Introduction

The Government of Prince Edward Island is the custodian of extensive information holdings and relies upon its information assets for fiscal, policy and program delivery initiatives. The management of public information requires that Government have an Information Security Policy (GISP) to protect the confidentiality, integrity and availability of the information assets in its care.

The Government Information Security Policy Manual provides the framework for Government organizations to establish local policies and procedures necessary for the protection of Government assets. Implementation of a structured Government Information Security Program will provide more consistent protection of information and technology resources.

The policies incorporate a risk assessment approach to security using Threat and Risk Assessment to consider:

- Business process and Government service delivery implications;
- Technological implications; and,
- Communication strategies including changes to personnel information security awareness programs.

The risk assessment approach enables:

- Compliance with legislative and policy objectives
- Cost-effective allocation of resources based on a risk assessment;
- Responsible governance of the Province's information assets; and,
- Secure provision of Government e-services.

Glossary

The Government Information Security Policy includes a Glossary of key terms. The first instance of a defined term in a policy is italicized. Terms from existing policies are adopted where appropriate.

Table of Contents

Chapter 1 – Security Policy 5
Chapter 2 – Organizing Information Security 9
Chapter 3 – Asset Management 19
Chapter 4 – Human Resources Security 23
Chapter 5 – Physical and Environmental Security 30
Chapter 6 – Communications and Operations Management 46
Chapter 7 – Access Control 77
Chapter 8 – Information Systems Acquisition, Development and Maintenance 102
Chapter 9 – Information Security Incident Management 115
Chapter 11 – Compliance 125
Appendix A – Glossary 133

Contact:

For inquiries regarding the Government Information Security Policy, contact the Office of Information Protection at ITSecurity@gov.pe.ca.

Chapter 1 – Security Policy

The Government Information Security Policy establishes requirements to ensure that information security policies remain current as business needs evolve and technology changes. This policy must be published and communicated to employees and relevant external parties.

1.1 Government Information Security Policy
1.1.1. Government Information Security Policy Document The Office of Information Protection is responsible for establishing, issuing and monitoring information security policies.
1.1.2. Review of the Government Information Security Policy The Government Information Security Policy must be reviewed on a regular basis and updated when required.

1.1	**Security Policy – Government Information Security Policy**
1.1.1	The Office of Information Protection is responsible for establishing, issuing and monitoring *information security* policies. a) *Government Information* Security Policy b) Departmental or agency Security Policy

Purpose: To establish comprehensive information security policies, processes and practices that will assist departments in delivering services.

1.1.1 a) Government Information Security Policy

The Government Information Security Policy is intended to establish minimum requirements for the secure delivery of Government services. Secure service delivery requires the assurance of *confidentiality*, *integrity*, *availability* and *privacy* of Government *information assets* through:

- Management and business processes that include and enable security processes;
- Ongoing *personnel* awareness of security issues;
- Physical security requirements for *information system*s;
- Governance processes for information technology;
- Reporting information security *event*s and weaknesses;
- Creating and maintaining *business continuity plans*; and,
- *Monitoring* for compliance.

The Office of Information Protection recognizes that information security is a process, which to be effective, requires management commitment, the active participation of all personnel and ongoing awareness programs. (ITSecurity@gov.pe.ca)

1.1.1 b) Departmental or agency Security Policy

Departments may develop and implement additional information security policies, standards and guidelines for use within their organization or for a specific information system or program. Departmentally developed information security policies, standards and guidelines can exceed but must not conflict with the baseline established by the Government Information Security Policy.

Departments must provide the Office of Information Protection with copies of any locally developed information security policies, standards or guidelines.

A central repository must be maintained by the Office of Information Protection for the collection and re-use of departmentally developed information security policies, standards or guidelines.

1.1.2. The Government Information Security Policy must be reviewed on a regular basis and updated when required.

a) Government Information Security Policy review – Office of Information Protection

b) Government Information Security Policy review – Departments and other agencies

Purpose: To ensure information security policies remain current with evolving business needs and technological changes.

1.1.2 a) Government Information Security Policy review – Office of Information Protection

The Office of Information Protection is responsible for reviewing information security policies, standards and guidelines on an annual basis. Policies and standards review must be initiated:

- In conjunction with legislative, regulatory or policy changes which have information management implications;
- During planning and implementation of new or significantly changed technology;
- Following a *Threat and Risk Assessment* of major initiatives (e.g., new information systems or contracting arrangements);
- When *audit* reports or security *risk* and controls reviews identify high risk exposures involving information systems;
- If threat or vulnerability trends produced from automated monitoring processes indicate the probability of significantly increased risk;
- After receiving the final report of investigation into information security *incident*s;
- Prior to renewing third party access agreements which involve major Government programs or services;
- When industry, national or international standards for information security are introduced or significantly revised to address emerging business and technology issues; and,
- When associated external agencies (e.g., Information and Privacy Commissioner and RCMP) issue reports or identify emerging trends related to information security.

1.1.2 b) Government Information Security Policy review – Departments and other agencies

Where Departments have developed departmental specific information security policies, standards and guidelines they must:

- Review them annually; and,
- Provide the Office of Information Protection with copies of updated documents.

Chapter 2 – Organizing Information Security

The protection of information assets requires a multi-disciplinary approach that is supported by the Government information security organization. This chapter describes the management structure needed to coordinate information security activities including required information security activities, which coordinates them and what agreements are required. This coordination applies to internal organizations and to external parties accessing or managing the organization's information assets.

The information security organization requires the support of a network of contacts in the information security community to elicit advice, trends and to deal with other external factors.

2.1 Internal Organization
2.1.1 Management commitment to information security Management must set direction and provide support for information security.
2.1.2 Information security co-ordination Implementation of information security activities across Government must be coordinated by the Office of Information Protection
2.1.3 Allocation of information security responsibilities Information security responsibilities must be documented
2.1.4 Approval process for information security processing facilities Establishment of new information systems and processing facilities requires formal management authorization.
2.1.5 Confidentiality agreements A confidentiality agreement reflecting organizational requirements for the handling of information must be in place and reviewed regularly.
2.1.6 Contact with special interest groups Appropriate contacts shall be maintained with specialist security forums and professional associations.
2.2 External Parties
2.2.1 Identification of risks related to external parties Assessment of risks from external party access to Government information, information systems or information processing facilities shall be undertaken and appropriate security controls implemented.
2.2.2 Addressing security when dealing with customers Identified security requirements must be addressed prior to granting external parties access to information, information systems or information processing facilities.
2.2.3 Addressing security in external party agreements Arrangements involving external party access to information, information systems or information processing facilities must be based on a formal contract containing necessary security requirements.

2.1	**Organizing Information Security – Internal organization**
2.1.1	Management must set direction and provide support for information security. a) *Chief Information Security Officer* b) Office of Information Protection c) Information Technology Architect

Purpose: To establish management direction on, and commitment to, information security to maintain the confidentiality, integrity and availability of Government information.

2.1.1 a) Chief Information Security Officer

The Chief Information Security Officer must establish an Information Security Program to manage and co- ordinate *information security activities* across Government by:

- Providing leadership on methodologies and processes for information security;
- Advising on the information security requirements for documented;
- Evaluating information received during and after an information security incident;
- Implementing performance measurement processes for security controls;
- Ensuring information security activities are in compliance with the Government Information Security Policy;
- Recommending appropriate actions in response to identified information security incidents and initiating audits where necessary; and,
- Building relationships with stakeholder and partner organizations including suppliers, other provincial security incident response centres and national incident response centres to assist in maintaining the Information Security Program.

2.1.1 b) Office of Information Protection

The Office of Information Protection provides the security infrastructure necessary to protect Government information assets by:

- Establishing an *information security architecture* for standard security controls across Government;
- Defining organizational roles and responsibilities for information security;
- Developing and reviewing the Government Information Security Policy;
- Monitoring and measuring the implementation of the Government Information Security Policy; and,
- Developing and delivering a program to maintain information security awareness.

The Office of Information Protection must also assist in establishing an Information Security Program to manage and co-ordinate information security across Government by:

- Identifying security controls required to enable service delivery and documenting those controls in the Government policy, standards and guidelines;
- Providing security-related technical architecture advice to planning and

development groups;
- Promoting information security education, training and awareness throughout the Government Information ;
- Identifying significant threat changes and exposures to threats of assets associated with information security;
- Ensuring the Information Incident Management Process is followed for all suspected or actual information incidents;
- Identifying responses to remediate activities that are not in compliance with policies, standards or best practices;
- Coordinating the implementation of information security controls;
- Interpreting the Government 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 major information security incidents;
- Identifying general business trends and emerging technologies, and recommending changes to Information Security Program;
- Analyzing and providing advice on emerging information security standards; and,
- Providing information security advice for business areas;
- Ensuring that standards/procedures to support day-to-day security activities are documented in compliance with the Government Information Security Policy;
- Coordinating information security awareness and education;
- Investigating reported information security events to determine if further investigation is warranted;
- Providing advice on security requirements for information systems development or enhancements;
- Developing and implementing information security policies, standards and guidelines;
- Promoting the consistent *application* of information security programs;
- Identifying issues related to information security disciplines and critical information asset protection;
- Identifying, assessing and managing information security *risks*; and,
- Conducting *Threat and Risk Assessment* of high profile initiatives.

2.1.1 c) Information Technology Consultatns (ITC's)

The responsibilities of the ITC's are:
- Being the single point of contact for information incidents within their department;
- Ensuring that the Information Incident Management Process is followed for all actual or suspected information incidents;
- Ensures information security reviews and audits are supported by the

department;

- Ensuring that departmental standards/procedures support day-to-day security activities and are documented in compliance with the Government Information Security Policy;
- Providing up-to-date information on issues related to information security;
- Assisting business areas in conducting *Threat and Risk Assessment*;
- Ensuring that each information system has a current *System Security Plan*;
- Coordinating departmental information security initiatives with cross-Government information security initiatives; and
- Raising departmental security issues to the Office of Information Protection.

2.1.2 Implementation of information security activities across Government must be coordinated by the Office of Information Protection.

a) Security co-ordination across Government

All ITC's and the Office of Information Protection

Purpose: To ensure that information security activities are carried out in a timely manner and that security issues are resolved.

2.1.2 a) Security Coordinator across Government

All ITC's and the Office of Information Protection

A cross-Government information model will provide advice and recommendations for:

- Developing and implementing information security policies, standards and guidelines;
- Promoting the consistent application of information security programs;
- Identifying issues related to information security discipline and critical information asset protection; and
- Identifying *Threat and Risk Assessments* of high profile initiatives.

2.1.3 Information security responsibilities must be documented.

a) Information security responsibilities

b) *Information Owners*

c) *Information Custodians*

Purpose: To define security roles and responsibilities for *information* and information systems.

2.1.3 a) Information security responsibilities

Responsibility for security throughout Government includes defining:

- The Information Owner and Information Custodian responsible for *information* and *information systems;*

- The assets and security processes; and,
- Authorization levels for access.

