, e.g. marking storage media, written procedures or metadata.

Information Owners must establish handling procedures for the secure processing, storage, transmission, declassification and destruction of information and digital media.

Agreements with other governments and organizations that include information sharing must include procedures to identify the level of sensitivity of the information and interpret the classification labels from external partners.

4.2.3 Handling of Assets

Information must be appropriately handled in accordance with its assigned level of sensitivity.

Information Owners and Service Owners must develop and implement procedures for handling, processing, storing and communicating information. Those procedures must consider:

- the level of sensitivity of the information;
- access restrictions supporting the safeguards for each level of sensitivity;
- maintenance of a formal record of the authorized recipients of assets;
- safeguarding temporary or permanent copies to a level consistent with the original;
- storage of information technology assets in accordance with the manufacturers' specifications; and
- clear marking of all copies of media for the attention of the authorized recipient.

Agreements with other governments and agencies that include information sharing must also include:

- identification of the classification of that information; and
- interpretation of the classification labels from other agencies.

4.3 Media Handling

Objective:
To prevent unauthorized disclosure, modification, removal or destruction of government information stored on media.

4.3.1 Management of Removable Media

All removable computer media must be managed and appropriate controls applied considering the sensitivity of the data they store.

Information Owners and Service Owners must:

- ensure that sensitive data on removable media is encrypted with approved methods;
- authorize the use of removable media during out-of-country travel;
- ensure users are familiar with the operation of removable media;
- ensure users are familiar with the policies on security incident reporting as described in Section 12.1.2; and
- ensure all users who are authorized to use removable media are aware of the need to safeguard government information in accordance with this policy.

Users of removable media must:

- have authorization from the Ministry to use removable media and store sensitive information on it;
- ensure that removable media in his or her care is only accessed by those authorized to do so;
- ensure that, where applicable, the media is password-protected and the password applied in accordance with Section 5.3.1;
- ensure that removable media is transported securely and not left unattended;
- ensure that sensitive information stored on removable media is encrypted by approved methods;
- ensure that data on removable media are not the only copies that exist, i.e. originals are on network shares;
- ensure that any removable media received from an external party is scanned for malware prior to use;
- ensured that any removable media received from a foreign country is first screened by Information Security Branch before connecting it to a government computer;
- ensure that removable media is not used for the storage of sensitive information when encryption is not available, e.g. storage card on a digital camera;
- ensure that sensitive information is not accessed while in a public place (e.g. coffee shop, airport, park); and
- immediately report the loss or theft removable media to the user's supervisor and the Information Technology Division Service Desk.

4.3.2 Disposal of Media

Media must be disposed of securely using formal procedures that consider the sensitivity of the information stored.

Purchasing Branch in Commercial Services Division of the Ministry of Central Services is responsible for preparing and publishing the "Electronic Storage Media Disposal Policy".

Information Owners must ensure that media that is no longer required operationally is disposed of securely and in accordance with the Electronic Storage Media Disposal Policy.

Information Security Branch must specify methods to sanitize disks and other digital media.

Media Sanitization Standard

The Government of Saskatchewan standard for media sanitization is:

US Department of Defense DoD 5220.22-M

Contact Information Security Branch for products that comply with this standard.

4.3.3 Physical Media Transfer

Media being physically transported must be appropriately protected.

When transporting physical media with sensitive information between sites:

- use a trusted courier;
- inspect the identification of couriers at pickup and delivery;
- obtain and retain receipts;
- pack the media in a manner that will prevent loss or damage;
- pack the media in a manner that does not disclose the level of sensitivity;
- pack it in a manner to make evident any attempted tampering.

When supported by a Threat and Risk Assessment or if enhanced security is required for other reasons:

- use a courier service that has a tracking number;
- hand deliver the media where necessary;
- use a double envelope (or double package) where the inner layer is marked with the level of sensitivity and instructions and it is packaged in another envelope;
- use a lockable container;
- encrypt the information stored on the media.

Government of Saskatchewan

Information Security Policy

Chapter 5

Access Control

Chapter 5 – Access Control		
5.1 Business Requirements of Access Control		
5.1.1	Access Control Policy	Access to information systems and services must be consistent with business needs and based on security requirements.
5.1.2	Access to Networks and Network Services	Users must only be provided with access to the networks and networks services that they have been specifically authorized to use.
5.2 User Access Management		
5.2.1	User Registration and De-registration	There must be a formal user registration and de-registration process for granting access to all information systems.
5.2.2	User Access Provisioning	There must be a formal user access provisioning process for assigning or revoking access rights to all information systems.
5.2.3	Management of Privileged Access Rights	The allocation and use of privileged access rights must be restricted and controlled for privileged users.
5.2.4	User Password Management	The issuance of authentication credentials must be controlled through a formal management process.
5.2.5	Review of User Access Rights	Information Owners must formally review user access rights at regular intervals.
5.2.6	Removal or Adjustment of Access Rights	The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

5.3 User Responsibilities		
5.3.1	Password Use	Users must follow the government's standards in the selection and use of passwords.
5.4 System and Application Access Control		
5.4.1	Information Access Restriction	Access to information and information systems functions must be restricted in accordance with the access control policy.
5.4.2	Secure Logon Procedures	Access to information systems and applications must use a secure logon process.
5.4.3	Password Management System	A password management system must be implemented to provide an effective, interactive means of ensuring quality passwords.
5.4.4	Use of Privileged Utility Programs	Use of system utility programs must be restricted and tightly controlled.
5.4.5	Access Control to Program Source Code	Access control must be maintained for program source libraries.

5.1 Business Requirement for Access Control

Objective:
To limit access to government information and information systems.

5.1.1 Access Control Policy

Access to information systems and services must be consistent with business needs and based on security requirements.

The Government of Saskatchewan must control access to information, information systems and business processes. Access must be authorized, managed, monitored and controlled on the basis of business needs and security requirements. Security controls to safeguard the confidentiality, integrity and availability of information and information assets must be implemented.

Access to Government information and information systems must be appropriate for the user's job description and role. It must consider the "need-to-know" and "least privilege" principles. (See the Glossary in Appendix A for an explanation of those terms.) In all cases there must be a method to validate the identification of the user.

The controls and standards described in this Chapter are the minimum requirements that must be applied by Information Owners and Service Owners.

Information Owners and Service Owners must:

- develop, document and implement procedures for the issuance of user IDs and user access rights to information and information systems;
- ensure that access to information and information systems is based on business needs and appropriate for the job responsibilities and role of the user(s);
- segregate the duties of administering access control, e.g., separate access request, access authorization and access administration and assign a business owner/approver for each;

- remove or revoke access rights when required in accordance with Section 5.2.2;
- review user access rights in accordance with Section 5.2.5;
- document the business requirements to exceed the existing access control rules and rights for each user or group of users;
- complete an inventory of business applications and all related information and information systems in accordance with Section 4.1.1; and
- ensure user access rights to each system are documented in accordance with Section 5.4.1.

Users must:

- ensure that computing devices are accessed only by those authorized to do so;
- ensure that computing devices are password-protected in accordance with Section 5.3.1;
- shut down all applications and logoff the network at the end of a shift or when not returning to the work area for an extended period;
- lock unattended computers with a password-protected screensaver or other approved mechanism in accordance with Section 7.2.8; and
- comply with the Information Technology Acceptable Usage Policy in accordance with Section 4.1.3.

5.1.2 Access to Networks and Network Services

Users must only be provided with access to the networks and networks services that they have been specifically authorized to use.

Information Owners and Service Owners must ensure that:

- users are granted access to only those networks required to fulfill their job responsibilities;
- access to networks is authorized in accordance with Section 5.1.1;
- users authenticate to networks in accordance with Section 5.4.2;
- procedures are implemented to protect access to networks and network services;
- access to networks, including remote access, is in accordance with standards published by Information Technology Division; and
- network services are monitored for compliance with this Section and unauthorized access attempts.

5.2 User Access Management

Objective:
To ensure authorized users access appropriate resources and to prevent unauthorized access to systems and services.

5.2.1 User Registration and De-Registration

There must be a formal user registration and de-registration process for granting access to all information systems.

a) Registration

Information Owners must manage access to information assets under their control. They must implement a user registration process which:

- ensures access requests are approved by the supervisor/manager of the user requesting access;
- ensures the reasons for requesting access are consistent with the duties of the user;
- ensures access is approved via the service request fulfillment processes;
- maintains records of access approvals;
- ensures personnel understand the conditions of access and, when appropriate, have signed confidentiality agreements;
- ensures access rights are consistent with the data uses documented in a Privacy Impact Assessment where applicable;
- ensures access is traceable to an identifiable individual or process;
- ensures each user is assigned a single unique user ID for accessing information systems;
- ensures that responsibilities for authorizing access are segregated from granting access;
- restricts access based on pre-defined role permissions; and
- provides secure and separate transmission of the user ID and password.

Enhanced user security screening or background checks must be completed prior to granting access when justified by the value and sensitivity of the asset or the findings of a Threat and Risk Assessment.

b) De-registration

Information Owners must formally assign responsibilities and implement processes to:

- remove access privileges for employees no longer with the organization;
- promptly review access rights whenever a user changes duties and responsibilities;
- promptly review access rights whenever the user's branch or Ministry is involved in significant reorganization;
- review access privileges for employees on extended absence or temporary assignments within ten working days of the change of status;
- remove access privileges for employees terminated for cause concurrent with notification to the individual; and
- periodically check for and remove inactive or redundant user accounts.

5.2.2 User Access Provisioning

There must be a formal user access provisioning process for assigning or revoking access rights to all information systems.

The provisioning process for assigning or revoking access rights granted to user IDs must include:

- obtaining authorization from the Information or Service Owner for the use of that system;
- verifying that the level of access granted is in accordance with Section 5.1;
- verifying that the level of access granted is consistent with the segregation of duties policy (Section 2.1.2) and other requirements;
- ensuring that access rights are not activated before authorization procedures are completed;
- maintaining a central record of access rights granted a user ID;
- adapting access rights of users who have changed roles and immediately removing or blocking access rights of users who have left government (Section 5.2.6); and
- periodically reviewing access rights with Information Owners (Section 5.2.5).

5.2.3 Management of Privileged Access Rights

The allocation and use of privileged access rights must be restricted and controlled for privileged users.

Information Owners and Service Owners must authorize the granting of system privileges. They must:

- identify and document the system privileges associated with each information system or service;
- ensure the process for requesting and approving access to system privileges includes management approval(s) prior to granting of system privileges;
- ensure processes are implemented to remove system privileges from users concurrent with changes in job status (e.g., transfer, promotion, termination);
- limit access to the fewest number of users needed to operate or maintain the system or service;
- ensure the access rights granted are limited to and consistent with the users' job function and responsibilities;
- maintain a record of users granted system privileges;
- ensure use of system privileges is recorded in audit logs that cannot be altered by the privileged user;
- implement processes for ongoing compliance checks of the use of system privileges; and
- regularly review authorizations in place to confirm that access is still needed and that the least number of users needed have access.

Local admin privileges are distinct from privileged access rights and must follow the appropriate process to be granted.

Access Control Standard for Local Admin on Desktops

Requests for local admin privileges must have business justification. Each request must be authorized by the Security Officer for the Ministry.

5.2.4 User Password Management

The issuance of authentication credentials must be controlled through a formal management process.

Service Owners must formally designate individuals who have the authority to issue and reset passwords. They must adhere to the following controls:

- passwords may only be issued to users whose identity has been confirmed prior to issuance;
- individuals with the authority to issue or reset passwords must transmit new passwords to the users in a secure manner (e.g., using approved encryption);
- temporary passwords must be changed on first use;
- users must not be asked to disclose their passwords;
- passwords must never be stored in an unprotected manner (i.e. use approved encryption and/or appropriate physical security); and
- default passwords provided by technology vendors must be changed to one that is compliant with government standards.

5.2.5 Review of User Access Rights

Information Owners must formally review user access rights at regular intervals.

Information Owners must implement processes to regularly review access rights to information and information systems. Access rights must be reviewed:

- at least annually;
- more frequently for privileged users and for systems with the highest sensitivity;
- when a user's status changes due to promotion, demotion, re-assignment, transfer, removal from a user group or other change that impacts that user's need to access information;
- as part of a major re-organization;
- with the introduction of new technology or applications; and
- when the access control procedures are changed.

Review of access rights must include:

- confirmation that access is based on the "need-to-know" and "least privilege" principles;
- review and verification of access control lists; and
- confirmation that changes to access rights are logged and can be audited.

5.2.6 Removal or Adjustment of Access Rights

The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

Information Owners and Service Owners must review access to information systems and information processing facilities when personnel change employment, including:

- when personnel assume new roles and responsibilities,
- during restructuring of positional or organizational roles and responsibilities,
- when personnel begin long-term leave.