2.1.3 b) Information Owners

Within the Government of Prince Edward Island, information ownership flows from the Crown to Government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

Information Owners have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure and will:

- Determine business requirements including information security needs;
- Ensure information and information systems are protected commensurate with the sensitivity of their information;
- Define security requirements during the planning stage of any new or significantly changed information system;
- 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,
- Be involved with security reviews and/or audits.

2.1.3 c) Information Custodian

Information Custodians maintain or administer information assets on behalf of the Information Owners by:

- Providing and managing security for the information asset throughout its lifecycle;
- Maintaining and operating the technical infrastructure that information and information systems reside on; and,
- Maintaining and operating the security infrastructure protecting information and information systems.

2.1.4	Establishment of new information systems and processing facilities requires formal management authorization.

a) Approval for *information processing facilities*
b) Approval for information systems
c) Acquisition of *hardware*, *firmware* and software
d) Use of non-Government hardware

Purpose: To ensure the secure operation of new or significantly modified *information systems* and information processing facilities using a formal review and approval process.

2.1.4 a) Approval for information processing facilities

Prior to constructing any new information processing facilities, Information Owners and Information Custodians must:

- Have a Threat and Risk Assessment completed;
- Address security requirements in the construction of the facility; and
- Obtain advice from the Office of Information Protection to ensure adherence to relevant policies, procedures, standards and guidelines.

2.1.4 b) Approval for information systems

Information Owners and Information Custodians of a new or significantly modified *information system* must:

- Have a Privacy Impact Assessment completed;
- Have a Threat and Risk Assessment completed;
- Address security requirements in the development of the system; and,
- Obtain approval from the Office of Information Protection to ensure adherence to relevant Core Policy and Procedure and the Government Information Security Policy.

2.1.4 c) Acquisition of hardware, firmware and software

Prior to acquisition of new hardware, firmware or software, Information Owners and Information Custodians must consult with the Office of Information Protection to:

- Evaluate the need for any additional security measures and the impact on existing security processes.

2.1.4 d) Use of non-Government hardware

Personnel must not store Government information on non-Government hardware unless authorized. Information Owners and Information Custodians must test non-Government hardware for vulnerabilities prior to connecting it to the Government network.

2.1.5 A confidentiality agreement reflecting organizational requirements for the handling of information must be in place and reviewed regularly.
a) Confidentiality agreements

Purpose: To ensure *personnel* understand their role in maintaining the confidentiality of *information* and information systems.

2.1.5 a) Confidentiality agreements

Information Owners and Information Custodians must:

- Ensure *employees* are informed of their obligation to maintain the confidentiality of information; and,
- Ensure individuals other than employees accept and sign an agreement to maintain the confidentiality of information.

Confidentiality requirements must be reviewed and updated annually.

2.1.6	Appropriate contacts shall be maintained with specialist security forums and professional associations. a) Participation in security forums and professional associations

Purpose: To promote and further employee knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities.

2.1.6 a) Participation in security forums and professional associations

The need for personnel with information security responsibilities to maintain their knowledge of information security industry trends, best practices, new technologies and threats or vulnerabilities can be achieved by:

- Participating in information exchange forums regarding best practices, industry standards development, new technologies, threats, vulnerabilities, early notice of potential attacks, and advisories;
- Maintaining and improving knowledge regarding information security best practices; and,
- Creating a support network of other security specialists.

The Chief Information Security Officer must promote professional certification, and membership in professional associations, for personnel with information security responsibilities throughout Government.

2.2	**Organizing Information Security – External parties**
2.2.1	Assessment of risks from *external party* access to Government information, information systems or information processing facilities shall be undertaken and appropriate security controls implemented. a) Risk assessment b) Risk mitigation and acceptance

Purpose: To ensure the *risks* of external party access to *information* and *information systems* are identified, assessed, mitigated and managed.

2.2.1 a) Risk assessment

Information Owners and Information Custodians are responsible for assessing the business requirements and associated risks related to external party access to information and information systems.

Risk assessments must be documented during the conceptual design phase of a project and updated throughout the lifecycle of the information system (e.g., prior to and following technical or business process changes to the information system).

The assessment of risks related to external party access must consider:

- If existing controls prevent external parties from accessing facilities or information that are not needed to meet the business requirements for the access,
- Impacts to the controls of the information processing facilities involved,
- The sensitivity of the information assets,
- Policies and processes the external party has for personnel hiring, training (on security and privacy issues) and incident reporting,
- Internal and external processes for managing and reporting security and privacy incidents,
- Processes for identifying, authorizing, authenticating and reviewing access rights of personnel and systems of the external party,
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information,
- Impacts to both parties resulting from assets being unavailable, and,
- Data integrity requirements including impacts of accessing or using inaccurate information.

2.2.1 b) Risk mitigation and acceptance

Prior to authorizing access by external parties to information and information systems Information Owners and Information Custodians must confirm that:

- The terms and conditions of access are documented (e.g. services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

2.2.2 Identified security requirements must be addressed prior to granting external parties access to information, information systems or information processing facilities.

a) Security requirements

Purpose: To ensure that *risks* associated with external party access to *information* and *information systems* have been mitigated by the use of security controls as determined by business needs.

2.2.2 a) Security requirements

Prior to granting access to non-public information and information systems for external parties Information Owners and Information Custodians must:

- Determine that mitigation strategies have been implemented to address security requirements;
- Review the *Threat and Risk Assessment*
- Review the completed Privacy Impact Assessment:
  - ✓ Legislative, regulatory and policy considerations, and,
  - ✓ *Intellectual property* rights obligations
- Determine that security controls will not adversely affect target service levels; and,
- Document the roles and responsibilities of the Information Owner, Information Custodian and the external party in a formal agreement.

2.2.3 Arrangements involving external party access to information, information systems or information processing facilities must be based on a formal contract containing necessary security requirements. a) External party access agreements b) Security requirements

Purpose: To ensure external parties accessing information assets and information processing facilities are required to implement and use security controls.

2.2.3 a) External party access agreements

Information Owners and Information Custodians must ensure access to information assets and information processing facilities by external parties is only provided after an access agreement has been completed.

Access agreements must include:

- Roles and responsibilities of the Information Owner, Information Custodian and the external party;
- Approved security controls;
- Conditions for contract termination;
- Audit and compliance monitoring rights, responsibilities and processes;
- Reporting obligations for suspected or actual security and privacy incidents;
- Renewal and extension conditions; and,
- Requirements for regular compliance reviews.

Approved forms of agreement may include:

- Professional Service Contracts (T.B. Section 13)
- Agreements for Alternate Service Delivery or Public Private Partnership;
- Information Sharing Agreement; or,
- Other forms of agreement as approved by Legal Services.

2.2.3 b) Security requirements

Information Owners and Information Custodians must ensure the security requirements of external party access agreements include:

- Notification of obligations of the parties to adhere to legislation and regulation;
- Requirements to adhere to agreed information security policies and procedures;
- Processes for amending the agreement;
- Acknowledgement by the external party that ownership of information is retained by the Province;
- Confidentiality obligations of the external party and their personnel or agents;
- Requirements for use of unique user identifiers;
- Processes for conducting audits and compliance monitoring activities;
- Responsibilities and processes for reporting security and privacy incidents; and,
- Assurances that disciplinary action will be applied to employees or contractors who fail to comply with the terms of the agreement.

Chapter 3 – Asset Management

Information and information systems services constitute valuable Government resources. The asset management chapter establishes the blueprint to identify the rules of acceptable use and the rules for protection: what assets to protect, who protects them and how much protection is adequate.

To account for the assets that require protection, this chapter specifies the requirement to designate who owns assets. Designated owners become responsible for protecting information and technology assets and to maintain the way assets are protected.

3.1 Responsibility for assets
3.1.1 Inventory of assets An inventory of all important assets associated with information systems must be documented and maintained.
3.1.2 Ownership of assets Information Owners and Information Custodians must be designated for all assets associated with information systems.
3.1.3 Acceptable use of assets Rules for the acceptable use of information systems must be identified, documented, and implemented.

3.1	**Asset Management – Responsibility for assets**
3.1.1	An inventory of all important assets associated with information systems must be documented and maintained. a) Identification of assets b) Documenting and maintaining asset inventories c) Loss, theft or misappropriation of assets

Purpose: To identify and manage *information* and *information technology assets* associated with information systems or services ("assets") to provide control and accountability, support strategic planning, enhance critical incident response, system planning, protection, maintenance and recovery.

3.1.1. a) Identification of assets

Information Owners and Information Custodians must identify assets under their control including:

- Software;
- Hardware;
- Services including computer and communications services, and general utilities;
- All other information assets including: database and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, archived information.

3.1.1 b) Documenting and maintaining asset inventories

Information Owners and Information Custodians must document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of an enterprise risk management strategy.

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

- Type of asset;
- Ownership;
- Format;
- Location;
- Back-up information and location;
- License information;
- Sensitivity and safeguards requirements;
- Criticality for service delivery and maintaining business functions;
- Consequences of loss.

Information Owners and Information Custodians are accountable for asset identification and inventory maintenance.

3.1.1 c) Loss, theft or misappropriation of asset

The loss, theft or misappropriate of assets must be reported immediately using the Lost or Stolen Computer or Electronic Storage Device Report. Where the loss, theft or misappropriate involves sensitive or confidential information, the Office of Information Protection will contact the affected department's FOIPP Coordinator.

3.1.2 Information Owners and Information Custodians must be designated for all assets associated with information systems.

a) Responsibilities for asset ownership
b) Designating Information Custodians.

Purpose: To designate custodians for assets with approved management responsibility for the protection of organizational assets associated with information and technology systems or services.

3.1.2 a) Responsibilities for asset ownership

An Information Owner is responsible for controlling the production, development, maintenance, use and security of information and technology assets within their jurisdiction. Information Owners are responsible for:

- Ensuring the appropriate safeguarding of information and technology systems or services;
- Defining and regularly reviewing access restrictions, classifications and safeguards in accordance with applicable policies; and,
- Designating Information Custodians and ensuring that they have the correct tools for protecting designated assets.
- Ensuring that final *disposition* has been done in accordance with the compliance of Retention Schedules.

3.1.2 b) Designating Information Custodians

Information Owners may delegate responsibility for custody of information and technology systems or services to Information Custodians.

Information Custodians will be responsible for:

- Overseeing the functioning of information and technology assets;
- Delivery of services in accordance with defined service requirements; and,
- Regular reporting on designated information and technology assets.

3.1.3 Rules for the acceptable use of information systems must be identified, documented and implemented. a) Acceptable use of Government resources

Purpose: To prevent misuse or compromise of Government information systems.

3.1.3 a) Acceptable use of Government resources

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

The requirements for personal use of Government information systems are described in the Treasury Board Manual (Section 5.06 IT Security and Computer Use and Section 16 Planning and Management of Information Technology.)

Chapter 4 – Human Resources Security

This chapter identifies the information security requirements for personnel that have an employment relationship with Government organizations. To reduce information security risks, the terms and conditions of employment must establish expectations for the protection of Government assets, information and services.