Information Owners and Service Owners must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by:

- removing or modifying physical and logical access,
- recovering or revoking access devices, cards and keys.

Information Owners and Service Owners must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes based upon the evaluation of risk factors such as:

- whether the termination or change is initiated by the user or by management,
- the reason for termination,
- the current responsibilities of the user, and
- the value of the assets currently accessible.

When a user terminates or transfers within the organization employee directories and other documentation must be updated to reflect the change.

Stale account reports must be distributed by Service Owners to the appropriate Information Owners on a prescribed schedule.

5.3 User Responsibilities

Objective:
To make users accountable for safeguarding their authentication information.

5.3.1 Password Use

Users must follow the government's standards in the selection and use of passwords.

Users must:

- change temporary passwords at first logon;
- select complex passwords in accordance with the standards described below;
- use a unique password (one that is for government business only and not the same as one that is for personal use);
- change passwords at specified intervals;
- not disclose passwords to anyone else;
- not write down passwords unless they are safeguarded with appropriate and approved physical security;
- not keep an electronic file of passwords unless it is safeguarded with approved encryption;
- change their passwords immediately after a suspected or actual compromise;

Password Standards

Account passwords must, at a minimum:

- have at least eight characters;
- contain characters from at least three of the following categories:
  - English uppercase letters (A – Z);
  - English lowercase letters (a – z);
  - numbers (0 – 9);
  - non-alphanumeric symbols (e.g.: !,#,$,%); and
  - Unicode characters;
- not contain three or more characters from the user's account name.

The password must be changed at least every ninety days. When supported by the operating system password history must be enabled and at least the previous seven passwords must be remembered and not reused. The minimum password age can be any value.

User accounts must be locked after five invalid login attempts. A locked account can be unlocked using the password reset tool or by contacting the Service Desk.

5.4 System and Application Access Control

Objective:
To prevent unauthorized access to systems and applications.

5.4.1 Information Access Restriction

Access to information and information systems functions must be restricted in accordance with the access control policy.

Every information system must have an access control policy that specifies access permissions for information and system functions. Information Owners and Service Owners are responsible for developing and implementing the access control policy for their business applications. The access control policy must specify:

- the information controlled;
- the system functions controlled; and
- the roles authorized to access the resource and what types of access are permitted (e.g. Read, Write, Execute, Delete).

Information system access controls must be configurable so that access permissions can be modified without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy. Access to them must be restricted.

Information that is publicly accessible must be segregated from sensitive information.

5.4.2 Secure Logon Procedures

Access to information systems and applications must use a secure logon process.

Logon processes must be configured to:

- not display details about backend systems prior to successful completion of the logon process;
- display a banner prior to logon warning that the computer must only be accessed by authorized users and that activities are monitored;
- comply with the Password Standards in Section 5.3.1;
- not display passwords in clear text as they are entered;
- validate logon information only on completion of all input data;
- record unsuccessful logon attempts;
- limit the number of unsuccessful logon attempts before locking the account;
- activate a password lock after a maximum of fifteen minutes of inactivity, requiring the user to re-authenticate, where applicable;
- prevent brute force logon attempts;
- not transmit passwords in clear text over a network; and
- information classification will determine the technical requirements for logon configuration processes.

Access Control Standard for Windows Service Accounts

Windows service accounts are required for various services to function on Windows servers providing services to Ministries. As the stability of these accounts impacts the availability of services they may fall outside of the standard account definition. This standard describes the requirements for all Windows service accounts. Accounts that meet the defined service account requirements do not require a Risk Management Decision Item (RMDI) as the risks are known and understood to be the same for all Windows services accounts. The requirements listed below provide a mechanism to ensure that risks associated with deviating from the standard user account and password policies are reduced.

Windows Service Accounts within the Government of Saskatchewan computing environment must meet all of the following requirements:

- the account does not allow interactive logins; end users will not be able to enter the account username and password to access network and domain resources on the government network;
- the account will be used for a specific function;
- the account has a defined account owner who is authorized to request changes related to the service account and is responsible for ensuring the security of the account password;
- the account password is randomly generated and has a minimum of 20 characters including upper and lower letters, numbers and special characters;
- the account password is provided only to the appropriate people at the time of service registration or adding batch processing jobs to the scheduling service and cannot be shared with any unauthorized individuals;
- the password will not expire but must be changed manually every 365 days; this can be done as part of a regular maintenance cycle; reports will identify any service account password that has exceeded the 365 day maximum age and remediation will be required immediately.

Access Control Standard for UNIX Service Accounts

This standard describes the requirements and attributes which will be used to classify a UNIX service account.

UNIX service accounts are required to run services on various UNIX servers. The maintenance and operation of UNIX services often requires execution of commands under the service account. UNIX systems allow for this through the use of `sudo` which eliminates the need for users to directly log into the system with service account credentials by allowing them to run specific commands with the privileges of the service account from their regular user account.
UNIX service accounts which adhere to the attributes and requirements listed below are considered to be compliant with security standards and do not require an RMDI.

The following requirements and attributes are used to define a compliant UNIX service account within the Government of Saskatchewan:

- service daemons must run under a service-specific account and must not be the `root` user nor have a user identifier (UID) of 0 (zero);
    - *There may be instances where a service control command must be executed as the root user, however, the daemon process should not be running as the root user. Access to the root user account via* `sudo` *should be restricted to system administrators only and any commands requiring execution as the root user should be executed by system administrators with the appropriate access.*
- the service account must not allow interactive logins; this can be achieved by ensuring that the default shell for the account is a null shell appropriate for the platform, typically `/bin/false`;
- the encrypted password for the service account must be null or an invalid entry to prevent direct login to the account;
- the service account must not have `sudo` access to other accounts;
- the service account will be set to “password does not expire;” there is no password to change so there is no need for manual password changes;
- an owner for the service account must be defined; the account owner will have the authority to request changes to the account.

sudo Configuration Requirements

Users may be granted access to service accounts through the sudo facility on UNIX systems. The use of sudo to access service accounts ensures that proper audit logging is maintained at all times. A restricted list of commands with the full path will be provided for inclusion in the sudo configuration as the command set for a specific service account. Command sets will be requested by the various functional groups within Information Technology Division and with service providers. Information Security Branch will review requested command sets to ensure that the command set does not include binaries which could be used to execute a shell as the service account as executing a shell would circumvent audit logging.

The ability to access service accounts via sudo may be achieved either by identifying specific users or groups in the config file. If groups are granted sudo access to a service account the group must not be a default system group. Groups should be created with role¬ specific access in mind.

Other Access Considerations

Other means of accessing non-user accounts on UNIX systems may currently be in place. For example, the use of authorized keys for SSH can allow users to access an account remotely through the secure shell or secure FTP. Authorized keys should be configured with a passphrase that meets the current password complexity specification. The use of blank passphrases for authorized keys is prohibited. Exceptions require acceptance of risk via the Risk Management Decision Item process.

Access Control Standard for Group Managed Service Accounts and Managed Service Accounts

Group Managed Service Accounts (GMSAs) are managed domain accounts that provide automatic password management and simplified Service Principal Name (SPN) management. This includes delegation of management to other administrators on individual servers or over multiple servers (i.e. clusters, server farms). When GMSAs are used as service principals, the Windows operating system manages the password for the account instead of relying on the administrator to manage the password.

GMSAs must be used on a go forward basis for new applications and upgrades.

GMSAs are compatible based on the application/function that is using the service account. They will have to be evaluated on a case-by-case basis.

Existing services accounts won't be reviewed unless the application undergoes an upgrade and the opportunity exists to review the service account.

On servers running Windows Server 2012 and newer, GMSAs must be used where the following conditions are true:

- the service account does not require interactive logins to be enabled;
- elevated privileges are not required by the service account;
- the application requiring a service account is certified to support GMSAs.

Managed Service Accounts

On servers running Windows Server 2008 R2 up to Windows Server 2012 managed services accounts (MSAs) must be used where the following conditions are true:

- GMSAs are not supported by the application;
- the service account does not require interactive logins;
- elevated privileges are not required by the service account;
- the application is capable of supporting service accounts using Kerberos encryption types.

Access Control Standard for Authentication Credentials

The purpose of this standard is to prevent unauthorized access to sensitive information. The data classification as determined by a Statement of Sensitivity can help determine the appropriate authentication controls to apply.

Requirements

Requirements are based on the information classification as determined in Section 4.2.1.

Public – Low

This level applies to read-only public data that uses authentication for purposes other than access control, such as to retain user personalization or configuration. This level requires authentication of a single-factor credential with low security requirements.

An electronic credential for the handling of non-sensitive information must use either:

a) a simple password (not required to comply with the Password Standards in Section 5.3.1); or
b) an assertion from another authentication service that uses any credential strength and authentication method and that is deemed by the relying party to be an authoritative and trusted service.

Class C – Medium

This level applies to sensitive information with low injury in the event of a disclosure. This level requires authentication with a single-factor credential.

An electronic credential intended to achieve a medium credential strength must use either:

a) a password that conforms to the Password Standards in Section 5.3.1;
b) an assertion from another authentication service that uses a comparable or higher credential strength and authentication method (Class C to A); or
c) a software- or hardware-based multifactor authentication system approved by Information Technology Division; it may or may not conform to the higher credential strength (Class B or A) standards (e.g. a one-time password device that is not FIPS 140-2 compliant).

Class B – High

Class B data accessed external of the electronic security perimeter requires encryption; internal to the GOS network encryption is not required.

An electronic credential intended to achieve a high credential strength must use either:

a) a cryptographic token that:
    i. uses a key and cryptographic mechanism compliant with FIPS 140-2 Level 1 or higher and that is approved by the Information Technology Division;
    ii. requires either 1) the use of a password or biometric by the individual to activate the cryptographic mechanism or 2) a password in combination with the cryptographic mechanism in the same authentication protocol; and
    iii. follows the Password Standards for any password used;
b) a one-time password device token that:
    i. depends on a symmetric key stored on a personal hardware device that is a cryptographic module compliant with FIPS 140-2 Level 1 or higher;
    ii. permits at least 106 possible password characters; and
    iii. requires the use of a password or biometric by the individual to activate the retrieval or generation of the one-time password;
c) an assertion from another authentication service that uses a Class B or Class A credential strength and authentication method (Class B or A).

Class A – Very High

This level applies to highly sensitive information. It requires multifactor authentication with a cryptographic token.

An electronic credential intended to achieve a very high credential strength must use a hardware-based cryptographic token that:

a) uses a key and cryptographic mechanism stored on a special hardware device validated at FIPS 140-2 Level 1 at a minimum;
b) requires either 1) the use of a password or biometric by the individual to activate the cryptographic mechanism or 2) a password in combination with the cryptographic mechanism in the same authentication protocol; and
c) follows the Password Standard in Section 5.3.1 for any password used.

5.4.3 Password Management System

A password management system must be implemented to provide an effective, interactive means of ensuring quality passwords.

A password management system must be in place. It must:

- enforce the use of individual user IDs and passwords;
- support user selection and change of passwords in compliance with the Government of Saskatchewan Password Standards (5.3.1);
- enforce the change of the temporary password at first logon or a password reset by an administrator;
- enforce password changes at the specified interval including advance notice of expiry;
- maintain a record of previous passwords and prevent re-use;
- not display the password on the screen when being entered;
- store password files separately from application system data;
- include protection from unauthorized access and manipulation; and
- store and transmit passwords in protected (e.g. encrypted) form.

5.4.4 Use of Privileged Utility Programs

Use of system utility programs must be restricted and tightly controlled.

Information Owners and Service Owners must limit the use of system utility programs by:

- defining and documenting authorization levels;
- restricting access to the minimum number of trusted, authorized users;
- periodically reviewing the status of users with permissions to use them;
- ensuring their use maintains segregation of duties;
- requiring a secure logon process;
- ensuring they are identified and their access logged;
- segregating them from application software where possible; and
- removing or disabling unnecessary and obsolete system utilities and software.

5.4.5 Access Control to Program Source Code

Access control must be maintained for program source libraries.

Program source code is code written by programmers which is compiled and linked to create executables. Associated items are designs, specifications, verification and validation plans.

Access to program source code and associated items must be controlled by:

- ensuring that, where possible, program source libraries are not held in production environments;
- establishing procedures for the management of program source code and libraries;
- ensuring that support personnel do not have unrestricted access to program source libraries;
- safeguarding system documentation;
- authorizing the updating of program source libraries and associated items;
- authorizing the issuance of program source code to application developers;
- logging the modification of program source code; and
- ensuring that the maintenance and copying of program source libraries is subject to strict change control procedures in accordance with Section 10.2.2.

Government of Saskatchewan

Information Security Policy

Chapter 6

Cryptography

Chapter 6 – Cryptography		
6.1 Cryptographic Controls		
6.1.1	Policy on the Use of Cryptographic Controls	The use of cryptographic controls must be based on the risk of unauthorized disclosure and the sensitivity of the information or information system that is to be protected.
6.1.2	Key Management	A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls

6.1 Cryptographic Controls

Objective:

To ensure proper and effective use of cryptography to protect the confidentiality and integrity of government information.

6.1.1 Policy on the Use of Cryptographic Controls

The use of cryptographic controls must be based on the risk of unauthorized disclosure and the sensitivity of the information or information system that is to be protected.

The Chief Information Officer provides government direction and leadership in the use of cryptography and the provision of cryptographic services (e.g. user registration services, key management). This is accomplished by:

- establishing policy and providing strategic direction on the use of cryptography;
- settings standards for cryptographic algorithms and key length; and
- approving the use of cryptographic services.

The Director, Information Security Branch, supports the use of cryptography in government by:

- defining and maintaining standards for cryptographic controls; and
- providing technical advice on the use of cryptography.

The cryptographic controls used to safeguard an information system must be based on the sensitivity of the information and include consideration of:

- integrity requirements (e.g. financial payment instructions in excess of a specified amount);
- non-repudiation requirements;
- authentication requirements;
- other security requirements (e.g. proof of origin, receipt or ownership);
- legislation, regulations or policies requiring the use of cryptography;
- restrictions on the export or use of cryptographic products; and
- risks related to long-term storage of electronic information (e.g. recovery of encrypted data, long-term key maintenance).

Government of Saskatchewan Cryptographic Standards

General

Cryptographic modules, cryptographic software and hardware used to safeguard sensitive government information must be validated to FIPS 140-2 standards. (see Glossary for an explanation of FIPS 140-2)

USB Drives

USB drives used to store sensitive government information must be protected against unauthorized access, loss and theft. A device chosen for this purpose must meet the following requirements:

- it uses hardware-based encryption;
- device is Validated to at least FIPS 140-2 Level 2;
- all user-writable drives on the device are fully encrypted;
- the encryption algorithm is AES-256;
- the device must be configured with a complex password that meets the minimum standard described in Section 5.3.1;
- the device must be configured to lockdown and destroy the encryption key after a maximum of ten failed login attempts.

Contact Information Security Branch for current products that meet these requirements and are available to government users through normal procurement channels.

External Hard Drives

External hard drives used to store sensitive government information must be protected against unauthorized access, loss and theft. A device chosen for this purpose must meet the following requirements:

- it uses hardware-based encryption;
- device is Validated to at least FIPS 140-2 Level 2;
- all user-writable drives on the device are fully encrypted;
- the encryption algorithm is AES-256;
- the device must be configured with a complex password that meets the minimum standard described in Section 5.3.1;
- the device must be configured to lockdown and destroy the encryption key after a maximum of ten failed login attempts.

Contact Information Security Branch for the current recommended products that meet these requirements and can be procured through normal channels.

Windows Laptops Hard Drive Encryption

Government laptops are sometimes used outside the security zones of government buildings. The content on their hard drives must be safeguarded against unauthorized access, loss and theft. The following security controls must be applied:

- all drives are safeguarded with full disk encryption;
- the encryption algorithm is AES-256;
- the encryption product used is validated to at least FIPS 140-2 Level 2;
- the user password must be complex and meet the minimum standards in accordance with Section 5.3.1.

Contact Information Security Branch for current products that meet these requirements and can be procured through normal channels.

Secure Shell (SSH) and Secure File Transfer Protocol (SFTP)

SSH is used by system administrators as a means of remotely managing and configuring a variety of hosts. SFTP is based on SSH and is implemented as a means of securely transferring files between hosts. Software solutions must be configured as follows:

- use SSH version 2;
- do not use host-based authentication;
- the LoginGraceTime must be set to a maximum of 120 seconds;
- the use of .rhosts and .shosts user files must be disabled;
- login via root is not permitted if the system is directly accessible via the internet;
- disable logging into accounts with empty passwords;
- the encryption algorithm must be AES with a minimum key length of 256 bits;
- the Message Authentication Code (MAC) must use a hash algorithm with 256 bits or stronger; and
- contact Information Security Branch for a government-authorized login banner.

6.1.2 Key Management

A key management system based on an agreed set of standards, procedures and methods must be used to support the use of cryptographic controls.

The Chief Information Officer is responsible for approving key management standards and processes including:

- selection and length of cryptographic keys;
- generation of keys;
- generation and distribution of public key certificates;
- distribution, storage and periodic updating of keys;
- revocation of keys (e.g. when a user changes role);
- recovery of keys that are lost, corrupted or expired;
- management of keys that may have been compromised;
- archiving keys and the maintenance of key history; and
- allocation of activation/de-activation dates.

Government of Saskatchewan

Information Security Policy

Chapter 7

Physical and Environmental Security

Chapter 7 – Physical and Environmental Security		
7.1 Secure Areas		
7.1.1	Physical Security Perimeter	Government information processing facilities must be protected by a physical security perimeter.
7.1.2	Physical Entry Controls	Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
7.1.3	Securing Offices, Rooms and Facilities	Controls to ensure security of information and information systems located in government offices, rooms and other facilities must be designed, applied and documented.
7.1.4	Protecting Against External and Environmental Threats	Physical protection against natural disasters, malicious attack or accidents must be designed and applied.
7.1.5	Working in Secure Areas	Additional security controls and procedures must be used by personnel when working in secure areas.
7.1.6	Delivery and Loading Areas	Access points such as reception, delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible, isolated from secure areas or offices to avoid unauthorized access.

7.2 Equipment		
7.2.1	Equipment Siting and Protection	Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.
7.2.2	Supporting Utilities	Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.
7.2.3	Cabling Security	Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.
7.2.4	Equipment Maintenance	Equipment must be correctly maintained to help ensure availability and integrity of sensitive information and assets.
7.2.5	Removal of Assets	Government-owned equipment, information and software must not be removed from government premises without prior authorization.
7.2.6	Security of Equipment and Assets Off-premises	Assets must be safeguarded using documented security controls when off-site from government premises.
7.2.7	Secure Disposal or Re-use of Equipment	All data and software must be erased from equipment prior to disposal or re-deployment.
7.2.8	Unattended User Equipment	Users must ensure unattended equipment has appropriate protection.
7.2.9	Clear Desk and Clear Screen Policy	Users must safeguard sensitive information from unauthorized access, loss or damage.

7.1 Secure Areas

Objective:

To prevent unauthorized physical access, damage and interference to the government's information and assets.

7.1.1 Physical Security Perimeter

Government information processing facilities must be protected by a physical security perimeter.

Information Owners must ensure appropriate controls are in place to establish secure areas. Sensitive information and assets must be protected while considering the safety of personnel. Control selection must be supported by a Threat and Risk Assessment.

Controls that must be applied are:

- security perimeters must be clearly defined, and the siting and strength of each of the perimeters must depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
- perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site must be of solid construction and all external doors must be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks, etc.; doors and windows must be locked when unattended and external protection must be considered for windows, particularly at ground level;
- a manned reception area or other means to control physical access to the site or building must be in place; access to sites and buildings must be restricted to authorized personnel only;
- physical barriers must, where applicable, be built to prevent unauthorized physical access and environmental contamination;

- all fire doors on a security perimeter must be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they must operate in accordance with local fire code in a failsafe manner;
- suitable intruder detection systems must be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas must be alarmed at all times; cover must also be provided for other areas, e.g. computer room or communications rooms;
- information processing facilities managed by the organization must be physically separated from those managed by external parties.

A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

Special consideration must be given towards physical access security when the facility houses multiple organizations.

7.1.2 Physical Entry Controls

Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

The following controls must be implemented:

- access to areas where sensitive information is processed or stored must be restricted to authorized personnel only;
- authentication controls , e.g. access control card system, must be used to authorize and validate all access;
- an audit trail of all access must be maintained;
- visitors must be escorted by authorized personnel;
- visitors must only be allowed access for specific and authorized purposes;
- the date and time of entry and departure of visitors must be recorded;
- all employees and other authorized personnel must wear visible identification;
- visitors must be issued badges or tags of a different colour than employees;
- employees must notify security personnel when they encounter unescorted visitors or anyone not wearing visible identification;
- external party support personnel may be granted restricted access only when required; their access must be authorized and monitored; and
- access rights must be regularly reviewed and updated, and revoked when necessary.

7.1.3 Securing Offices, Rooms and Facilities

Controls to ensure security of information and information systems located in government offices, rooms and other facilities must be designed, applied and documented.

Information Owners and Ministry Security Officers must regularly assess the security of areas where sensitive information is processed and/or stored. Controls that may be implemented to reduce associated risks are:

- physical entry controls described in Section 7.1.2;
- ensure sensitive information is stored properly when not in use in accordance with Section 7.2.9; and
- directories that identify the locations of data centres and other areas where sensitive information is stored must not be made public.

7.1.4 Protecting Against External and Environmental Threats

Physical protection against natural disasters, malicious attack or accidents must be designed and applied.

Information Owners, Ministry Security Officers, planners and architects must incorporate – to the extent possible – physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disaster. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to building code and fire regulations:

- combustible or hazardous materials must be stored at a safe distance from the secure area;
- bulk supplies, e.g. stationary, must not be stored in a secure area;
- fallback equipment and backup media must be located at a safe distance to avoid damage from a disaster affecting the main site; and
- environmental alarm systems, fire suppression and firefighting systems must be installed.

7.1.5 Working in Secure Areas

Additional security controls and procedures must be used by personnel when working in secure areas.

Information Owners and Ministry Security Officers must identify and document requirements that apply to personnel who have been authorized to work in secure areas. Authorized personnel must be informed that:

- sensitive information cannot be discussed in a non-secure area;
- sensitive information cannot be disclosed to personnel who do not have a need-to-know;
- no type of photographic, smartphone, video, audio or other recording equipment can be brought into a secure area unless specifically authorized;
- maintenance staff, cleaners and others who require periodic access to the secure area must be screened and their names added to an access list; and
- visitors must be authorized, logged and escorted.

7.1.6 Delivery and Loading Areas

Access points such as reception, delivery and loading areas and other points where unauthorized persons may enter the premises must be controlled and, if possible, isolated from secure areas or offices to avoid unauthorized access.

Information Owners, Ministry Security Officers, planners and architects must ensure that:

- access to a delivery and loading area from outside of the building must be restricted to identified and authorized personnel;
- the delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
- the external doors of a delivery and loading area must be secured when the internal doors are opened;
- loading docks and delivery areas must be regularly inspected and actively monitored;
- incoming material must be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;
- incoming material must be registered in accordance with asset management procedures (Section 4.1.1) on entry to the site; and
- incoming and outgoing shipments must be physically segregated where possible.

7.2 Equipment

Objective:

To prevent loss, damage, theft or compromise of assets and interruption to the government's operations.

7.2.1 Equipment Siting and Protection

Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.

Information Owners, Ministry Security Officers, planners and architects must ensure that Government facilities are designed in a way that safeguards sensitive information and assets.

Servers, routers, switches and other centralized computing equipment must be located in a room with access restricted to only those personnel who require it.

Workstations, laptops, digital media and storage devices must be located and used in an area that is not accessible to the public.

Equipment must be located, and monitors angled, in such a way that unauthorized persons cannot observe the display.

Shared printers, scanners, copiers and fax machines cannot be located in an area that is accessible to the public.

Kiosks and other devices that are intended for public use must be clearly labelled and placed in a publicly accessible area.

7.2.2 Supporting Utilities

Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.

The following controls must be implemented to help ensure availability of critical services.

All supporting utilities such as electricity, water supply, sewage, heating/ventilation and air conditioning must be adequate for the systems they are supporting. Support utilities must be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply must be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans must cover the action to be taken on failure of the UPS. A back-up generator must be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel must be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators must be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large, a separate power substation.

Emergency power off switches must be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting must be provided in case of main power failure.

The water supply must be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. An alarm system to detect malfunctions in the supporting utilities must be evaluated and installed if required.

Telecommunications equipment must be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services must be adequate to meet local legal requirements for emergency communications.

7.2.3 Cabling Security

Power and telecommunications cabling carrying data or supporting information services must be protected from interception or damage.

Power and telecommunications lines into information processing facilities must be underground, where possible, or subject to adequate alternative protection.

When identified in a Threat and Risk Assessment, network cabling must be protected from unauthorized interception or damage by using a conduit and by avoiding routes through public areas.

Power cables must be segregated from communications cables to prevent interference.

Cables and equipment must be clearly marked to minimize handling errors such as accidental patching of wrong network cables. A documented patch list must be used to reduce the possibility of errors.