This chapter references the terms and conditions set by the PEI Public Service Commission for employees and identifies the conditions for external personnel such as contractors.

Management and personnel have different security responsibilities and liabilities that apply prior, during, and at the time of termination of employment. Prior to employment, emphasis is on the awareness of the expected roles and responsibilities, the screening of prospects and the existence of agreements. During employment, policies establish management responsibilities, education, training and formal processes to handle problematic security situations. This chapter also establishes rules to ensure a secure transition when employment is ended or changed.

4.1 Prior to employment
4.1.1 Roles and Responsibilities Security roles and responsibilities for personnel must be documented.
4.1.2 Screening Personnel screening must be performed prior to entering a working relationship with the Province.
4.1.3 Terms and conditions of employment The terms and conditions of employment must document the responsibility of personnel for information and information systems security
4.2 During employment
4.2.1 Management responsibilities Management must ensure personnel comply with security policies and procedures.
4.2.2 Information security awareness, education and training Personnel must receive appropriate information security training and be informed of changes to the Government Information Security Policy and practices.
4.2.3 Disciplinary process Security breaches or policy violations caused by personnel must be reviewed by Management.
4.3 Termination or change of employment
4.3.1 Termination responsibilities Responsibilities for employment termination must be documented.
4.3.2 Return of assets Personnel must return Government assets upon termination or change of employment.
4.3.3 Removal of access rights The access rights of personnel to information systems must be removed upon termination of employment and reviewed upon change of employment.

4.1	**Human Resources Security – Prior to employment**
4.1.1	Security roles and responsibilities for personnel must be documented. a) Security roles and responsibilities b) Communication of security roles and responsibilities

Purpose: To ensure personnel are informed of their information security roles and responsibilities.

4.1.1 a) Security roles and responsibilities

Information Owners and Information Custodians must:

- Document information security roles and responsibilities for personnel in job descriptions, standing offers, contracts, and information use agreements; and,
- Review and update information security roles and responsibilities when conducting staffing or contracting activities.

4.1.1 b) Communication of security roles and responsibilities

Managers must ensure personnel are informed of their security roles and responsibilities by establishing processes for communicating security roles and responsibilities to protect information system assets.

4.1.2	Personnel screening must be performed prior to entering a working relationship with the Province. a) Screening for employees b) Screening for contractors

Purpose: To verify employment qualification claims made by personnel.

4.1.2 a) Screening for employees

The process for employee screening is detailed in PEI Public Service Commission Recruitment and Staffing section of the Human Resource Policy Manual, sub 6.03. Pre-Interview (screening).

4.1.2 b) Screening for contractors

The process for the hiring of contractors is outlined in Treasury Board Manual, section 13.04 Selection of Contractors. Each department is responsible for screening each contractor to ensure that they indeed meet the criteria outlined and the process should be commensurate with the sensitivity of the information and nature of work to be performed.

4.1.3	The terms and conditions of employment must document the responsibility of personnel for information and information systems security. a) Terms and conditions of employment for employees b) Terms and conditions of employment for non-employees c) Communication of terms and conditions of employment d) Violation of terms and conditions of employment

Purpose: To establish the terms and conditions of employment for information and information systems security.

4.1.3 a) Terms and conditions of employment for employees

The terms and conditions of employment for *employees* are defined in the PEI Public Service Commission Human Resource Policy and Procedures Manual (Section 5.0).

4.1.3 b) Terms and conditions of employment for non-employees

The terms and conditions of employment for personnel other than employees must include:

- Legal responsibilities and rights (e.g., laws relating to intellectual property rights, freedom of information and privacy);
- Confidentiality requirements that include responsibilities for the handling and storage of information assets; and,
- Consequences of failing to adhere to the terms and conditions.

4.1.3 c) Communication of terms and conditions of employment

Managers must ensure terms and conditions of employment are understood and agreed to by personnel prior to employment or provision of services.

4.1.3 d) Violation of terms and conditions of employment

Personnel in violation of the terms and conditions of employment are subject to disciplinary action including dismissal, cancellation of contract and/or other legal remedies.

4.2 Human Resources Security – During employment
4.2.1 Management must ensure personnel comply with security policies and procedures. a) Management responsibilities b) Review of security roles and responsibilities

Purpose: To establish management responsibilities for ongoing support and implementation of information security.

4.2.1 a) Management responsibilities

Managers must support the implementation of information security policies and practices by:

- Ensuring personnel are informed of information security roles and responsibilities prior to being granted access to information or information systems;
- Supporting and encouraging personnel to adhere to information security policies; and,
- Requiring that personnel conform to the terms and conditions of employment, including information security policies.

4.2.1 b) Review of security roles and responsibilities

Managers must annually review and validate security roles and responsibilities in job descriptions, standing offers, contracts and information use agreements and when:

- Staffing or restructuring public service or contract positions; or,
- Implementing new or significant changes to, information systems.

4.2.2 Personnel must receive appropriate information security training and be informed of changes to the Government Information Security Policy and practices. a) Orientation for new personnel b) Ongoing information security awareness, education and training

Purpose: To increase personnel awareness and understanding of security threats, *risks* and concerns and information security policies and procedures.

4.2.2 a) Orientation for new personnel

Managers must include an information security awareness component in orientation processes that personnel must complete prior to accessing information or information systems.

4.2.2 b) Ongoing information security awareness, education and training

Managers must provide ongoing information security awareness, education and training, addressing topics including:

- Protection of information;
- Known information security threats;
- Legal responsibilities;
- Information security policies and directives;
- Procedures for reporting information security events to the Office of Information Protection;
- Appropriate use of Government resources;
- Technology training;
- Information on disciplinary processes; and,
- How to obtain security advice.

4.2.3 Security breaches or policy violations caused by personnel must be reviewed by Management and reported to the Office of Information Protection.

a) Reviewing security breaches and policy violations and reporting to the Office of Information Protection.

Purpose: To ensure a process is in place to review the activities of personnel who commit a security breach or policy violation.

4.2.3 a) Reviewing security breaches and policy violations

Upon receipt of information identifying personnel responsible for a security breach or policy violation, managers are responsible for:

- Ensuring the Office of Information Protection has been informed of the potential security breach or policy violation;
- Assisting in an investigation and verifying the details of the security breach or policy violation;
- Determining, in consultation with the PEI Public Service Commission, if disciplinary action is warranted for employees;
- Determining if disciplinary action is warranted for non-employees; and,
- Arranging for permanent or temporary removal of access privileges when appropriate.

4.3 Human Resources Security – Termination or change of employment
4.3.1 Responsibilities for employment termination must be documented. a) Termination of employment responsibilities

Purpose: To ensure information security responsibilities upon termination of employment are defined and assigned.

4.3.1 a) Termination of employment responsibilities

Managers must advise personnel of ongoing confidentiality responsibilities that continue to apply after termination of employment.

4.3.2 Personnel must return Government assets upon termination or change of employment. a) Return of assets

Purpose: To ensure personnel return physical and information assets at termination of employment.

4.3.2 a) Return of assets

Managers must document the return of Government assets in the possession of personnel upon termination of their employment using standard processes. These processes must ensure the:

- Return of:
  - ✓ documents, files, data, books and manuals in physical or other *media* formats including other information assets developed or prepared by an employee or contractor in the course of their duties,
  - ✓ computer hardware, software and equipment (e.g., *mobile devices*, portable media), and
  - ✓ access devices, cards, vouchers and keys (e.g., credit cards, taxi cards, travel vouchers);
  - ✓ Returned items are verified against established asset inventories;
  - ✓ Recovery or compensation for assets not returned, based on established criteria regarding depreciation and replacement value for classes of items; and,
  - ✓ Identification of unreturned access devices, cards and keys that could permit unauthorized access or alteration/destruction of assets, so that information and/or security systems can be protected.

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

a) Change of employment status b) Action upon termination or change of employment c) Reduction of access rights

Purpose: To ensure physical and logical access rights to *information systems* and information processing facilities are managed in relation to the security responsibilities of the job requirements.

4.3.3 a) Change of employment status

Managers 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 commence long-term leave; and,
- Updating directories, documentation and systems.

4.3.3 b) Action upon termination or change of employment

Managers 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; and,
- Updating directories, documentation and systems.

4.3.3 c) Reduction of access right

Managers 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 employee/contactor or by management;
- The reason for termination;
- The current responsibilities of the employee/contractor; and,
- The value of the assets currently accessible.

Chapter 5 – Physical and Environmental Security

This chapter identifies requirements for the protection from environmental and man-made threats to personnel and property in information processing facilities. One of the principles used for protection is the use of security zones to place computers, people and information in secure areas. Safety measures for equipment installations are also described.

Requirements for the installation, operation, protection and maintenance of computer equipment are identified to preserve the confidentiality, integrity and availability of Government information and information systems.

5.1 Secure areas
5.1.1 Physical security perimeter Government information processing facilities must be protected by a physical security perimeter.
5.1.2 Physical entry controls Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
5.1.3 Securing offices, rooms and facilities Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.
5.1.4 Protecting against external and environmental threats Physical security controls must be designed to protect against damage from natural or man-made disaster.
5.1.5 Working in secure areas Additional security controls and procedures must be used by personnel working in secure areas.
5.1.6 Public access, delivery and loading areas Access to delivery and loading areas must be controlled, and where possible separated from information processing facilities.
5.2 Equipment security
5.2.1 Equipment sitting and protection Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.
5.2.2 Supporting utilities Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.
5.2.3 Cabling security Power and telecommunications cabling must be protected from interception and damage.
5.2.4 Equipment maintenance Equipment must be correctly maintained to enable continued availability and integrity.

5.2.5 Security of equipment off-premises Equipment must be protected using documented security controls when off-site from Government premises.
5.2.6 Secure disposal or re-use of equipment All data and software must be erased from equipment prior to disposal or re-deployment.
5.2.7 Removal of property Equipment, information or software belonging to the Province must not be removed from Government premises without prior authorization.

5.1	**Physical and Environmental Security – Secure areas**
5.1.1	Government information processing facilities must be protected by a physical security perimeter. a) Security perimeter b) Maintenance

Purpose: to prevent unauthorized physical access to Government information processing facilities.

5.1.1 a) Security perimeter

Information Owners and Information Custodians must establish the appropriate type and number of restricted zones to achieve the necessary conditions for personnel safety, and for the protection of, sensitive or valuable information and assets. Establishment of restricted zones must be supported by a *Threat and Risk Assessment*.

All information processing facilities are a *Restricted Access Security Zone*.

Appropriate security controls must be applied to reduce the level of identified *risks* and include:

- A structure that prevents external visual and audio observations and complies with all local building codes for structural stability (external walls, internal walls, ceilings and doors). Walls surrounding the facility must be extended from true floor to true ceiling (slab to slab), to prevent unauthorized entry and minimize environmental contaminations such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) must be applied to prevent unauthorized access;
- All information processing facilities must be equipped with physical intrusion alarm systems that automatically alert monitoring staff to take immediate action;
- Information processing facilities must be equipped with doors that close automatically. These doors must set off an audible alarm when kept open beyond a certain period of time;
- All fire doors must be equipped with crash bars to allow a quick exit in the event of an emergency.