When a Threat and Risk Assessment finds a need for more safeguards, consider:

- installation of rigid conduit and locked rooms or boxes at inspection and termination points;
- use of alternative routings and/or transmission media providing appropriate security;
- use of fibre optic cabling;
- use of electromagnetic shielding to protect the cables;
- initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables; and
- controlled access to patch panels and cable rooms.

7.2.4 Equipment Maintenance

Equipment must be correctly maintained to help ensure availability and integrity of sensitive information and assets.

When equipment is serviced Information Owners must consider the sensitivity of the information it holds and the value of the assets. The following controls must be applied:

- equipment must be maintained in accordance with the supplier's recommended schedule and specifications;
- only authorized maintenance personnel may carry out repairs and service equipment;
- records must be kept of all suspected faults and all preventive and corrective maintenance;
- maintenance must be scheduled at a time of day that limits interference with services or operations;
- users must be notified before equipment is taken off-line for maintenance;

If off-site maintenance is required then the asset must be cleared of all sensitive information. If it's not possible to de-sensitize assets before sending for maintenance then the Ministry Security Officer and Information Owner must consider destruction of the asset.

7.2.5 Removal of Assets

Government-owned equipment, information and software must not be removed from government premises without prior authorization.

Information Owners must establish a formal authorization process for the removal of assets for re-location, loan, maintenance, disposal or any other purpose. Authorization must include:

- item description and serial number(s);
- information indicating where the asset will be located;
- the removal date and return date;
- the name of the individual responsible for the asset; and
- the reason for removal.

The description and serial numbers must be verified when the asset is returned.

Personnel must be informed of and accept responsibility for protection of the asset.

7.2.6 Security of Equipment and Assets Off-Premises

Assets must be safeguarded using documented security controls when off-site from government premises.

Information Owners must ensure that equipment used or stored off-site is safeguarded in accordance with the sensitivity of the information and the value of the assets. Controls to apply include:

- encrypt sensitive data when determined by a Threat and Risk Assessment;
- use a logical or physical access control mechanism (BIOS password, USB key, smart card) to protect against unauthorized access;
- use a physical locking or similar mechanism to restrain the equipment;
- ensure personnel are instructed on the proper use of the chosen controls.

Personnel in possession of government equipment:

- must not leave it unattended in a public place;
- must ensure the equipment is under his/her direct control at all times when traveling;
- must take measure to prevent viewing of sensitive information by unauthorized personnel;
- must not allow other persons to use the equipment;
- must report loss or stolen equipment immediately.

7.2.7 Secure Disposal or Re-Use of Equipment

All data and software must be erased from equipment prior to disposal or re-deployment.

Information owners must consider the sensitivity of information and the value of the assets when determining whether or not hardware or media will be re-used or destroyed.

Prior to re-use within government:

- the integrity of government records must be maintained by adhering to Records Management policies (see Section 14.1.3);
- information and software are must be backed up by the original Information Owner; and
- the storage media must be wiped in accordance with Section 4.3.2.

Storage media that will no longer be used in government must be wiped by a method approved by the Director, Information Security Branch, in compliance with Section 4.3.2. Asset inventories must be updated to record details of the data wiping including:

- asset identifier;
- date of erasure;
- names of personnel conducting the erasure.

When a supplier conducts the data wiping there must be contractual and audit procedures to ensure complete destruction of the information. The government must receive certification that the destruction has occurred.

7.2.8 Unattended User Equipment

Users must ensure unattended equipment has appropriate protection.

User must safeguard unattended equipment by:

- terminating the active session when finished;
- lock the session with a password protected screen saver or other approved mechanism;
- logoff computers, servers, mainframes and other devices when the session is finished;
- enabling password protection on mobile devices and portable storage devices; and
- secure devices with a cable lock when enhanced physical security is justified.

7.2.9 Clear Desk and Clear Screen Policy

Users must safeguard sensitive information from unauthorized access, loss or damage.

Users must secure their work space when it cannot be monitored by authorized personnel. Secure work spaces by:

- clearing desktops and work areas;
- locking hard copy sensitive information in an appropriate cabinet;
- locking portable storage devices with sensitive information in an appropriate cabinet;
- activating a password-protected screen saver;
- safeguarding incoming and outgoing mail;
- retrieving documents from printers and fax machines; and
- ensuring that sensitive hard copy documents no longer needed are placed in shredding bins, not recycle bins.

When visitors, cleaning staff or other personnel without a “need-to-know” are in the area, safeguard sensitive information by:

- covering up and maintaining control of hard copy files;
- blanking computer screens or activating the password-protected screen saver.

Sensitive information must not be discussed in public or other areas where there is a risk of being overheard by unauthorized personnel.

Government of Saskatchewan

Information Security Policy

Chapter 8

Operations Security

Chapter 8 – Operations Security		
8.1 Operational Procedures and Responsibilities		
8.1.1	Documented Operating Procedures	Operating procedures and responsibilities for information systems must be authorized, documented and maintained.
8.1.2	Change Management	Changes to business processes and information systems that affect information security must be controlled.
8.1.3	Capacity Management	The use of information system resources must be monitored and optimized with projections made of future capacity requirements.
8.1.4	Separation of Development, Testing and Operational Environments	Development, testing and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment.
8.2 Protection from Malware		
8.2.1	Controls Again Malware	Detection, prevention and recovery controls – supported by user awareness procedures – must be implemented to protect against malware.
8.3 Backup		
8.3.1	Information Backup	Backup copies of Information, software and system images must be made, secured and be available for recovery.

8.4 Logging and Monitoring		
8.4.1	Event Logging	Event logs recording user activities, exceptions, faults and information security events must be produced, kept and regularly reviewed.
8.4.2	Protection of Log Information	Information system logging facilities and log information must be protected against tampering and unauthorized access.
8.4.3	Administrator and Operator Logs	Activities of privileged users must be logged and the log subject to regular independent review.
8.4.4	Clock Synchronization	Computer clocks must be synchronized for accurate recording.
8.5 Control of Operational Software		
8.5.1	Installation of Software on Operational Systems	The installation of software on operational information systems must be controlled.
8.6 Technical Vulnerability Management		
8.6.1	Management of Technical Vulnerabilities	Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risk.
8.6.2	Restrictions on Software Installation	Rules governing the installation of software by users must be established and implemented.
8.7 Information Systems Audit Considerations		
8.7.1	Information Systems Audit Controls	Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.

8.1 Operational Procedures and Responsibilities

Objective:

To ensure correct and secure operations of information systems.

8.1.1 Documented Operation Procedures

Operating procedures and responsibilities for information systems must be authorized, documented and maintained.

Information Owners and Service Owners must ensure that operating procedures and standards are:

- documented;
- approved by the appropriate authority;
- consistent with government policies;
- reviewed and updated periodically;
- reviewed and updated when there are changes to equipment/systems or changes in business services and the supporting information systems operations; and
- reviewed and updated following a related security incident investigation.

The documentation must contain detailed instructions regarding:

- information processing and handling;
- system re-start and recovery;
- backup and recovery including on-site and off-site storage;
- exceptions handling, including a log of exceptions;
- output and media handling, including secure disposal or destruction;
- audit and system log management;
- change management including scheduled maintenance and interdependencies;
- computer room management and safety;
- Information Incident Management Process;
- Disaster Recovery;
- Business Continuity Plan; and
- contact information for operations, technical, emergency and business personnel.

8.1.2 Change Management

Changes to business processes and information systems that affect information security must be controlled.

Information Owners and Service Owners must document and implement a change management process. Changes must be controlled by:

- identifying and recording significant changes;
- assessing the potential impact, including that on security, of the changes;
- obtaining approval of changes from those responsible for the information system;
- planning and testing changes including the documentation of fallback procedures;
- communicating change details to relevant personnel; and
- evaluating that planned changes were implemented as intended.

Information Owners and Service Owners must plan for changes by:

- assessing the potential impact of the proposed change on security by conducting either a security review or a Threat and Risk Assessment, depending on the size of the change;
- identifying the impact on agreements with business partners and external parties including information sharing agreements, Memoranda of Understanding, licensing and provision of services;
- determining if re-certification or re-accreditation of the information system is required;
- preparing change implementation plans that include testing and contingency plans in the event of problems;
- obtaining approvals from affected Information Owners; and
- training technical and operational staff as necessary;

Information Owners and Service Owners must implement changes by:

- notifying affected internal parties, business partners and external parties;
- completing re-certification or re-accreditation prior to implementation;
- training users if necessary;
- documenting the process throughout the testing and implementation phases; and
- confirming the changes have been performed and no unintended changes took place.

8.1.3 Capacity Management

The use of information system resources must be monitored and optimized with projections made of future capacity requirements.

Information Owners and Service Owners are responsible for implementing capacity management processes by:

- documenting capacity requirements and capacity planning processes;
- including capacity requirements in service agreements; and
- monitoring and optimizing information systems to detect impending capacity limit.

Information Owners and Service Owners must project future capacity requirements based on:

- new business and information systems requirements;
- statistical or historical capacity requirements; and
- current and expected trends in information processing capabilities (e.g. introduction of more efficient hardware or software).

Information Owners and Service Owners must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a treat to system security or services.

8.1.4 Separation of Development, Testing and Operational Environments

Development, testing and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment.

Information Owners and Service Owners must:

- separate operational environments from test and development environments by using different servers, domains and partitions;
- ensure that production servers do not host test or development services or applications;
- prevent the use of test and development identities as credentials for operational systems;
- store source code in a secure location away from the operational environment and restrict access to specified personnel;
- prevent access to compilers, editors and other tools from operational systems;
- use approved change management processes for promoting software from development/test to operational;
- prohibit the use of operational data in development, test or training systems; and
- prohibit the use of sensitive information in development, test or training systems in accordance with Section 10.3.1.

8.2 Protection from Malware

Objective:

To ensure that information systems are protected against malware.

8.2.1 Controls Against Malware

Detection, prevention and recovery controls – supported by user awareness procedures – must be implemented to protect against malware.

Information Owners and Service Owners must protect government information systems from malicious code by:

- installing, updating and using software designed to scan, detect, isolate and delete malicious code;
- prohibiting the use of unauthorized software;
- checking files, email attachments and file downloads for malicious code before use;
- maintaining business continuity plans to recover from malicious code incidents;
- maintain a critical incident management plan to identify and respond to malicious code incidents;
- maintaining a register of specific malicious code countermeasures (e.g. blocked websites, blocked file extensions, blocked network ports) including a description, rationale, approval authority and the date applied; and
- developing user awareness programs for malicious code countermeasures.

Ministry Security Officers are responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

8.3 Backup

Objective:
To protect against loss of data.

8.3.1 Information Backup

Backup copies of information, software and system images must be made, secured, and be available for recovery.

Information Owners and Service Owners must define and document backup and recovery processes that consider the confidentiality, integrity and availability requirements of information and information systems.

Backup and recovery processes must comply with:

- Ministry business continuity plans (if applicable);
- policy, legislative, regulatory and other obligations; and
- records management requirements (Section 14.1.3).

The documentation for backup and recovery must include:

- types of information to be backed up;
- schedules for the backup of information and information systems;
- backup media management;
- methods for performing, validating and labeling backups; and
- methods for validating the recovery of information and information systems.

Backup media and facilities must be appropriately secured based on a security review or Threat and Risk Assessment. Controls to be applied include:

- use approved encryption;
- physical security;
- access controls;
- methods of transit to and from off-site locations;
- appropriate environmental conditions while in storage; and
- off-site locations must be at a sufficient distance to escape damage from an event at the main site.

8.4 Logging and Monitoring

Objective:
To log events and monitor compliance.

8.4.1 Event Logging

Event logs recording user activities, exceptions, faults and information security events must be produced, kept and regularly reviewed.

Information Owners must ensure that event logs are used to record user and system activities, exceptions and events (security and operational). The degree of detail to be logged must be based on the value and sensitivity of the information and the criticality of the system. The resources required to analyze the logs must also be considered. Where applicable, event logs must include:

- user ID;
- system activities;
- dates, times and details of key events (e.g. logon, logoff);
- device identity and location;
- logon method;
- records of successful and unsuccessful system access attempts;
- records of successful and unsuccessful data and other resource access attempts;
- changes to system configuration;
- use of elevated privileges;
- use of system utilities and applications;
- network addresses and protocols;
- alarms raised by the access control system;
- activation and de-activation of protection systems (e.g. anti-virus, intrusion detection); and
- records of transactions executed by users in applications.

Event logs may contain sensitive information and therefore must be safeguarded in accordance with Section 8.4.2.

System administrators must not have the ability to modify, erase or de-activate logs of their own activities.

If event logging is disabled the decision must be documented. Include the name and position of the approver, date and rationale for de-activating the log. When applicable update the Privacy Impact Assessment and Threat and Risk Assessment to reflect this decision.

Event logs may be configured to alert someone if certain events or signatures are detected. Information Owners must establish and document alarm response procedures in accordance with Section 12.1.2 to ensure they are responded to immediately and consistently. Normally, response to an alarm will include:

- identification of the event;
- isolation of the event and affected assets;
- identification and isolation of the source;
- corrective action;
- forensic analysis;
- action to prevent recurrence; and
- securing of event logs as evidence.

8.4.2 Protection of Log Information

Information system logging facilities and log information must be protected against tampering and unauthorized access.

Information Owners must implement controls to protect logging facilities and log files from unauthorized modification, access or destruction. Controls must include:

- physical security safeguards;
- permission for administrators and operators to erase or de-activate logs;
- multifactor authentication for access to sensitive records;
- backup of audit logs to off-site facilities;
- automatic archiving of logs to remain within storage capacity; and
- scheduling the audit logs as part of the records management process.

Event logs must be retained in accordance with the records retention schedule for the information system. Retain them indefinitely if an investigation has commenced or it is known that evidence may be obtained from them (see Section 12.1.7).

8.4.3 Administrator and Operator Logs

Activities of privileged users must be logged and the log subject to regular independent review.

The activities of system administrators, operators and other privileged user must be logged including:

- the time an event (e.g. success or failure) occurred;
- event details including files accessed, modified or deleted, errors and corrective action taken;
- the account and the identity of the privileged user involved; and
- the systems processes involved.

Logs of the activities of privileged users must be checked by the Information Owner or delegate. Checks must be conducted regularly and randomly. The frequency must be determined by the value and sensitivity of the information and criticality of the system. Following verification of the logs they must be archived in accordance with the applicable records retention schedule.

8.4.4 Clock Synchronization

Computer clocks must be synchronized for accurate recording.

System administrators must synchronize information system clocks to the local router gateway or a government approved host.

System administrators must confirm system clock synchronization following power outages and as part of incident analysis and event log review.

8.5 Control of Operational Software

Objective:
To ensure the integrity of operational systems.

8.5.1 Installation of Software on Operational Systems

The installation of software on operational information systems must be controlled.

To minimize the risk of damage to operational systems Information Owners must implement the following procedures when installing software:

- updates of operational systems must be planned, approved, assessed for impacts, tested and logged;
- a release manager must be appointed to coordinate the install and update of software, applications and program libraries;
- operations personnel and end users must be notified of the changes, potential impacts and, if required, given additional training;
- production systems must not contain development code or compilers;
- user acceptance testing must be extensively and successfully conducted on a separate system prior to production implementation;
- a rollback strategy must be in place and previous versions of application software retained;
- old software versions must be archived with configuration details and system documentation; and
- updates to program libraries must be logged.

8.6 Technical Vulnerability Management

Objective:
To prevent exploitation of technical vulnerabilities.

8.6.1 Management of Technical Vulnerabilities

Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risk.

To support technical vulnerability management, Information Owners and Service Owners must maintain an inventory of information assets in accordance with Section 4.1.1. Specific information must be recorded including:

- the software vendor;
- version numbers;
- current state of deployment; and
- the person(s) responsible for the system.

Vulnerabilities which impact government information systems must be addressed in a timely manner to mitigate or minimize the impact on government operations. Service Owners must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- monitoring external sources of information on published vulnerabilities;
- assessing the risk of published vulnerabilities;
- testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- applying corrective measures to address the vulnerabilities; and,
- reporting to the Director, Information Security Branch, on progress in responding to vulnerabilities.

Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the change management controls (Section 8.1.2) or by following the information security incident response procedures (Chapter 12).

Responsibilities for vulnerability response must be included in service agreements with suppliers.

8.6.2 Restrictions on Software Installation

Rules governing the installation of software by users must be established and implemented.

Users are not allowed to install software on government devices unless specifically authorized by a Service Owner or a system administrator.

Service Owners are responsible for the installation of software, updates and patches.

8.7 Information Systems Audit Considerations

Objective:
To minimize the impact of audit activities on operational systems.

8.7.1 Information Systems Audit Controls

Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.

Prior to commencing compliance checking activities such as audits or security reviews of operational systems the Director, Information Security Branch, and the Information Owner must define, document and approve the activities. Among the items upon which they must agree are:

- the audit requirements and scope of the checks;
- audit personnel must be independent of the activities being audited;
- the checks must be limited to read-only access to software and data, except for isolated copies of system files, which must be erased or given appropriate protection if required when the audit is complete;
- the resources performing the checks must be explicitly identified;
- existing security metrics will be used where possible;
- all access must be monitored and logged and all procedures, requirements and responsibilities must be documented;
- audit tests that could affect system availability must be run outside business hours; and
- appropriate personnel must be notified in advance in order to be able to respond to any incidents resulting from the audit.

Government of Saskatchewan

Information Security Policy

Chapter 9

Communications and Network Security

Chapter 9 – Communications and Network Security		
9.1 Network Security Management		
9.1.1	Network Controls	A range of controls must be implemented to achieve and maintain security within the government network.
9.1.2	Security of Network Services	Security mechanisms, service levels and management requirements of all network services must be documented and included in any network service agreement.
9.1.3	Segregation in Networks	Groups of information services, users and information systems must be segregated on networks.
9.2 Information Transfer		
9.2.1	Information Transfer Policies and Procedures	Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services.
9.2.2	Agreements on Information Transfer	Agreements must address the secure transfer of business information between the government and external parties.
9.2.3	Electronic Messaging	Information transmitted by electronic messaging must be appropriately protected.
9.2.4	Confidentiality or Non-disclosure Agreements	Requirements for confidentiality or non-disclosure agreements reflecting the government's needs for the protection of information must be identified, documented and regularly reviewed.

9.1 Network Security Management

Objective:

To ensure the protection of information in networks and its supporting information processing facilities.

9.1.1 Network Controls

A range of controls must be implemented to achieve and maintain security within the government network.

Service Owners must implement a governance framework that monitors and increases the security posture of the government's networks.

a) Control and Management of Networks

Service Owners must implement network infrastructure security controls and security management systems for networks to ensure the safeguarding of information and information systems. Controls must be selected based on a Threat and Risk Assessment. Assets to be considered include:

- information in transit;
- network infrastructure;
- device configuration, access control definitions, routing information, cryptographic keys;
- network management information;
- network pathways and routes;
- network resources such as bandwidth;
- network security boundaries and perimeters; and
- information system interfaces.

b) Configuration Control

Service Owners must manage and control changes to network device configuration information such as configuration data, access control definitions, routing information and passwords. Network device configuration data must be protected from unauthorized access, modification, misuse or loss by the use of the following controls:

- encryption;
- access control and multifactor authentication;
- configuration change logs;
- baseline configuration protected by cryptographic checksums;
- configuration ports are to be disabled if not required;
- regular backups; and
- performing status accounting to ensure that configuration baselines reflect actual device configuration.

c) Trusted Path

Depending on the data classification, information must be transmitted using a trusted path with the following controls:

- data, message or session encryption in accordance with access controls standards in Chapter 5; and
- a means to detect tampering.

d) Wireless Local Area Networking

Wireless networks must:

- be authorized by Information Technology Division;
- use strong link-layer encryption such as Wi-Fi Protected Access 2;
- ensure that user and device network access are controlled by government authentication services; and
- use strong, frequently changed, automatically expiring encryption keys and passwords.

e) Equipment Management

Service Owners and suppliers must document responsibilities and procedures for operational management of network infrastructure including devices at network boundaries and in user areas.

f) Monitoring, Logging and Detection

Centralized log management must be enabled including logging of:

- traffic traversing network security boundaries;
- traffic within networks housing sensitive or mission critical systems or information;
- security events on network devices such as operator login and configuration changes; and
- security events on systems that provide authentication and authorization services to network infrastructure devices (e.g. routers, firewalls, switches).

Logs must be continuously monitored to enable detection and response to security events and intrusions (e.g. automation of log monitoring and alerting).

Devices with the technical capability of remote logging capability (such as syslog or snmp) are to log access requests to the configuration port.

Service Owners must ensure there is a clear segregation of duties for personnel involved in logging, monitoring and detection activities.

Network discovery tools must be used to monitor and identify unauthorized systems connected to the network.

Active automated surveillance of networks must be implemented to detect and report on security events (e.g. network intrusion).

Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems.

g) Egress Filtering

To prevent interruptions to Ministries' services caused by unauthorized malicious traffic exiting the partnership network, Service Owners must ensure that:

- egress filtering is enabled;
- egress filtering procedures are reviewed when necessary and adjusted to meet current security best practices; and
- every firewall has a "default deny" rule in use and the principle of least privilege is followed.

9.1.2 Security of Network Services

Security mechanisms, service levels and management requirements of all network services must be documented and included in any network service agreement.

Formal network service agreements must be established with network service providers. The agreements must specify services offered, service levels, security requirements and security features of network services. They must also specify:

- the schedule for ongoing verification of network security controls;
- the rights of either party to monitor, audit or investigate as needed;
- security incident response, contacts and procedures; and
- the requirement to meet or exceed baseline government security policies and standards.

Service Owners must confirm that specified security features are enabled prior to commencement of service delivery.

9.1.3 Segregation in Networks

Groups of information services, users and information systems must be segregated on networks.

Service Owners must segregate services, users and information systems to support business requirements, connectivity and access control. The segregation must be based on the management of risk, the segregation of duties and the principle of "least privilege."

Service Owners must establish network perimeters and control traffic flow between networks. Network traffic flow control points such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers must be implemented at multiple points throughout the network to provide the required level of control.

Techniques and technologies selected for network segregation must be based on the findings of a Threat and Risk Assessment. Factors to consider include:

- the sensitivity of the information and system;
- the trustworthiness of the network as revealed by the amount of uncontrolled malicious traffic, the level of device identification and authentication, and the sensitivity to eavesdropping;
- transparency, usability and management costs of network segregation technologies;
- privileged networks (networks with unrestricted or a higher level of access to other networks) must be on a separate network segment physically separated by a firewall; and
- the availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

9.2 Information Transfer

Objective:
To maintain the security of information transferred within an organization and with any external entity.

9.2.1 Information Transfer Policies and Procedures

Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services.

Users of electronic communication services must comply with the following policies:

- Information Technology Acceptable Usage Policy (Section 4.1.3);
- Electronic Messaging (Section 9.2.3); and
- Protection of Records (Section 14.1.3).

User must not forward sensitive government communications outside the government network unless there is a “need-to-know” by the intended recipient.

Users must not forward sensitive government information or communications to externally hosted storage (e.g. cloud storage facilities such as Google Drive) for any reason.

The auto-forwarding of internal email to external addresses is not permitted.

Employees must:

- take appropriate precautions when discussing sensitive information in a telephone call; and
- not leave sensitive information in voice mail or an answering machine.

Wireless communications must be safeguarded in accordance with Section 9.1.1.

Information Owners and Service Owners must implement the following controls to further safeguard electronic communications:

- protecting information from interception, copying, modification, mis-routing and destruction;
- in accordance with Section 8.2.1 protection against malware that may be transmitted through the use of electronic communication services;
- protecting sensitive information that is in the form of an attachment; and
- encrypting information to protect the confidentiality and integrity.

9.2.2 Agreements on Information Transfer

Agreements must address the secure transfer of business information between the government and external parties.

Information Owners and Service Owners must ensure the terms and conditions for exchanging information assets with external parties are documented in an agreement. The agreement must define:

- accountability for custody and control;
- authority to publish, grant access to or re-distribute the information;
- purpose and authorized use(s) of the information and software;
- limitations on data linkage;
- duration, renewal and termination provisions;
- primary contacts for agreement, governance and management;
- an agreed labelling system that properly interprets the classification levels of the various parties (see Section 4.2.2);
- safeguarding information in accordance with its classification level;
- requirements for handling information (e.g. recording recipients, confirming receipt, reviewing records);
- media management and destruction procedures;
- technical standards for transmission, recording or reading information or software;
- reporting requirements following from security and privacy incidents and breaches;
- liability, accountability and mitigation strategies following from incidents and breaches;
- problem resolution and escalation processes.

Information or software covered by and exchange agreement must be subjected to a Privacy Impact Assessment and a Threat and Risk Assessment.

9.2.3 Electronic Messaging

Information transmitted by electronic messaging must be appropriately protected.

The Service Owner must approve implementation of, and modifications to, electronic messaging systems.

To safeguard the integrity of government messages, the electronic messaging services must have a means of:

- protecting messages from unauthorized access, modification or denial of service;
- ensuring correct addressing and transportation of messages;
- providing reliable and available messaging infrastructure; and
- conforming with legislative and regulatory requirements.