When the doors are opened an audible alarm may also be set off;

- Alarm systems must be continuously monitored (i.e. 24 hours a day, 7 days a week);
- Access to restricted zones must be controlled, authorized and monitored as required by the applicable zone; and,
- Government information processing facilities must be physically separated from those managed by third parties.

5.1.1 b) Maintenance

Information Custodians must review, and where appropriate test, physical security and environmental control requirements annually.

Security requirements for facilities must be evaluated prior to significant:

- Alteration to building layouts;
- Change to equipment/systems located in the facility;
- Change in operations; and,
- As part of any related security incident investigation.

The effective use of restricted access zones in an open office environment depends on the implementation of appropriate security procedures, which may include:

- Respecting the need-to-access principle and zone perimeters;
- Escorting visitors;
- Securing sensitive or valuable information and assets when leaving the work areas; and,
- Taking precautions when discussing sensitive information.

Physical security for information processing facilities is the responsibility of the Information Custodian.

5.1.2 Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. a) Entry controls b) Maintenance

Purpose: To prevent unauthorized physical access to Government information

5.1.2 a) Entry controls

Access to any Government *information processing facility* or areas where sensitive information is kept must be restricted. Entry controls must identify, authenticate and monitor all access attempts to a *Restricted Access Operations Zone* or a *Restricted Access Security Zone* as follows:

- Every person authorized to enter a facility including visitors must be issued with an identification badge that contains identifying information (such as name and photograph) and their level of building access. Badge colour or some other bold identifier may be used to represent the level of access;
- All badges must be checked prior to entry. A receptionist, security guard or electronic reader that logs the identity, time, date, and access privileges of each entry attempt must do such checking. Entry control may be achieved using keys, proximity card readers or other technologies;
- Personnel must challenge anyone in a secure area who is not displaying an identification badge;

- Visitor or temporary access badges must be returned and accounted for at the end of each day;
- Entry logs must be reviewed on a quarterly basis;
- All entry logs must be secured and maintained according to the approved records retention schedule for the system or information asset; and,
- Access rights to secure areas must be reviewed and updated regularly.

5.1.2 b) Maintenance

Information Custodians are responsible for reviewing physical entry control requirements annually. All entry controls in place must be tested annually.

Security requirements for facilities must be evaluated prior to:

- Alteration to building layouts;
- Change to equipment/systems located in the facility;
- Change in operations; and,
- As part of any related security incident investigation.

5.1.3 Physical security requirements must be designed, documented and applied for all areas in and around an information processing facility.
a) Design considerations

Purpose: To enhance physical and environmental security of information processing facilities by considering all security requirements during the design of the facility.

5.1.3 a) Design considerations

Information Custodians must design, document and approve security controls for information processing facilities based on a *Threat and Risk Assessment*. Considerations must include:

- Determining security perimeter and maintenance factors;
- Establishing appropriate *security zones*;
- Design and construction complying with health and safety regulations and standards;
- Selecting unobtrusive sites and keep signage to the minimum required for meeting fire and other safety requirements;
- Limiting the identification of information processing facility locations, in publicly and internally available directories, to the minimum required; and,
- Selecting sites so that public access can be strictly controlled or avoided.

5.1.4 Physical security controls must be designed to protect against damage from natural or man- made disaster.

a) Design and site selection

Purpose: To enhance physical and environmental security by designing and applying physical security controls to protect against damage from natural or man-made disaster.

5.1.4 a) Design and site selection

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

- Combustible or hazardous materials must be stored at a safe distance from the secure area. Bulk supplies must not be stored within the secure area;
- Installing intrusion and environmental alarm systems, fire suppression and fire fighting systems; and,
- Fallback equipment (e.g., for DRP) and backup media must be sited at a safe distance to avoid damage from a disaster affecting the main site.

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

a) Secure area requirements for personnel

b) Other secure area requirements

Purpose: To prevent unauthorized physical access to Government information by designing and applying additional security controls and procedures for employees working in secure areas.

5.1.5 a) Secure area requirements for personnel

Information Owners and Information Custodians must identify and document requirements that apply to personnel authorized to work in secure areas. Information Owners and Information Custodians are responsible for informing personnel working within a secure area that:

- Activities within a secure area are confidential and must not be discussed in a non-secure area, or with persons who do not have a need-to-know;
- Sensitive information must not be discussed with persons without a need-to-know;
- No type of photographic (including cameras in mobile devices), video, audio or other recording equipment is to be brought into a *Restricted Access Security Zone* unless authorized; and,
- Input and feedback to strengthen security controls is encouraged.

5.1.5 b) Other secure area requirements

Information Owners and Information Custodians must identify and document requirements for

other individuals who may need access to a secure area. Information Owners and Information Custodians are responsible for ensuring that:

- ❖ Maintenance staff, cleaners and others who may require access on an ongoing basis to the secure area must be screened and their names placed on access lists; and,
- ❖ Visitors must obtain approval for visits, be appropriately screened, and their entry and departure times logged. Personnel must escort visitors when they are within the secure area.

Unoccupied secure areas must be physically locked and periodically checked. Physical intrusion alarms must be installed to automatically alert monitoring staff of a breach.

5.1.6 Access to delivery and loading areas must be controlled, and where possible separated from information processing facilities. a) Controlling access to delivery and loading areas b) Security controls for co-located information processing facilities and loading areas

Purpose: To prevent unauthorized physical access to Government information by controlling access to delivery and loading areas and separating them from information processing facilities whenever possible.

5.1.6 a) Controlling access to delivery and loading areas

Information Custodians, planners and architects must ensure that access to delivery and loading areas or *Reception Zone* is controlled when considering building design and specifications. The following factors must be considered:

- ❖ Delivery and loading areas must be designed so that supplies can be unloaded without delivery personnel gaining access to *restricted access zones* or other parts of the building;
- ❖ A combination of internal and external locking doors or gates must be used to provide security;
- ❖ Incoming material must be inspected for potential threats before being moved to or from the delivery and loading area. Inspections can be undertaken randomly if resources are not available to inspect every package;
- ❖ Bills of lading must be compared to goods delivered
- ❖ Loading docks and delivery areas must be regularly inspected and actively monitored; and,
- ❖ Records must be kept for deliveries and pick-ups.

For leased facilities that include delivery and loading areas, a *Threat and Risk Assessment* and inspection prior to leasing should be conducted to determine that access can be adequately controlled.

5.1.6 b) Security controls for co-located information processing facilities and loading areas.

When delivery and loading areas are not separate from information processing facilities or other secure areas the following security controls shall be considered:

- Physical controls (e.g., locked doors) that secure the external doors of a delivery and loading area when the internal doors are opened;
- Setting and maintaining hours of operation for delivery and pick-up;
- Continuous monitoring of the access to information processing facilities;
- Continuous monitoring of the delivery and loading areas, and,
- Records must be kept for deliveries and pick-ups.

5.2	**Physical and Environmental Security – Equipment security**
5.2.1	Equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards. a) Equipment sitting b) Equipment protection

Purpose: To reduce *risks* to equipment from unauthorized access, environmental threats and hazards.

5.2.1 a) Equipment sitting

Information Owners, Information Custodians, planners, and architects must collaborate to ensure that the design and layout of information processing facilities provides protection from security threats as supported by a *Threat and Risk Assessment*. Safeguards must include:

- Locating servers and other centralized computing equipment within a *Restricted Access Security* Zone;
- Locating work stations, laptops and printers in an Restricted Access Operations Zone;
- Protecting information processing equipment from observation by unauthorized persons, including by observing through windows and walking through work areas; and,
- Locating shared printers, scanners, copiers, and facsimile machines away from public or reception areas, or in passageways or other areas where users who do not have a need-to-know can access printed material.

Information Owners and Information Custodians are responsible for ensuring that kiosks and public terminal safeguards are based on a Threat and Risk Assessment and reviewed annually.

5.2.1 b) Equipment protection

Information Owners, Information Custodians, planners, and architects must collaborate to

ensure that the design and layout of information processing facilities provides protection from physical and environmental hazards. Safeguards must include:

- Using equipment designed for suppression of electromagnetic emanations that may be used to capture information, when the need is supported by a Threat and Risk Assessment;
- Ensuring that equipment is properly vented and that the temperatures and humidity in information processing facilities are appropriate for operating equipment safely;
- Providing lightning protection for information processing facilities which includes surge protection for power and communications;
- Assessing and protecting equipment to minimize damage from fire suppression and other safety systems;
- Protecting equipment from potential damage from environmental hazards such as water, dust, vibration, and sunlight;
- Providing personnel with approved eating and drinking areas separate from work areas containing equipment;
- Briefing personnel who work with equipment about safety practices in the workplace;
- Keeping information processing facilities free of biological pests that pose hazards to equipment and power systems; and,
- Regularly inspecting the information processing facility(s) for integrity of ceilings, walls, windows, and other infrastructure for damage from water and other environmental factors that may pose a threat to safe equipment operation.

5.2.2 Equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities. a) Planning and design b) Maintenance

Purpose: To ensure continued availability by protecting equipment from disruptions caused by failures in supporting utilities.

5.2.2 a) Planning and design

Information Custodians, planners, architects and engineers must collaborate in the planning and design of an *information processing facility* to ensure that supporting utilities (e.g., water, power, sewage, heating, ventilation) are adequate to support personnel and systems that will be located in the facility. This includes estimating current and future utility capacity requirements for the facility. In addition to meeting the building code and other regulations, the following shall be included in facility planning and specifications:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;

- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems;
- Multiple connections to the power utility for critical systems and equipment;
- Multiple telecommunications connections to prevent loss of voice services; and,
- Adequate voice communications to meet regulatory requirements for emergencies.

5.2.2 b) Maintenance

Information Custodians must ensure that facilities are inspected regularly in accordance with building codes and other regulations. Evacuation and other emergency drills must be practiced regularly in collaboration with fire and emergency services. The facility requirements for utilities shall be re-evaluated:

- During the planning phase for replacing or changing existing technology hardware;
- When moving significant numbers of new staff into facilities;
- During the planning of renovations or major changes to an existing facility;
- Prior to leasing a facility; and,
- When there are major changes to the surrounding area that may affect utilities, evacuation routes or other safety aspects.

5.2.3 Power and telecommunications cabling must be protected from interception and damage. a) Protection b) Inspection and monitoring

Purpose: To ensure continued availability and integrity by protecting power and telecommunications cabling from interception and damage.