Users must:

- use only government electronic messaging services;
- use authorized systems for remote access to government messaging systems;
- use only authorized encryption for email or attachments when required; and
- safeguard sensitive information transmitted via electronic messaging in the same way one safeguards other formats.

Email and other electronic messages may qualify as government records and thus subject to The Archives and Public Records Management Act and other legislation and policies. For guidance, refer to the Provincial Archives of Saskatchewan.

Government email is automatically archived. For more information see:

http://www.employeeservices.gov.sk.ca/autoarchiving

9.2.4 Confidentiality or Non-disclosure Agreements

Requirements for confidentiality or non-disclosure agreements reflecting the government's needs for the protection of information must be identified, documented and regularly reviewed.

In accordance with Human Resources policies all employees of executive government must sign the Oath or Declaration of Office. The oath includes a statement that the employee will not disclose sensitive government information.

Individuals other than employees must accept and sign an agreement to not disclose sensitive government information. The agreement must contain:

- a description of the information to be protected;
- expected duration of the agreement;
- required actions when the agreement is terminated;
- responsibilities and actions of signatories to avoid unauthorized disclosure of sensitive information;
- the permitted use of sensitive information and the rights of the signatory to use it;
- the right of the Government to audit and monitor activities;
- the process for notification and reporting of unauthorized disclosure or other potential breaches;
- terms for information to be returned or destroyed when the agreement is terminated; and
- expected actions to be taken in case of a breach of the agreement.

Government of Saskatchewan

Information Security Policy

Chapter 10

System Acquisition, Development and Maintenance

Chapter 10 – System Acquisition, Development and Maintenance		
10.1 Security Requirements of Information Systems		
10.1.1	Information Security Requirements Analysis and Specification	Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.
10.1.2	Security Application Services on Public Networks	Information in application services on public networks must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.
10.1.3	Protecting Application Services Transactions	Information systems that involve on-line transactions must have security controls commensurate with the value and level of sensitivity of the information.
10.2 Security in Development and Support Processes		
10.2.1	Secure Development Policy	Rules for the development of software and systems must be established and applied to developments within government.
10.2.2	System Change Control Procedures	Changes to software must be controlled by the use of formal change control procedures.
10.2.3	Technical Review of Applications After Operating Platform Changes	Information systems must be reviewed and tested when operating system changes occur.
10.2.4	Restrictions on Changes to Software Packages	Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.
10.2.5	Secure System Engineering Principles	Principles for engineering secure systems must be established, documented, maintained and applied to any information system implementation efforts.

10.2.6	Secure Development Environment	Secure development environments for system development and integration efforts must be established and appropriately protected throughout the entire system development lifecycle.
10.2.7	Outsourced Development	Controls must be applied to secure outsourced information system development.
10.2.8	System Security Testing	Testing of security functionality must be carried out during development.
10.2.9	System Acceptance Testing	Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions.
10.3 Test Data		
10.3.1	Protection of Test Data	Test data must be protected and controlled using the same procedures as those in operational systems.

10.1 Security Requirements of Information Systems

Objective:

To ensure that security is an integral part of information systems across their entire lifecycle, including those that provide services over public networks.

10.1.1 Information Security Requirements Analysis and Specification

Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

When developing, acquiring or making major changes to an information system, Information Owners and Service Owners must:

- prepare a Statement of Sensitivity to determine the confidentiality, integrity and availability requirements of the system
- apply security controls based on a Threat and Risk Assessment;
- document the roles and responsibilities related to information system security management;
- document specific procedures and standards used to mitigate risks and safeguard the information systems; and
- document communication procedures for security-related events and incidents.

10.1.2 Securing Application Services on Public Networks

Information in application services on public networks must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.

Prior to implementing an information system that involves electronic commerce, Information Owners must:

- conduct the information security requirements analysis described in Section 10.1.1;
- ensure that user notification and acceptance of terms and conditions of use complies with government policies and standards; and
- ensure that multifactor authentication is used where applicable based on the data classification.

Ministries should consider including applications on public networks in their Business Continuity Planning.

10.1.3 Protecting Application Services Transactions

Information systems that involve on-line transactions must have security controls commensurate with the value and level of sensitivity of the information.

Information Owners and Service Owners must ensure that security controls are implemented to prevent incomplete transmission, mis-routing, repudiation of transaction, unauthorized message duplication and replay. Controls to consider include:

- validating and verifying user credentials;
- digital signatures and encryption;
- secure communication protocols; and
- storing online transaction details on servers within the appropriate network security zone.

Information Owners and Service Owners must ensure that information systems used for processing payment card transactions or connected to payment card transaction processing systems comply with the Payment Card Industry (PCI) Data Security Standard as published by the PCI Security Standards Council.

Information Owners and Service Owners must contact Information Security Branch before initiating any project that involves payment card transactions.

10.2 Security in Development and Support Processes

Objective:

To ensure that information security is designed and implemented within the system development lifecycle.

10.2.1 Secure Development Policy

Rules for the development of software and systems must be established and applied to developments within government.

Secure development is a requirement to build and support a secure service, architecture, software and system. Information Owners and Service Owners must consider:

- security of the development environment;
- guidance on security in the software development lifecycle including methodology and secure coding guidelines;
- security requirements in the design phase;
- security checkpoints within the project milestones;
- secure repositories;
- security in version control;
- required security application knowledge; and
- developers' capability for avoiding, finding and fixing vulnerabilities.

Secure programming techniques must be used for both new developments and code re-use scenarios.

10.2.2 System Change Control Procedures

Changes to software must be controlled by the use of formal change control procedures.

To help ensure that information systems are not compromised by unauthorized changes to software, the following controls must be applied.

When introducing new systems and major changes to existing systems, Information Owners and Service Owners must follow a formal change control process that includes:

- documentation;
- specification;
- testing;
- quality control;
- approval; and
- a managed implementation.

The change control process must also include:

- an analysis of the impacts of the change;
- specifications of security controls;
- ensuring that existing security controls are not compromised;
- ensuring that application developers can only access required program source code libraries in accordance with Section 5.4.5; and
- obtaining a formal agreement and approval for the change.

The following processes must also be included:

- records of agreed authorization levels;
- change requests must be received from authorized users;
- annual reviews of change controls and integrity procedures;
- identification of all software, information, database entities and hardware that require amendment;
- accepting changes by authorized personnel prior to implementation;
- updating and archiving system, operational and user documentation;
- maintaining version control; and
- change requests logging.

Application and operational change control procedures must be integrated when practicable.

New software, including patches, service packs and other updates, must be tested in an environment that is segregated from the development and production environments. Automated updates will not be used on critical systems.

10.2.3 Technical Review of Applications after Operating System Changes

Information systems must be reviewed and tested when operating system changes occur.

To help ensure that information systems will not be disrupted or compromised, Information Owners and Service Owners must implement the following processes:

- a technical review of application control and integrity procedures which tests the impact of operating system changes on business critical applications;
- timely notification to allow appropriate tests and reviews before implementation; and
- assigning responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes to a specific group or individual.

10.2.4 Restrictions on Changes to Software Packages

Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.

A software update management process must be maintained for commercial-off-the-shelf (COTS) software. This is intended to ensure that:

- up to date and approved patches have been applied; and
- the version of software in use is supported by the vendor.

Other than patches supplied by the vendor, commercial off the shelf (COTS) software must not be modified except in extraordinary circumstances (e.g. when needed for a critical business requirement). Those circumstances must be documented and approved by the Information Owner.

If changes to COTS software are required the Information Owner and Service Owners must determine and document:

- the impact on security controls in the software;
- the consent of the vendor, if required;
- if the required functionality is included in a newer version of the software;
- if government will be responsible for maintenance of the software after the change; and
- compatibility with other software in use.

If changes are made to COTS software the original version must be kept in an unaltered state. The changes must be:

- logged and documented, including a detailed technical description;
- applied to a copy of the original software; and
- tested and reviewed to ensure that the modified software operates as intended.

10.2.5 Secure System Engineering Principles

Principles for engineering secure systems must be established, documented, maintained and applied to any information system implementation efforts.

Information Owners and Service Owners must:

- ensure that secure information system engineering procedures based on security engineering principles are established, documented and applied to information system engineering activities;
- ensure that security is designed into all architecture layers: business, data, applications and technology;
- ensure the need for information security is balanced with the need for accessibility;
- analyze new technology for security risks and review the design against known attack patterns; and
- ensure that security engineering principles are reviewed and updated regularly.

10.2.6 Secure Development Environment

Secure development environments for system development and integration efforts must be established and appropriately protected throughout the entire system development lifecycle.

The “secure development environment” refers to the people, processes and technology associated with system development and integration.

Information Owners and Service Owners must establish secure development environments by considering:

- the sensitivity of data to be processed, stored and transmitted by the system;
- applicable external and internal requirements (e.g. regulations, policies);
- security controls already implemented;
- human resource security;
- the degree of outsourcing;
- the need for segregation between different development environments;
- access control to the environment;
- monitoring of change to the environment and code it stores;
- storing backups at secure offsite locations; and
- control over movement of data to and from the environment.

10.2.7 Outsourced Development

Controls must be applied to secure outsourced information system development.

To help ensure that software performs as expected and meet security requirements, Information Owners and Service Owners must implement the following controls when outsourcing development:

- procurement policy for licensing, ownership and intellectual property rights;
- contractual requirements for secure design, coding and testing practices in accordance with Section 10.2.1;
- provision of the approved threat model to the external developer;
- acceptance testing for the quality and accuracy of the deliverables;
- provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;
- testing of the software for vulnerabilities and malicious code;
- escrow arrangements if source code is no longer available;
- contractual right to audit development processes and controls; and
- the government remains responsible for compliance with applicable laws and control efficiency verification.

10.2.8 System Security Testing

Testing of security functionality must be carried out during development.

Information Owners and Service Owners must ensure that new and updated systems require thorough testing and verification during the development processes. A detailed schedule of activities must be prepared with test inputs and expected outputs under a range of conditions.

Tests must initially be performed by the development team. Independent acceptance testing must then be undertaken (for both in-house and outsourced developments) to ensure that the system works as expected and only as expected. The extent of testing must be in proportion to the importance and nature of the system.

See Section 8.1.4 for instructions regarding the separation of development, testing and operational environments.

10.2.9 System Acceptance Testing

Acceptance testing programs and related criteria must be established for new information systems, upgrades and new versions.

Information Owners and Service Owners must document system acceptance criteria as part of the system development and acquisition process. The criteria include:

- projected performance and resource capacity requirements;
- restart plans and procedures;
- impact on routine operating procedures and manual procedures;
- implementation of security controls;
- assurance that installation of the new system will not adversely affect existing systems particularly at peak processing times;
- training requirements; and
- user acceptance testing.

10.3 Test Data

Objective:
To ensure the protection of data used for testing.

10.3.1 Protection of Test Data

Test data must be protected and controlled using the same procedures as those in operational systems.

Information Owners must ensure that:

- personal and other sensitive data from operational systems is not used as test data;
- the extraction of test data from operational systems is authorized and logged;
- test data is safeguarded in accordance with its level of sensitivity; and
- data from operational systems is removed from the test environment once testing is complete.

Government of Saskatchewan

Information Security Policy

Chapter 11

Supplier Relationships

Chapter 11 – Supplier Relationships		
11.1 Information Security in Supplier Relationships		
11.1.1	Information Security Policy for Supplier Relationships	Information security requirements for mitigating the risks associated with supplier's access to the government's information assets must be agreed with the supplier and documented.
11.1.2	Addressing Security Within Supplier Agreements	Arrangements with suppliers involving accessing, processing, storing, communicating or managing the Government's information, information systems or information processing facilities must be based on a formal agreement containing necessary security requirements.
11.1.3	Information and Communication Technology Supply Chain	Agreements with suppliers must include requirements to address the risks associated with information and communications technology services and product supply chain.
11.2 Supplier Service Delivery Management		
11.2.1	Monitoring and Review of Supplier Services	The government must regularly monitor and review supplier service delivery.
11.2.2	Managing Changes to Supplier Services	Change management process for services provided by suppliers must take into account the criticality of the information systems, processes involved and assessment of risks.

11.1 Information Security in Supplier Relationships

Objective:

To ensure protection of government information assets that are accessible by suppliers.

11.1.1 Information Security Policy for Supplier Relationships

Information security requirements for mitigating the risks associated with supplier's access to the government's information assets must be agreed with the supplier and documented.

Security controls must be implemented before a supplier is allowed to access the government's information assets. The controls include processes and procedures to be implemented by government and those that must be implemented by the supplier. Among the controls are:

- identifying and documenting the types of suppliers (e.g. IT services, logistics, utilities, financial services, IT infrastructure) that the government will allow to access its information;
- a standardized process and lifecycle for managing supplier relationships;
- defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;
- minimum information security requirements as determined by the data classification and type of access to serve as the basis for individual supplier agreements based on the government's needs and its risk profile;
- processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;
- accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;
- types of obligations applicable to suppliers to safeguard the government's information;
- handling incidents and contingencies associated with supplier access including responsibilities of both the government and suppliers;

- resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;
- awareness training for the government's personnel involved in acquisitions regarding applicable policies, processes and procedures;
- awareness training for the government's personnel interacting with suppliers regarding rules of engagement and behaviour based on the type of supplier and the level of access;
- conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
- managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period; and
- non-disclosure agreements to safeguard sensitive information.

11.1.2 Addressing Security within Supplier Agreements

Arrangements with suppliers involving accessing, processing, storing, communicating or managing the Government's information, information systems or information processing facilities must be based on a formal agreement containing necessary security requirements.

Information Owners and Service Owners, in consultation with Information Security Branch, must ensure that agreements are established to document both parties' obligations to fulfil relevant information security requirements. The following terms must be considered for inclusion in the agreements:

- description of the information to be accessed and methods of access;
- the security classification level of the information and, if applicable, a mapping between the government's classification scheme and that of the supplier;
- legal and regulatory requirements, intellectual property rights and copyright requirements;
- obligation of each party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
- rules of acceptable use;
- either 1) an explicit list of supplier personnel authorized to access or receive the government's information or 2) procedures and conditions for granting and removal of authorization for access to or receipt of the government's information by supplier personnel;
- information security policies relevant to the specific contract;
- incident management requirements and procedures including notification and collaboration during incident remediation;
- training and awareness requirements;
- relevant regulations required for sub-contracting, including the controls that need to be implemented;
- a contact person for information security issues;
- screening requirements, if applicable, for supplier's personnel including responsibilities for conducting the screening and notification if screening results show cause for concern;
- right to audit the supplier's processes and controls related to the agreement;
- defect resolution and conflict resolution processes;
- supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

- supplier's obligations to comply with the government's security requirements; and
- procedures for continuing processing in the event the supplier becomes unable to supply its products or services.

11.1.3 Information and Communication Technology Supply Chain

Agreements with suppliers must include requirements to address the risks associated with information and communications technology services and product supply chain.

Information Security Branch must define information security requirements that apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships.

Service Owners must ensure that the following are included in supplier agreements:

- for information and communication technology services, requiring that suppliers propagate the government's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to government;
- implementing a monitoring process and acceptable methods for validating that delivered products and services are adhering to the stated security requirements;
- obtaining assurance that the delivered products are functioning as expected without any unexpected or unwanted features;
- defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the government and suppliers; and
- implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks; This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

11.2 Supplier Service Delivery Management

Objective:

To maintain an agreed level of information security in line with supplier agreements.

11.2.1 Monitoring and Review of Supplier Services

The government must regularly monitor and review supplier service delivery.

Information Owners and Service Owners must monitor and review the security-related terms and conditions in agreements with suppliers. The processes must include:

- designating responsibility for monitoring to an employee;
- monitoring service performance levels to verify adherence to the agreements;
- reviewing service reports produced by the supplier;
- conducting audits of suppliers and follow-up on identified issues;
- handling information security incidents in accordance with Chapter 12 and implementing any recommended controls that follow from the review;
- resolving and managing any other identified problems;
- ensuring the supplier maintains sufficient service capability in accordance with Chapter 13 where applicable.

Non-security related items are handled in accordance with Procurement Policies of the Ministry of Central Services.

11.2.2 Managing Changes to Supplier Services

Change management process for services provided by suppliers must take into account the criticality of the information systems, processes involved and assessment of risks.

Information Owners and Service Owners must ensure agreements with suppliers include provisions for amending agreements in response to changes in legislation, regulation, business requirements, policy or service delivery.

Information Owners and Service Owners must ensure that the security-related change management process for services delivered by suppliers includes:

- reviewing and updating the Threat and Risk Assessment (or other related security assessment) to determine the impact on security controls;
- implementing new or enhanced security controls when identified by the risk assessment;
- reviewing and updating the Privacy Impact Assessment (if applicable); and
- initiating and implementing revisions to policies and procedures.

Contact the Ministry of Central Services for complete procurement policies and standards.

Government of Saskatchewan

Information Security Policy

Chapter 12

Information Security Incident Management

Chapter 12 – Information Security Incident Management		
12.1 Management of Information Security Incidents and Improvements		
12.1.1	Responsibilities and Procedures	Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.
12.1.2	Reporting Information Security Events	Information security events must be reported through appropriate management channels immediately.
12.1.3	Reporting Information Security Weaknesses	Personnel using information systems must note and report any observed or suspected security weaknesses in those systems.
12.1.4	Assessment of and Decision on Information Security Events	Information security events must be assessed to determine if they are to be classified as information security incidents.
12.1.5	Response to Information Security Incidents	Information security incidents must be responded to in accordance with documented procedures.
12.1.6	Learning from Information Security Incidents	Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.
12.1.7	Collection of Evidence	Evidence collected during information security incident investigations must be collected using processes that ensure it can be reliably used for legal or disciplinary proceedings.

12.1 Reporting Information Security Events and Weaknesses

Objective:

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

12.1.1 Responsibilities and Procedures

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.

The Director, Information Security Branch, is responsible for the following procedures:

- incident response planning and preparation;
- monitoring, detecting, analyzing and reporting of information security events and incidents;
- logging incident management activities;
- handling of forensic evidence;
- assessment of and decision on information security events and assessment of information security weaknesses; and
- response and recovery from an incident.

12.1.2 Reporting Information Security Events

Information security events must be reported through appropriate management channels immediately.

All users of Government information systems must report information security events immediately to the Information Technology Division Service Desk. Examples of events include, but are not limited to:

- ineffective security control;
- breach of information confidentiality, integrity or availability expectations;
- human errors;
- non-compliance with policies or guidelines;
- breaches of physical security;
- uncontrolled system changes;
- unauthorized installation of software or hardware;
- malfunctions of software or hardware;
- access violations;
- malicious software; and
- lost or stolen information assets.

Information security events reported to a Ministry by a supplier (see Section 11.1.2) must be further reported to Information Security Branch.

12.1.3 Reporting Information Security Weaknesses

Personnel using information systems must note and report any observed or suspected security weaknesses in those systems.

All users of Government information systems must report security weaknesses to their Ministry Security Officer. Follow the authorized reporting process.

No user may attempt to exploit any security weakness.

12.1.4 Assessment of and Decision on Information Security Events

Information security events must be assessed to determine if they are to be classified as information security incidents.

Information Security Branch must assess each information security event. Based on the incident classification scale it must be decided if the event must be classified as an information security incident.

Results of the assessment and decision must be recorded in detail for future reference and verification.

12.1.5 Response to Information Security Incidents

Information security incidents must be responded to in accordance with documented procedures.

Information security incidents must be responded to by Information Security Branch personnel or others designated by the Director, Information Security Branch.

The response must include:

- collecting evidence as soon as possible after the occurrence;
- conducting information security forensics analysis if required;
- escalation, if required;
- ensuring that all response activities are properly logged for later analysis;
- communicating the existence of the incident and any relevant details to internal and external people and organizations with a “need-to-know;”
- dealing with information security weaknesses found to have caused or contributed to the incident; and
- once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis must take place, as necessary, to identify the source of the incident.

Service Owners must ensure that incidents involving supplier services are handled in accordance with the procedures documented in supplier agreements.

12.1.6 Learning from Information Security Incidents

Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

Information Security Branch is responsible for monitoring and evaluating information security incidents by:

- using statistical analysis of incident frequency, type and location to identify trends;
- ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and Business Continuity and Disaster Recovery Plans;
- advising Information Owners and Ministry Security Officers of evolving security threats and mitigation strategies;
- evaluating the effectiveness of incident management, response and reporting; and
- evaluating the effectiveness of information security technologies.

12.1.7 Collection of Evidence

Evidence collected during information security incident investigations must be collected using processes that ensure it can be reliably used for legal or disciplinary proceedings.

It may not be known at the time of an incident whether or not it will result in formal administrative or legal proceedings. Any evidence must be collected with those possibilities in mind in an effort to help ensure the admissibility and weight.

Evidence must be collected by procedures developed by the Director, Information Security Branch. The chain of custody must be maintained.

Evidence may only be collected by individuals authorized by the Director, Information Security Branch.

Information Owners, Ministries and Agencies in receipt of a legal order to produce electronic evidence must immediately contact the Director, Information Security Branch.

For information on computer media, mirror images or copies must be made depending on the type of media. A log of all actions taken during the copying process must be kept and the process witnessed. The original media must be placed in a tamperproof bag, initialed and dated, kept under lock and key and remain untouched. Any forensic work must only be performed on the copies of the evidential material.

Government of Saskatchewan

Information Security Policy

Chapter 13

Information Security Aspects of Business Continuity Management

Chapter 13 – Information Security Aspects of Business Continuity Management		
13.1 Information Security Continuity		
13.1.1	Planning Information Security Continuity	The government must determine its requirements for information security and the continuity of information security management in a crisis, disaster or other adverse situations.
13.1.2	Implementing Information Security Continuity	The government must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
13.1.3	Verify, Review and Evaluate Information Security Continuity	The government must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.
13.2 Redundancies		
13.2.1	Availability of Information Processing Facilities	Information systems must be implemented with redundancy sufficient to meet availability requirements.

13.1 Information Security Continuity

Objective:

To embed information security continuity in the government's business continuity management systems.

13.1.1 Planning Information Security Continuity

The government must determine its requirements for information security and the continuity of information security management in a crisis, disaster or other adverse situations.

Information security requirements must be determined when planning for business continuity and disaster recovery.

Information Owners and Service Owners must determine whether the continuity of information security is captured within the business continuity management process and the disaster recovery management process.

In the absence of formal business continuity and disaster recovery planning, information security management must assume that information security requirements remain the same in adverse situations, compared to normal operational conditions.

13.1.2 Implementing Information Security Continuity

The government must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Information Owners and Service Owners must ensure that:

- an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
- incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated; and
- documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event while maintaining its information security to a predetermined level based on management-approved information security continuity objectives.

Information Owners and Service Owners must establish, document, implement and maintain:

- information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- process, procedures and implementation changes to maintain existing information security controls during an adverse situation; and
- compensating controls for information security controls that cannot be maintained during an adverse situation.

13.1.3 Verify, Review and Evaluate Information Security Continuity

The government must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Information Owners and Service Owners must verify information security management continuity of its information assets by:

- exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;
- exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with continuity objectives; and
- reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Your Ministry may have developed its own policy regarding Business Continuity Planning. If so, refer to it for requirements for exercising and updating business continuity plans.

13.2 Redundancies

Objective:

To ensure availability of the government's information systems.

13.2.1 Availability of Information Processing Facilities

Information systems must be implemented with redundancy sufficient to meet availability requirements.

Information Owners and Service Owners must identify business requirements for the availability of information systems. When the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures must be considered.

Where applicable, redundant information systems must be tested to ensure the failover from one component to another works as intended.

Government of Saskatchewan

Information Security Policy

Chapter 14

Compliance

Chapter 14 – Compliance		
14.1 Compliance with Legal and Contractual Requirements		
14.1.1	Identification of Applicable Legislation and Contractual Requirements	The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.
14.1.2	Intellectual Property Rights	Controls must be implemented to ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and proprietary software licensing.
14.1.3	Protection of Records	Government records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release.
14.1.4	Privacy and Protection of Personally Identifiable Information	Security controls must be applied to protect privacy and personally identifiable information in accordance with relevant legislation.
14.1.5	Regulation of Cryptographic Controls	Cryptographic controls must be used in conjunction with relevant agreements, laws and regulations.
14.2 Information Security Reviews		
14.2.1	Independent Review of Information Security	Independent reviews of the Information Security Program must be regularly conducted.
14.2.2	Compliance with Security Policies and Standards	Managers must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards
14.2.3	Technical Compliance Review	Information systems must be regularly reviewed for compliance with security policies and standards.

14.1 Compliance with Legal and Contractual Requirements

Objective:

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security.

14.1.1 Identification of Applicable Legislation and Contractual Requirements

The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained.

Information Owners and Service Owners are responsible for ensuring that statutory, regulatory, policy and contractual requirements of each information system are:

- identified and documented before commencing a system development or enhancement initiative; and
- reviewed prior to, or concurrent with, changes to legislation, regulation or policy.

14.1.2 Intellectual Property Rights

Controls must be implemented to ensure compliance with legal, regulatory and contractual requirements related to intellectual property rights and proprietary software licensing.