5.2.3 a) Protection

Information Custodians, planners and architects must include the protection of power and telecommunications cabling from interception and damage when designing or leasing facilities. The following methods can increase protection:

- Power and telecommunications cabling must be underground and/or in a secure conduit;
- Power cables should be protected with electromagnetic shielding;
- When supported by a *Threat and Risk Assessment*, consideration must be given to use of fibre optics for telecommunications cabling;
- Cables must not be accessible in public areas;

- Power and telecommunications cabling must be segregated in accordance with building codes and other regulations; and,

- Inspection boxes, termination points, patch panels, control rooms and other facilities must be secured and located inside a *Restricted Access Security Zone*.

5.2.3 b) Inspection and monitoring

Information Custodians must ensure that:

- The integrity of power and telecommunications cables are monitored through regular inspections and reports;
- Records of patches and other changes are maintained and inspected for completeness and correctness; and,
- Power and telecommunications cabling and wiring closets are inspected regularly and monitored for unauthorized access or inappropriate activity. The frequency of monitoring activities must be supported by a Threat and Risk Assessment.

5.2.4 Equipment must be correctly maintained to enable continued availability and integrity. a) Routine maintenance b) Maintenance of systems, hardware or media containing Government information

Purpose: To ensure the continued availability and integrity of equipment through correct maintenance.

5.2.4 a) Routine maintenance

Equipment being repaired or maintained must be protected commensurate with the sensitivity of the information it contains and the value of the equipment. Information Owners and Information Custodians must determine if repair or maintenance can be conducted off-site. The need to protect sensitive information may justify equipment destruction and replacement rather than repair or maintenance.

Information Custodians are responsible for:

- Ensuring the scheduling of routine, preventive maintenance of equipment by qualified, authorized personnel;
- Ensuring that maintenance is performed in accordance with the manufacturer's specifications, in compliance with warranty requirements, and using safe practices as specified in building codes, other regulation and insurance policies;
- Ensuring that, where possible, maintenance is scheduled to avoid interference with services or operations;
- Notifying affected users prior to taking equipment off-line for scheduled maintenance;

Ensuring that the value and sensitivity of the information contained on the device is considered prior to approval of off-site maintenance. Equipment sent for off-site maintenance must be inspected and logged out;

- ❖ Ensuring that equipment returning from off-site repair or maintenance is inspected and logged in; and,
- ❖ Maintaining detailed records to identify trends, weaknesses and additional maintenance requirements which must include:
  - ✓ Place, date, time, type of scheduled maintenance and technical staff,
  - ✓ Suspected and actual *fault*s identified,
  - ✓ Diagnostics performed and corrective action taken,
  - ✓ Unusual or unexpected events, such as early failures or breakdowns, and,
  - ✓ Any other event that requires maintenance.

5.2.4 b) Maintenance of systems, hardware or media containing Government Information Security Policy information

Information Custodians must consult with Information Owners regarding the value and sensitivity of the information stored on hardware or media when determining whether repairs will be conducted.

Information Custodians must ensure that information is safeguarded and:

- ❖ Maintenance on critical systems is undertaken in such a manner that the system is not off-line due to scheduled maintenance;
- ❖ Maintenance is factored into system availability requirements; and,
- ❖ Repair or maintenance is conducted within Canada.

5.2.5 Equipment must be protected using documented security controls when off-site from Government premises.
a) Authorized use
b) Security controls

Purpose: To protect equipment in the custody of personnel from loss or unauthorized access.

5.2.5 a) Authorized use

Information Owners and Information Custodians must authorize and document off-site use of equipment. Equipment for off-site usage may include:

- ❖ Desktop and laptop computers;
- ❖ *Portable storage devices*;
- ❖ Mobile devices; and,
- ❖ Printers, scanners, copiers and facsimiles.

5.2.5 b) Security controls

Information Owners and Information Custodians must ensure that Government equipment being used off- site is protected commensurate with the sensitivity of the information it contains and the value of the equipment.

Information Custodians must ensure that:

- Sensitive data is encrypted where supported by a *Threat and Risk Assessment*;
- Equipment is protected from unauthorized access by the use of a logical or physical access control mechanism (e.g., password, USB key or smart card);
- Equipment is protected from loss with a physical locking, restraint or security mechanism when appropriate; and,
- *Personnel* are familiar with operation of the protection technologies in use.

To provide further protection personnel must:

- Not leave Government equipment unattended in a public place;
- Ensure that equipment is under their direct control at all times when travelling;
- Use the physical locking, restraint or security mechanisms provided by the Information Custodian whenever possible;
- Take measures to prevent viewing of sensitive information other than by authorized persons;
- Not permit other persons to use the equipment; and,
- Report loss of equipment immediately using the Lost or Stolen Computer or Electronic Storage Device Report

5.2.6 Information, records and software must be protected against unauthorized disclosure when hardware and media are reassigned or destroyed. a) Reassignment of hardware and media b) Destruction of hardware

Purpose: To protect information from unauthorized disclosure.

5.2.6 a) Reassignment of hardware and media

Information Owners must consider the value and sensitivity of the information stored on hardware or media when determining whether it will be reassigned within Government or destroyed.

Prior to reassignment of hardware or media within Government, Information Owners and Information Custodians must ensure:

- That the integrity of the Government records is maintained by adhering to Records Management policies;
- Information and software is erased using methods and standards approved by the Office of the Information Protection;
- Roles and responsibilities are documented; and,

- Asset inventories are updated to record details of the erasure and reassignment including:
  - ✓ Asset identifier,
  - ✓ Date of erasure,
  - ✓ Names of personnel conducting the erasure,
  - ✓ Date of transfer, and,
  - ✓ Name of new asset custodian.

Where information is erased by third parties there must be contractual and audit procedures to ensure complete destruction of the information. Third parties must certify that destruction has occurred.

5.2.6 b) Destruction of hardware

Information Owners and Information Custodians are responsible for ensuring hardware media used to store information or software is destroyed in a secure manner.

Warranty repairs or servicing for hardware used to store information or software must be sent to a Government approved site in a secure manner.

Hardware must be destroyed if the integrity of the information cannot be ensured during warranty repairs and servicing. (e.g., work done outside Canada (Refer to GISP 5.2.4)).

5.2.7 Equipment, information or software belonging to the Province must not be removed from Government premises without prior authorization.
a) Authorized removal of assets

Purpose: To protect *assets* belonging to the Province from unauthorized removal.

5.2.7 a) Authorized removal of assets

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

- Description and serial numbers;
- Information about where the asset will be located;
- The removal date and return date;
- The identity of the individual responsible for the asset; and,
- Reason for removal of the asset.

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 (e.g., Terms and Conditions of Use).

Personnel removing assets from Government premises should be challenged to present an authorization for removal.

Personnel removing assets without authorization may be subject to disciplinary action.

Chapter 6 – Communications and Operations Management

This chapter establishes a framework to support the integration of information security in the services provided by Government information processing facilities.

Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide services. Services can be delivered by external parties and by computer networks and by all services that exchange information. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve.

Controls for operations include documented processes, staff duties and formal methods to implement changes to facilities. This includes: methods to protect information, create copies for back-up and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

6.1 Operational procedures and responsibilities
6.1.1 Documented operating procedures Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained.
6.1.2 Change management Changes to information systems and information processing facilities must be controlled.
6.1.3 Segregation of duties Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems.
6.1.4 Separation of development, test and operational facilities Development and test information systems must be separated from operational information systems.
6.2 Third party service delivery management
6.2.1 Service delivery Prior to using external information and technology services, security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.
6.2.2 Monitoring and review of third party services Government must regularly monitor and review services, reports and records provided by external parties and carry out regular audits.
6.2.3 Managing changes to third party services Change management processes for information system services delivered by external parties must take into account the criticality of the information systems, processes involved and assessment of risks.
6.3 System planning and acceptance
6.3.1 Capacity management

The use of information system resources must be monitored, optimized and projections made of future capacity requirements.
6.3.2 System acceptance Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
6.4 Protection against malicious and mobile code
6.4.1 Controls against malicious code Security awareness, prevention and detection controls must be utilized to protect information systems against malicious code.
6.4.2 Controls against mobile code Mobile code must be restricted to the intended information system or environment.
6.5 Back-up
6.5.1 Information back-up Information and information systems must be backed up and the recovery process tested regularly.
6.6 Network Management
6.6.1 Network controls A range of controls must be implemented to achieve and maintain security within the Government network.
6.6.2 Security of network services Security features, service levels and management requirements of all network services must be documented and included in any network service agreement.
6.7 Media Handling
6.7.1 Management of removable computer media All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.
6.7.2 Disposal of media Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.
6.7.3 Information handling procedures Media must be handled and stored so as to prevent unauthorized information disclosure or misuse.
6.7.4 Security of system documentation Systems documentation must be protected from unauthorized access.
6.8 Exchanges of information
6.8.1 Information exchange 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.
6.8.2 Exchange agreements Information and software exchange agreements between the Province and other organizations must be documented.
6.8.3 Physical media in transit

Media being physically transported must be appropriately protected.
6.8.4 Electronic messaging Information transmitted by electronic messaging must be appropriately protected.
6.8.5 Business information systems Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems.
6.9 Electronic commerce services
6.9.1 Electronic commerce Information in electronic commerce information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.
6.9.2 On-Line Transactions Information systems utilizing on-line transactions must have security controls commensurate with the value and sensitivity of the information.
6.9.3 Publicly available information Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.
6.10 Monitoring
6.10.1 Audit logging Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.
6.10.2 Monitoring system use The use of information systems must be monitored and the result of the monitoring activities must be regularly reviewed.
6.10.3 Protection of log information Information system logging facilities and log information must be protected against tampering and unauthorized access.
6.10.4 Administrator and operator logs Activities of privileged users must be logged, and the log must be subject to regular independent review.
6.10.5 Fault logging Faults must be logged, analyzed and appropriate action taken.
6.10.6 Clock synchronization Computer clocks shall be synchronized for accurate reporting.

6.1	**Communications and Operations Management – Operational procedures and responsibilities**
6.1.1	Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained. a) Operating procedures

Purpose: To ensure correct operations of information systems and information processing facilities.

6.1.1 a) Operating procedures

Information Custodians must ensure that approved operating procedures and standards are:

- Documented;
- Consistent with Government policies;
- Reviewed and updated annually;
- Reviewed and updated when there are:
  - ✓ Alterations to building layouts,
  - ✓ Changes to equipment/systems located in the facility, and,
  - ✓ Changes in business services and the supporting information systems operations; and,
  - ✓ Reviewed and updated as part of any related security incident investigation.

Operations documentation must contain detailed instructions regarding:

- Information processing and handling;
- System re-start and recovery;
- Back-up 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; and,
- Operations, technical, emergency and business contacts

6.1.2 Changes to information systems and information processing facilities must be controlled.

a) Change management process
b) Planning changes
c) Implementing changes

Purpose: To ensure changes to information systems and facilities are applied correctly and do not compromise the security of *information* and *information systems*.

6.1.2 a) Change management process

Information Owners and Information Custodians must document and implement a change management process to control changes by:

- Identifying and recording significant changes;
- Assessing the potential impact, including the security impact, of the change;
- Obtaining approval of changes from the manager(s) responsible for the information system;
- Planning and testing changes including documenting fallback procedures;
- Communicating change details to relevant personnel; and,
- Evaluating that planned changes were performed as intended.