Information Owners and Service Owners must protect intellectual property by:

- acquiring software from reputable vendors ;
- maintaining proof and evidence of ownership or right to use;
- implementing controls to ensure that the maximum allowable number of users is not exceeded;
- carrying out checks to verify that only authorized software and licensed products are installed;
- adhering to license terms and conditions;
- transferring licenses to others only when authorized;
- detecting and removing unlicensed software;
- ensuring intellectual property, licensed software and information are removed from digital media prior to disposition;
- complying with the terms and conditions for software and information obtained from public networks;
- not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law;
- not copying, in full or in part, books, articles, reports or other documents other than permitted by copyright law; and
- informing personnel of government policies including those pertaining to appropriate use of government resources.

14.1.3 Protection of Records

Government records must be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

The Archives and Public Records Management Act, 2015, subsidiary Regulations and policies outline the requirements for the retention and disposal of government records.

The Provincial Archives of Saskatchewan is responsible for:

- providing records and information management services to the Provincial Government;
- the development and dissemination of policies, procedures, standards and guidelines related to records and information management;
- records management advice and support to government institutions; and
- processing the requests for disposal of government records.

The Saskatchewan Records Management Policy is published on the Provincial Archives of Saskatchewan web site.

14.1.4 Privacy and Protection of Personally Identifiable Information

Security controls must be applied to protect privacy and personally identifiable information in accordance with relevant legislation.

The Freedom of Information and Protection of Privacy Act, its subsidiary Regulations and policies govern the protection of personal information held by the Government of Saskatchewan.

The Ministry of Justice's Access and Privacy Branch helps government institutions in their compliance with this legislation.

See Section 4.2.1 for instructions on how to classify personally identifiable information.

This security policy, standards and related guidelines include controls for the safeguarding of all sensitive information.

14.1.5 Regulation of Cryptographic Controls

Cryptographic controls must be used in conjunction with relevant agreements, laws and regulations.

Information Owners and Service Owners must:

- ensure the use of cryptographic controls when supported by the data classification;
- consult with Information Security Branch regarding the records management, electronic commerce, information access, privacy and security issues prior to acquiring cryptographic controls;
- ensure encrypted government information assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys as defined by the Chief Information Officer; and
- if acquiring cryptographic controls from outside Canada the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into Canada.

See Chapter 6 for policy on use of cryptography.

14.2 Information Security Reviews

Objective:

To ensure that information security is implemented and operated in accordance with the government's policies and procedures.

14.2.1 Independent Review of Information Security

Independent reviews of the Information Security Program must be regularly conducted.

The Information Technology Division Security Program is audited annually by the Provincial Auditor of Saskatchewan.

The Director, Information Security Branch, may initiate a supplemental audit or review to:

- assess the effectiveness of the Information Security Program;
- document the results; and
- report the results to senior management.

This review must be conducted by an independent supplier.

The Chief Information Officer must address the weaknesses and non-compliant controls that are identified in reports from the Provincial Auditor or independent reviewers.

14.2.2 Compliance with Security Policies and Standards

Managers must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.

Information Owners and Service Owners must ensure security policies and processes are implemented and adhered to by:

- conducting periodic self-assessments;
- initiating independent assessments, reviews or audits; and
- ensuring personnel receive regular information security awareness updates.

When review processes indicate non-compliance with policies Information Owners and Service Owners must:

- determine cause(s);
- assess the threats and risks on non-compliant processes;
- document the marginal risks; and
- determine and implement corrective action.

14.2.3 Technical Compliance Review

Information systems must be regularly reviewed for compliance with security policies and standards.

Service Owners must periodically test information system technical control compliance by using automated tools to:

- detect network intrusion;
- conduct vulnerability assessments and/or penetration testing;
- determine if information system patches have been applied;
- confirm that technical controls have been implemented and are functioning as intended.

Service Owners must perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or system changes have not been made.

Service Owners who are responsible for technical compliance checking must:

- consult Operations personnel prior to initiating tests;
- notify the Director, Information Security Branch, prior to testing to prevent triggering false security alarms;
- ensure that the automated testing of operational systems is conducted by authorized personnel;
- assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Ministry Security Officer;
- provide affected Information Owners and the Director, Information Security Branch, with copies of test results and action plans;
- provide the Director, Information Security Branch with the internal or external audit reports immediately upon receipt; and
- maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

Ministries must consult with the Director, Information Security Branch, prior to issuing Requests for Proposal or contracts for technical compliance checking.

The Director, Information Security Branch, must provide summarized reports to the Chief Information Officer on the status and results of testing.

Government of Saskatchewan

Information Security Policy

Glossary

Some of the definitions here are borrowed from the following sources. In some cases the definition has been modified to meet the needs of the Government of Saskatchewan.

International Standards Organization

"Information technology – Security techniques – Information security management systems – Overview and vocabulary" Chapter 2: Terms and definitions
Third edition 2014-01-15
ISO/IEC 27000:2014

Government of Canada

Information Security Glossary
Terminology Bulletin 290 2013
http://www.bt-tb.tpsgc-pwgsc.gc.ca/btb.php?lang=eng&cont=2093

IT Security Risk Management: A Lifecycle Approach
ITSG-33 – Annex 5: Glossary
Communications Security Establishment Canada, November 2012

Government of British Columbia

Information Security Policy Version 2.2 October 2012
Appendix A – Glossary

Government of the United States

Committee on National Security Systems Instruction No. 4009
Committee on National Security Systems (CNSS) Glossary
CNSS Secretariat, National Security Agency
April 6, 2015

National Institute of Standards and Technology
US Department of Commerce
Glossary of Key Information Security Terms
NISTIR 7298 Revision 2 May 2013

Term	Definition
access control	means to ensure that access to any information system resource is authorized and restricted based on business and security requirements;
Access Control List (ACL)	a list of permissions associated with an object; the list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object;
Advanced Encryption Standard (AES)	A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.
AES-256	an implementation of the Advanced Encryption Standard that uses a cipher key of 256 bits;
application	a software program hosted by an information system;
asset	hardware, software, network infrastructure and all forms of electronic information that has value to the government;
audit	independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures;
audit log	a chronological record of system activities; includes records of system accesses and operations performed in a given period;
authentication	verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system;
availability	property of being accessible and usable upon demand by an authorized entity;
backup	a copy of files and programs made to facilitate recovery, if necessary;
biometric	measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual; facial images, fingerprints, and handwriting samples are all examples of biometrics;
chain of custody	a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer;
commercial-off-the-shelf (COTS)	a software and/or hardware product that is commercially ready-made and available for sale, lease, or license to the general public;
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes;

Term	Definition
control	the management, operational, and technical controls prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information;
countermeasure	see “control”
cryptographic key	a value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification;
cryptography	the discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification;
digital signature	an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature; digital signatures provide authenticity protection, integrity protection, and non-repudiation;
disaster recovery plan (DRP)	the procedures and information necessary to recover critical IT functions from any event that may interrupt an operation or affect service or program delivery, within the timeframes determined in the Business Impact Assessment;
egress filtering	the practice of monitoring and potentially restricting the flow of information outbound from one network to another, typically from a private network to the Internet;
electronic messaging services	services providing interpersonal messaging capability; meeting specific functional, management, and technical requirements; and yielding a business-quality electronic mail service suitable for the conduct of official government business;
electronic storage media	includes computer hard drives, memory sticks, CD ROM’s, floppy disks, digital video discs, microcomputer tapes, microfiche, microfilm, point-of-sale credit card terminals, portable digital assistants (PDAs) or any other permanent electronic storage media; other storage media included are cellular phones with internal storage, film, video and audio tapes, or any other recordable media or devices with memory; (Saskatchewan Electronic Storage Media Disposal Policy)
electronic security perimeter	the logical or physical demarcation point between networks of differing security protection requirements, ownership or governance;
employee	a person appointed pursuant to *The Public Service Act, 1998.*
encryption	the process of changing plaintext into ciphertext for the purpose of security or privacy;

Term	Definition
event	an identified occurrence of a system or service state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant;
executive government	means the executive government of Saskatchewan; (*The Executive Government Administration Act)*
FIPS 140-2 Validated	A product or cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in Federal Information Protection Standard (FIPS) 140-2 (as amended). Validated modules are approved for the protection of Sensitive Information in the US Government and Protected Information in the Government of Canada. For further information see the US National Institute of Standards and Technology (NIST) discussing CMVP.
firewall	a gateway that limits access between networks in accordance with local security policy;
government records	include all recorded information that relates to the transaction of government business, regardless of format (e.g. documents, maps, e-mails, photographs, etc.); (Saskatchewan Records Management Policy) also see “record”
incident	an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies;
information processing facilities	any information processing system, service or centralized infrastructure, or the physical location housing it;
information security	the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability;
information security event	see “event”
information security incident	see “incident”
information system	a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

Term	Definition
injury	the damage to the national interests and non-national interest that business activities serve resulting from the compromise of IT assets;
integrity	property of accuracy and completeness;
intellectual property	creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights;
intrusion	an information security incident involving unauthorized access to, or activity on, a computer system or network;
intrusion detection	the process of monitoring activity occurring in a computer system or network and analyzing them for signs of possible events;
key management	the processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys;
least privilege	the security objective of granting users only those accesses they need to perform their official duties;
local admin	in a Windows environment means unrestricted access to a specific computer;
malicious code	malicious code is designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, disclosing unauthorized information, corrupting information, denying service, or stealing resources. Types of malicious code include viruses, worms, Trojans, spyware and denial of service attacks.
malware	see “malicious code”
media	devices onto which information is recorded, stored, or printed within an information system;
media sanitization	the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means;
ministry	means a ministry, department, secretariat, office or other similar agency of the executive government; (*The Executive Government Administration Act*)

Term	Definition
mobile device	A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. See portable storage device.
monitoring	a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards;
multifactor authentication	authentication using two or more factors to achieve authentication; factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
need-to-know	a requirement for a person to have access to particular information to perform his or her duties;
network	information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices;
network security zone	a logical entity containing one or more types of services and entities of similar security requirements and/or risk levels;
network segregation	the separation of groups of users, information systems and services with similar business functions by control of network traffic flow, e.g., by use of security gateways, physically separate networks or access controls;
network service agreement	the contract or agreement between a service provider and a service consumer which defines the services to be delivered and the terms and conditions of delivery;
non-repudiation	protection against an individual falsely denying having performed a particular action; provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message;
personal health information	personal health information as defined in *The Health Information Protection Act;*

Term	Definition
personal information	personal information as defined in *The Freedom of Information and Protection of Privacy Act;*
portable storage device	Portable device that can be connected to an information system (IS), computer, or network to provide data storage. These devices interface with the IS through processing chips and may load driver software, presenting a greater security risk to the IS than non-device media, such as optical discs or flash memory cards. Note: Examples include, but are not limited to: USB flash drives, external hard drives, and external solid state disk (SSD) drives. Portable Storage Devices also include memory cards that have additional functions aside from standard data storage and encrypted data storage, such as built-in Wi-Fi connectivity and global positioning system (GPS) reception.
Privacy Impact Assessment (PIA)	a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation; (Office of the Saskatchewan Information and Privacy Commissioner)
privilege	a right granted to an individual, a program, or a process;
privileged user(s)	users with permissions to alter access rights and structures of information systems; this includes (but is not limited to) system administrators, network administrators, database administrators, security administrators, web site administrators, system operators and network operators;
record	means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or other mechanism that produces records; *(The Archives and Public Records Management Act)* also see “government records”
remote access	access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet);
removable media	see “portable storage device”
risk	combination of the probability of an event and its consequence;
risk analysis	the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact;
risk assessment	see “risk analysis”
safeguard	see “control”
security control	see “control”

Term	Definition
security incident	see “incident”
security posture	the security status of a the government’s networks, information, and systems based on resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the government’s information technology and information and to react as the situation changes;
security weakness	a fault or deficiency in an application, procedure, process or associated technology that may result in a security incident;
spyware	code with malicious intent that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge;
telework	Telework is the regular performance of work by an employee from a Teleworkplace. (Human Resource Manual PS 1104)
threat	potential cause of an unwanted incident, which may result in harm to a system or organization;
threat and risk assessment (TRA)	the evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and other assets at risk;
trusted path	a network path that has been protected from eavesdropping, intrusion and data tampering;
uninterruptible power supply (UPS)	a backup power source for computers and computer networks to ensure on-going operation in the event of a power failure;
user ID	unique symbol or character string used by an information system to identify a specific user;
virtual private network (VPN)	a logical network layer, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks;
virus	A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.
vulnerability	weakness of an asset or control that can be exploited by one or more threats;
vulnerability assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.