6.1.2 b) Planning changes

Information Owners and Information Custodians must plan for changes by:

- Assessing the 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 third parties including information sharing agreements, Memoranda of Understanding, licensing and provision of services;
- Preparing change implementation plans that include testing and contingency plans in the event of problems;
- Obtaining approvals from affected Information Owners and Information Custodians; and,
- Training technical staff and operations staff if required.

6.1.2 c) Implementing changes

Information Owners and Information Custodians must implement changes by:

- Notifying affected parties, including business partners and third parties;
- Training users if required;
- Documenting and reviewing the documentation throughout the testing and implementation phases;

- ❖ Recording all pertinent details regarding the changes; and,
- ❖ Checking after the change has been performed that only the intended changes took place.

6.1.3 Duties and areas of responsibility must be segregated to reduce opportunities for unauthorized modification or misuse of information systems. a) Segregation of duties b) Critical or sensitive information systems

Purpose: To reduce *risk* of loss, fraud, error and unauthorized changes to information.

6.1.3 a) Segregation of duty

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

- ❖ Requiring complete and accurate documentation for every information system;
- ❖ Rotating job duties periodically to reduce the opportunity for single individuals to have sole control and oversight on key systems; where possible;
- ❖ Automating functions to reduce the reliance on human intervention for information systems;
- ❖ Requiring that individuals authorized to conduct sensitive operations do not audit those operations;
- ❖ Requiring that individuals responsible for initiating an action are not also responsible for authorizing that action; and,
- ❖ Implementing information systems security controls to minimize opportunities for collusion.

6.1.3 b) Critical or sensitive information systems

Where supported by a *Threat and Risk Assessment* or other formal assessment Information Owners and Information Custodians must employ *two person access control* to preserve the integrity of the information system.

6.1.4 Development and test information systems must be separated from operational information systems. a) Separation requirements

Purpose: To reduce the *risk* of unauthorized or inadvertent changes to operational *information systems* or information systems under development or being tested.

6.1.4 a) Separation requirements

Information Custodians must protect operational information systems by:

- ❖ Separating operational environments from test and development environments ;

- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified personnel;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;
- Prohibiting the use of operational data in development, test or training information systems; and,
- Prohibiting the use of personal information in development, test or training information systems.

6.2	**Communications and Operations Management – External service delivery management**
6.2.1	Prior to using external information and technology services, security controls, service definitions and delivery levels must be identified and included in the agreement with the external party. a) Identifying security requirements in procurement b) Service level continuity

Purpose: To ensure service agreements with external parties specify requirements for security and service level continuity.

6.2.1 a) Identifying security requirements in procurement documents

Information Owners and Information Custodians must include security requirements in procurement documents for *information* and *information system* services being delivered by external parties.

Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and,
- Developing transition and fall back plans (e.g., migration from one service provider to another).

6.2.1. b) Service level continuity

Information Owners and Information Custodians must ensure service agreements with external parties document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process owners;
- Audit and compliance monitoring rights and responsibilities;

- ❖ Communicating requirements to service providers;
- ❖ Obtaining periodic confirmation from service providers that adequate capacity is maintained; and,
- ❖ Reviewing the adequacy of the service provider's contingency plans for responding to disasters or major service failures.

6.2.2 Government must regularly monitor and review services, reports and records provided by external parties and carry out regular audits.
a) Monitoring and review of external party services

Purpose: To ensure that services delivered by external parties maintain compliance with security and audit requirements.

6.2.2 a) Monitoring and review of external party services

Information Owners and Information Custodians must establish processes to manage and review the information security of external party delivered services by:

- ❖ Assigning responsibility for monitoring to a designated staff member;
- ❖ Maintaining an inventory of agreements and associated access rights;
- ❖ Monitoring for compliance through processes such as:
  - ✓ Conducting internal self Assessment of control processes,
  - ✓ Requiring external parties conduct and submit self Assessment,
  - ✓ Using embedded audit tools,
  - ✓ Requiring external parties to submit annual management assertions that controls are being adhered to,
  - ✓ Conducting independent security reviews, audits and updates to *Security Reviews*, and, Analysis of *audit logs*; and,
  - ✓ Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents.

6.2.3 Change management processes for information system services delivered by external parties must take into account the criticality of the information systems, processes involved and assessment of risks.
a) Change management

Purpose: To ensure that changes to *information system* services delivered by external parties maintain or enhance security controls.

6.2.3 a) Change management

Information Owners and Information Custodians must ensure agreements with external party service providers include provisions for:

- ❖ Amending agreements when required by changes to legislation, regulation, business requirements, policy or service delivery; and,

- Requiring the service provider to obtain pre-approval for significant changes involving:
  - ✓ Network services,
  - ✓ New technologies,
  - ✓ Use of new or enhanced system components (e.g., software or hardware),
  - ✓ System development, test tools and facilities,
  - ✓ Modification or relocation of the physical facilities, and,
  - ✓ Sub-contracted services.

Information Owners and Information Custodians must ensure the change management process for information systems services delivered by external parties includes, as required:

- Reviewing and updating the *Threat and Risk Assessment* to determine impacts on security controls;
- Implementing new or enhanced security controls where identified by the risk assessment;
- Reviewing and updating the *Privacy Impact Assessment*;
- Initiating and implementing revisions to policies and procedures; and,
- Revising personnel awareness and training programs.

6.3	**Communications and Operations Management – System planning and acceptance**
6.3.1	The use of information system resources must be monitored, optimized and projections made of future capacity requirements. a) Resource *capacity management* b) Resource capacity planning

Purpose: To reduce the *risk* of system failures and unacceptable performance levels by monitoring and optimizing resources to meet current and future information system capacity requirements.

6.3.1 a) Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes,
- Including capacity requirements in service agreements;
- Monitoring and optimizing *information systems* to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
  - ✓ New business and information systems requirements,
  - ✓ Statistical or historical capacity requirement information, and,
  - ✓ Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

6.3.1 b) Resource capacity planning

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

6.3.2 Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
- a) System acceptance process
- b) System acceptance criteria
- c) *Security certification*

Purpose: To ensure that new or upgraded *information systems* are tested against defined, agreed and documented criteria for acceptance, prior to becoming operational.

6.3.2 a) System acceptance process

Information Owners must ensure that definition of system acceptance criteria are included as part of the system development and acquisition process.

Prior to implementing new or upgraded information systems, Information Owners and Information Custodians must ensure:

- ❖ Acceptance criteria are identified including privacy, security, systems development and user acceptance testing; and
- ❖ Security certification is attained, indicating the system meets minimum acceptance criteria

6.3.2 b) System acceptance criteria

Information Owners and Information Custodians must document system acceptance criteria, including:

- ❖ Projected performance and resource capacity requirements;
- ❖ Disaster recovery, restart, and contingency plans and procedures;
- ❖ Impact on standardized 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;
- ❖ Business continuity arrangements;
- ❖ Training requirements; and,
- ❖ User acceptance testing.

6.3.2 c) Security certification

The Information Owners and Information Custodians must receive assurance that a new or updated information system meets minimum security acceptance criteria.

Assurance should be obtained by conducting either an independent *Threat and Risk Assessment* or a *Security Review* which determines whether a system includes adequate controls to mitigate security *risks*. This process will also determine the effect of the new system on the overall security of Government information systems.

6.4	Communications and Operations Management – Protection against malicious and *mobile code*
6.4.1	Security awareness, prevention and detection controls must be utilized to protect information systems against *malicious code*. a) Prevention and detection controls b) User awareness

Purpose: To protect the integrity of information systems and software through requirements for the prevention and detection of malicious code.

6.4.1 a) Prevention and detection controls

Information Custodians must protect Government *information systems* from malicious code (e.g., viruses, worms) by undertaking such activities as:

- Installing, updating and consistently using software (e.g., anti-virus or anti-spyware software) designed to scan for, detect and provide protection from malicious code;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malicious code before use; and,
- Maintaining business continuity plans to recover from malicious code incidents.

The Chief Information Security Officer must ensure processes are implemented to:

- Maintain a critical incident management plan to identify and respond to malicious code incidents; and,
- Maintain a register of specific malicious code countermeasures (e.g., blocked websites, blocked electronic mail attachment file types and blocked network ports) including a description, the rationale, the approval authority and the date applied.

6.4.1 b) User awareness

The Office of Information Protection is responsible for developing user awareness programs for malicious code countermeasures.

The Office of Information Protection is responsible for communicating technical advice and providing information and awareness activities regarding malicious code.

6.4.2 Mobile code must be restricted to the intended information system or environment. a) Mobile code categorization b) Restrictions on mobile code

Purpose: To protect information systems from malicious mobile code.

6.4.2 a) Mobile code categorization

The Chief Information Security Officer must establish processes for categorizing mobile code *technologies* to identify *risk* and restrict use based on potential to cause damage or be used maliciously.

Proposals for the use of new and emerging mobile code *technologies* must be referred to the Office of the Information Protection prior to use.

6.4.2 b) Restrictions on mobile code

Information Owners must ensure Information Custodians permit access to, or use of, mobile code if required for business functions. Methods to restrict or contain mobile code include:

- Compartmentalization of mobile code execution to a logically isolated environment;
- Blocking receipt or execution of mobile code; and,
- Restricting system resources available to the mobile code.

User (client) systems must be configured to warn users of mobile code risks and prompt them to consider risks prior to opening files or e-mail attachments that may contain mobile code.

Mobile code authored by the province must be:

- Digitally signed;
- Published on an authorized, trustable source; and
- Transmitted to client systems over encrypted channels.

6.5	**Communications and Operations Management – Back-up**
6.5.1	Information and information systems must be backed up and the recovery process tested regularly. a) Defining requirements b) Safeguarding backup facilities and media c) Testing

Purpose: To enable the timely recovery of *information* and *information systems.*

6.5.1 a) Defining requirements

Information Owners and Information Custodians must define and document backup and recovery processes that reflect the sensitivity and availability requirements of *information* and *information systems* including:

- Confirming that the backup and recovery strategy complies with:
  - ✓ Business continuity plans,
  - ✓ Policy, legislative, regulatory and other legal obligations, and,
  - ✓ Records management requirements.

- Documenting the backup and recovery process including:
  - ✓ Types of information to be backed up
  - ✓ Schedules for the backup of information and information systems,
  - ✓ Backup media management (e.g. retention period, pattern of backup cycles),
  - ✓ Methods for performing, validating and labeling backups, and
  - ✓ Methods for validating recovery of the information and information system.

6.5.1 b) Safeguarding backup facilities and media

Information Custodians must conduct a *Threat and Risk Assessment* to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards include:

- Using encryption to protect the backed up information;
- Using digital signatures to protect the integrity of the information;
- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

6.5.1 c) Testing

Information Custodians must regularly test backup and recovery processes.

6.6	**Communications and Operations Management – Network security management**
6.6.1	A range of controls must be implemented to achieve and maintain security within the Government network. a) Control and management of networks b) Configuration control c) Secured path d) Wireless Local Area Networking e) Equipment management f) Logging, monitoring and detection g) Coordination and consistency of control implementation

Purpose: To ensure that network security controls and network security management practices are implemented and documented to protect the *network infrastructure*, information traversing the network, and network-attached information systems.

6.6.1 a) Control and management of networks

Information Custodians must implement network infrastructure security controls and security management systems for networks to ensure the protection of information and attached *information systems*.

Selection of controls must be based on a *Threat and Risk Assessment*, taking into account the information sensitivity determined by the Information Owners, and applicability to the network technology.

The Threat and Risk Assessment must consider network-related assets which require protection including:

- Information in transit;
- Stored information (e.g., cached content, temporary files);
- Network infrastructure;
- Network configuration information, including device configuration, access control definitions, routing information, passwords and *cryptographic keys*;
- *Network management information*;
- *Network pathways and routes*;
- Network resources such as bandwidth;
- Network security boundaries and perimeters; and,
- Information system interfaces to networks.

6.6.1 b) Configuration control

To maintain the integrity of networks, Information Custodians 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 controls such as:

- Encryption;
- Access controls and multi-factor *authentication*;
- Monitoring of access;
- Configuration change logs;
- Configuration baselines protected by cryptographic checksums; and,
- Regular backups.

Status accounting must be regularly performed to ensure that configuration baselines reflect actual device configuration.

6.6.1 c) Secured path

Where required by sensitivity of information or a Threat and Risk Assessment, information must only be transmitted using a *secured path.*

Secured paths for information transmission must use controls such as:

- Data, message or session encryption, such as SSH, SSL or VPN tunnels; and,
- Systems to detect tampering.

6.6.1 d) Wireless Local Area Networking

Wireless Local Area Networks must utilize the controls specified by the Chief Information Security Officer and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access;
- User and device network access controlled by Government authentication services;
- The use of strong, frequently changed, automatically expiring encryption keys and passwords;
- Segregation of wireless networks from wired networks by the use of filters, firewalls or proxies; and,
- Port-based access control, for example use of 802.1x technology.

Where supported by a Threat & Risk Assessment, additional controls for wireless networks may

include:

- Virtual Private Network tunnel technology;
- The use of Desktop Terminal Services (DTS) technology; and,
- Intrusion detection systems, firewalls and Media Access Control (MAC) address filtering.

6.6.1 e) Equipment management

Information Custodians must document responsibilities and procedures for operational management of network infrastructure, including devices at network boundaries and in user areas.

6.6.1 f) Logging, monitoring and detection

To facilitate monitoring, response and investigation, logging to a centralized log management service must be enabled, including logging of:

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

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

Information Custodians must ensure there is a clear segregation of duties for personnel involved in logging, monitoring or detection activities.

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

Sensors enabling on-demand capture of network traffic must be implemented at network security boundaries and within networks housing sensitive information or information systems as determined by a Threat and Risk Assessment.

6.6.1 g) Coordination and consistency of control implementation

Information Owners and Information Custodians must document network security controls in the *System* Security Plan including:

- A summary of *risks* identified in the Threat and Risk Assessment;
- Roles and responsibilities for network security management;
- Specific procedures and standards used to mitigate risks and protect the network;

- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures (including monitoring frequency, review and remediation processes).

6.6.2 Security features, service levels and management requirements of all network services must be documented and included in any network service agreement. a) Network service agreement

Purpose: To specify what security features are required for delivery of a network service.

6.6.2 a) Network service agreement

Formal *network service agreements* must be established between *network service providers* and consumers of network services to specify service levels, services offered, security requirements and security features of network services.

The network service agreement must include specification of:

- The rules of use to be followed by consumers to maintain the security of network services;
- The schedule for ongoing verification of network security controls;
- The rights of either party to monitor, audit or investigate as needed;
- Security incident response responsibilities, contacts and procedures; and,
- The requirement to meet or exceed Government security policy and standards.

Information Owners and Information Custodians must confirm that the specified security features are implemented prior to commencement of service delivery.

6.7	**Communications and Operations Management – Media handling**
6.7.1	All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media. a) Management of Government records b) Use of portable storage devices c) Human factors d) Risk assessment factors and controls e) Mandatory controls

Purpose: To ensure that *risks* to information introduced by portable storage devices are sufficiently managed.

6.7.1 a) Management of Government records

The Public Archives and Records Office Recorded Information Management Unit delivers a corporate program that provides central recorded information management services and support to all departments, agencies, corporations and commissions within the Government of

Prince Edward Island. It also audits and monitors the development and maintenance of recorded information management programs in departments. This is all governed by the *Archives and Records Act.*

6.7.1 b) Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments.

Information Owners, Information Custodians and Managers must:

- Ensure that use of portable storage devices is managed and controlled to mitigate risks;
- Document processes for authorizing use of portable storage devices; and,
- Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity, a *Threat and Risk Assessment* must be performed prior to permitting the use of a class of portable storage devices.

Technical standards for each class of media must be documented including mandatory controls, permitted information sensitivity and strength of controls such as encryption key length.

6.7.1 c) Human factors

Information Owners, Information Custodians *and Managers* must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with operation of the required protection technologies and when they must be used; and,
- Familiar with security event and loss reporting procedures.

6.7.1 d) Risk assessment factors

The Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media destruction;
- Improper long term storage environment;
- Exposure to malicious and mobile code; and,
- Incomplete erasure of data prior to device disposal.

Information sensitivity must be considered in the risk assessment.

6.7.1 e) Mandatory controls

Minimum information protection safeguards for the use of portable storage devices include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Not storing the only version of a document on portable storage devices;
- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices;
- Adherence to manufacturer specifications for media storage environment; and,
- Documented portable storage devices handling procedures including:
  - ✓ Off-site storage,
  - ✓ Third party transportation,
  - ✓ Information backup,
  - ✓ Prevention of mobile and malicious software,
  - ✓ Logging of media custody and location to allow for accounting and audit,
  - ✓ Media labeling to indicate owner and special handling restrictions,
  - ✓ Maintenance of information where the information storage requirement exceeds the expected media lifetime, and,
  - ✓ Secure erasure and disposal.

6.7.2 Media must be disposed of securely and in a manner appropriate for the sensitivity of the data contained on the media.

a) Secure disposal of media

Purpose: To ensure that information cannot be retrieved from media that is no longer in use.

6.7.2 a) Secure disposal of media

Information Owners and Information Custodians must ensure that media that is no longer required operationally (e.g., due to expiry, surplus, damage or wear), is disposed of securely. Prior to disposal, the Departmental Records Management Liaison Officer must be consulted. Media disposal procedures must:

- Be documented and communicated to personnel;
- Specify erasure and disposal measures whose strength is based on information sensitivity and type of media (e.g., erasure software);
- Include secure destruction of media if erasure is not sufficient, or not cost effective (e.g., destruction by shredding, incineration or chemical dissolution);
- Include secure storage measures for media collected for and awaiting erasure or disposal, to avoid undetected theft of small amounts of media from large volumes

awaiting disposal; and,
- ❖ Include audit logs of media disposal.

The Information Access Operations, Shared Services PEI is responsible for ensuring secure disposal services are available to Information Owners and Information Custodians.

6.7.3 Media must be handled and stored so as to prevent unauthorized information disclosure or misuse. a) Media handling procedures

Purpose: To ensure that documented procedures are used for handling and storage of media in accordance with the sensitivity of information stored on the media.

6.7.3 a) Media handling procedures

Information Owners and Information Custodians must document media handling procedures that are compliant with the information sensitivity and handling requirements for information stored on the media.

If information of various sensitivities is stored on media, the media must be handled according to the highest sensitivity of the information stored.

Media handling documentation must include procedures for:
- ❖ Access control restrictions and authorization;
- ❖ Correct use of technology (e.g., encryption) to enforce access control;
- ❖ Copying and distribution of media, including minimization of multiple copies, marking of originals and distribution of copies;
- ❖ Operating the media storage environment and managing media lifespan according to manufacturer specifications;
- ❖ Regular status accounting of media;
- ❖ Maintenance of media transfer and storage records;
- ❖ Media destruction and disposal; and,
- ❖ User awareness training.

Only approved media devices appropriate for the sensitivity of the information being stored may be used.

6.7.4 Systems documentation must be protected from unauthorized access. a) Protection of systems documentation

Purpose: To prevent unauthorized access to sensitive information contained in *systems documentation*.

6.7.4 a) Protection of systems documentation

Information Custodians and Information Owners must ensure that documented procedures for the secure use and storage of system documentation are established and followed. Procedures must:

- Establish lists of users authorized to access system documentation on a '*need to know*' basis;
- Establish handling rules for the information regardless of storage media (e.g., electronic, paper);
- Require use of access controls, passwords, encryption or digital signatures as appropriate; and,
- Include a compliance monitoring process

6.8	**Communications and Operations Management – Exchanges of information**
6.8.1	Information exchange policies, procedures and controls must be documented and implemented to protect the exchange of information through all types of electronic communication services. a) Electronic information exchange

Purpose: To protect *information* from unauthorized disclosure.

6.8.1 a) Electronic information exchange

The Office of Information Protection must document and implement procedures to protect information from interception, copying, miss-routing and destruction when being transmitted electronically or verbally. Transmission methods include but are not limited to:

- E-mail, including attachments;
- Electronic file transfer (e.g., File Transfer Protocol (FTP), Electronic Data Interchange (EDI));
- Use of mobile devices
- Telephone, cell, and other voice messaging;
- Faxes; and,
- Instant messaging.

6.8.2	Information and software exchange agreements between the Province and other organizations must be documented. a) Exchange agreements b) Information and software exchange requirements

Purpose: To protect *information* or software from loss or unauthorized disclosure.

6.8.2 a) Exchange agreements

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

- Custody and control accountabilities;
- Authority of a custodian to publish, grant access to or redistribute the information;
- Purpose and authorized uses of the information or software;
- Limitations on data linkage;
- Duration, renewal and termination provisions;
- Primary contacts, for agreement, governance and management;
- Requirements for:
  - ✓ Protecting information according to whether it is personal and/or confidential,
  - ✓ Handling information (e.g., recording authorized recipients, confirming receipt of transmitted data, periodically reviewing records of authorized recipients),
  - ✓ Labeling information (e.g., methods to be used to apply and recognize labeling),
  - ✓ Maintaining integrity and *non-repudiation* of information, and,
  - ✓ Media management and destruction;
- Technical standards for transmission, recording or reading information or software;
- Responsibilities for reporting privacy and security incidents and breaches;
- Liability, accountability and mitigation strategies, for attempted, suspected or actual privacy and security incidents and breaches; and,
- Problem resolution and escalation processes.

6.8.2 b) Information and software exchange requirements

Information Owners and Information Custodians must ensure the following are completed for the information or software covered by the exchange agreement:

- An approved Privacy Impact Assessment; and,
- A Threat and Risk Assessment.

Exchange agreements must be reviewed by legal counsel for the Province prior to being signed.

6.8.3 Media being physically transported must be appropriately protected.
a) Media transport procedures

Purpose: To protect *information* from unauthorized disclosure or loss during transport of physical media.

6.8.3 a) Media transport procedures

The Office of Information Protection must document and implement security measures for the protection of media during transport. If information of various sensitivities is stored on media, the media must be protected according to the highest sensitivity of the information stored.

Minimum media transport requirements are:

- Using couriers that are approved by Government;
- Inspecting identification credentials of couriers upon pick-up and delivery of packages;
- Obtain and retain receipts for media shipments;
- Using packaging that will protect the media from loss or damage; and,
- Packaging so that the data stored on the media is not displayed

6.8.4 Information transmitted by electronic messaging must be appropriately protected.
a) General requirements
b) Custody of *electronic messages*

Purpose: To enable secure and trustworthy electronic messaging

6.8.4 a) General requirements

Electronic messaging services must be managed to protect the integrity of Government messages by:

- 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 to legislative, regulatory and policy requirements.

The Chief Information Security Officer must approve implementation of, and significant modification to, electronic messaging systems.

Personnel must support the responsible use of electronic messaging services by:

- Using only Government electronic messaging systems, including systems for *remote access* to Government messaging systems from publicly available networks; and,

- Maintaining the confidentiality and privacy of information being communicated in electronic messages as appropriate to the sensitivity of the information.

6.8.4 b) Custody of electronic messages

Electronic messages created, compiled on, sent or received on Government *information systems* are records of the Government. These records:

- Are the property of the Government of Prince Edward Island;
- Must be managed in accordance with the *Archives and Records Act* and the policies, standards and procedures in the Classification and Retention Manual; and,
- Are subject to the access and the protection of privacy provisions of the *Freedom of Information and Protection of Privacy Act.*

6.8.5	Security controls must be implemented to mitigate the business and security risks associated with the interconnection of *business information systems*. a) Information in business information systems

Purpose: To restrict access to information in shared business information systems.

6.8.5 a) Information in business information systems

Information Owners must document and implement procedures to restrict access to information in interconnected internal administrative and productivity information systems such as e-mail, calendars and financial systems.

A Threat and Risk Assessment must be conducted to:

- Determine if business information systems provide sufficient protection for the information being shared;
- Define controls to manage information sharing;
- Reduce the *risk* of social engineering; and,
- Identify access control requirements.

6.9	**Communications and Operations Management – Electronic commerce services**
6.9.1	Information in *electronic commerce* information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification. a) Electronic commerce

Purpose: To enable secure electronic commerce for the delivery of Government services.

6.9.1 a) Electronic commerce

Prior to initiating or implementing electronic commerce information systems Information Owners and Information Custodians must:

- Ensure that a *Threat and Risk Assessment* is conducted and addresses threats and *risks* related to electronic commerce;
- Confirm that a *Privacy Impact Assessment* has been conducted and approved;
- Determine the security of the information and information system(s) involved;
- Ensure that the user notification and acceptance of terms and conditions of use complies with Government policies and standards;
- Ensure *multi factor* authentication is used where the sensitivity and value of the information requires;

- Develop and implement processes to maintain content currency;
- Confirm the information system has received security certification and Payment Card Industry (PCI) *accreditation;* and,
- Develop Business Continuity Plans and supporting *Disaster Recovery Plans.*

6.9.2 Information systems utilizing on-line transactions must have security controls commensurate with the value and sensitivity of the information.
a) On-line transaction security

Purpose: To maintain the confidentiality, integrity and availability of on-line transactions in information systems.

6.9.2 a) On-line transaction security

Information Owners and Information Custodians are responsible for ensuring information systems containing on-line transactions implement security controls commensurate with the value and sensitivity of the information.

Security controls must be implemented to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate *network security zone*.

6.9.3 Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.
a) Internet site security

Purpose: To protect the integrity and accuracy of information on publicly available information systems.

6.9.3 a) Internet site security

Information Owners must approve the publication, modification or removal of information on publicly available information systems. Information Custodians are responsible for maintaining the accuracy and integrity of the published information. Security controls must be developed,

documented and implemented to:

- Maintain a record of changes to published information;
- Maintain the integrity of published information;
- Prevent the inappropriate release of sensitive or personal information;
- Monitor for unauthorized changes; and,
- Prevent unauthorized access to networks and information systems.

6.10 Communications and Operations Management – Monitoring
6.10.1 Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations. a) Audit logging b) Audit log retention c) Response to alarms

Purpose: To ensure usage of *information systems* can be monitored and audited.

6.10.1 a) Audit logging

Information Owners and Information Custodians must ensure that audit logs are used to record user and system activities, exceptions and information security and operational events including information about activity on networks, applications and systems. Information Owners and Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs. Audit logs should include, when relevant, the following information:

- User identifier;
- Dates, times and details of key events (e.g., logon and logoff);
- Logon method, location, terminal identity (if possible), network address;
- Records of successful and unsuccessful system access attempts;
- Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;
- Changes to system configuration;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and type of access (e.g., view, read, modify, delete);
- Network addresses and protocols;
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems (e.g., anti-virus, intrusion detection).

Audit logs may contain confidential data and access must be restricted to personnel with 'need-to-know' privileged access and be protected accordingly.

Information Owners and Information Custodians must not have the ability to modify, erase or de-activate logs of their own activities.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log. Where required, the *Privacy Impact Assessment* and/or *Threat and Risk Assessment* must be updated to reflect this decision.

6.10.1 b) Audit log retention

Audit logs must be:

- Retained according to the approved records retention schedule for the system or information asset; and,
- Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

6.10.1 c) Response to alarms

Information Custodians must establish and document alarm response procedures in collaboration with Information Owners to ensure alarms are responded to immediately and consistently.

Information Custodians should have documented authority to shut down all or part of a system or network when the alarm indicates new unacceptable threats are present. When exercising this authority Information Custodians must report the circumstances to the Information Owners as soon as possible.

Normally, the response to an alarm will include:

- Identification of the alarm event;
- Isolation of the event including affected assets;
- Identification and isolation or neutralization of the source;
- Corrective action;
- Forensic analysis of event;
- Action to prevent recurrence;
- Securing of audit logs as evidence.

6.10.2 The use of information systems must be monitored and the result of the monitoring activities must be regularly reviewed.
a) Monitoring the use of information systems
b) Review of monitoring activities

Purpose: To detect unusual or unauthorized use of *information systems*.

6.10.2 a) Monitoring the use of information systems

Information Owners and Information Custodians must ensure that the use of information systems can be monitored to detect activities including: authorized and unauthorized accesses, system alerts and failures. Information Owners and Information Custodians must identify the activities to be reported as part of an exception reporting process. Information custodians must implement, manage and monitor logging systems for:

- Authorized access, including:
- User identifier,
- Date and time of log on and log off,
- Type of event(s),
- Files accessed, and,
- Programs, privileges and/or utilities used;
- Privileged operations, including:
  - ✓ Use of privileged accounts (e.g., System Administrator, Data Base Administrator)
  - ✓ System start-up and shutdown, and,
  - ✓ Input/output device attachment and/or detachment;
  - ✓ Unauthorized access attempts, including:
  - ✓ Failed or rejected user actions, data access or other resource attempts,
  - ✓ Access policy violations and notifications for network gateways and firewalls, and, alerts from intrusion detection systems;
  - ✓ System alerts or failures, including:
  - ✓ Console alerts or messages,
  - ✓ System log exceptions,
  - ✓ Network management alarms, and,
  - ✓ Access control system alarms; and,
  - ✓ Changes to, or attempts to change, system security settings and controls.

6.10.2 b) Review of monitoring activities

Information Custodians must set up and document processes for the review of audit logs based on the Information Owners assessment of the value and sensitivity of the information assets, the criticality of the system and the resources required for review.

Audit log reviews should:

- Prioritize reviews of high value and highly sensitive information assets,
- Be based on a documented *Threat and Risk Assessment*,
- Utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity) and facilitate ongoing analysis and review.

Monitoring should be tested at least annually to ensure that desired events are detected.

Analysis of monitoring activities can indicate:

- The efficacy of user awareness and training and indicate new training requirements;
- Vulnerabilities that could be, or that are being, exploited; or

- Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

6.10.3 Information system logging facilities and log information must be protected against tampering and unauthorized access. a) Protecting information system logging facilities

Purpose: To preserve the integrity of *information system* logging facilities and log information.

6.10.3 a) Protecting information system logging facilities

Information Owners are responsible for ensuring periodic independent reviews or audits are conducted to confirm that Information Custodians have implemented appropriate controls.

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

- Physical security safeguards such as situating logging facilities within a secure zone with restricted access;
- Administrators and operators must not have permission to erase or de-activate logs of their own activities;
- Consideration of *multi-factor* authentication for access to sensitive records;
- Back-up of audit logs to off-site facilities;
- Automatic archiving of audit logs to remain within storage capacity;
- Scheduling the audit logs as part of the records management process.

6.10.4 Activities of privileged users must be logged, and the log must be subject to regular independent review. a) Activities logged b) Independent review

Purpose: To protect Government *information* from unauthorized access, modification or deletion.

6.10.4 a) Activities logged

Privileged users typically have extensive system permissions not granted to most users. Information Owners and Information Custodians must ensure that the activities of privileged

users are regularly reviewed including logging:

- Event occurrence times;
- Event details, such as files accessed, modified or deleted, errors and corrective action;
- Identity of the account and the privileged user involved; and,
- The system processes involved.

6.10.4 b) Independent review

Information Custodians must have a documented process to ensure that activity of privileged users is independently checked by the Information Owner or delegate. Checks should be conducted regularly and at random with the frequency being commensurate with the criticality, value and sensitivity of system and information assets. Following verification of logs, the individual checking them should digitally sign them and store or archive them securely in accordance with the approved records retention schedule.

6.10.5 Faults must be logged, analyzed and appropriate action taken.
a) Reporting and logging faults
b) Analysis, resolution and corrective action

Purpose: To support system security by establishing processes for reporting, logging, analyzing, resolving and correcting system faults.

6.10.5 a) Reporting and logging faults

Information Owners and Information Custodians must implement processes for monitoring, reporting and logging system faults reported by users and automated detection systems. Fault logging requirements should be determined through a *Threat and Risk Assessment*. Fault logs should include:

- Description of fault including date/time, location, extent of fault, probable source/cause;
- Actions taken to respond to and/or resolve the fault; and,
- Corrective action taken.

6.10.5 b) Analysis, resolution and corrective action

Information Custodians must review fault logs to ensure that faults have been resolved and regularly report fault incidents and resolution actions to Information Owners. Analysis and corrective action includes:

- Defining the fault and probable cause(s);
- Assessing the effectiveness of corrective action(s);
- Checking to ensure that corrective action has not introduced unforeseen vulnerabilities;

- ❖ Identifying trends so that corrective action makes increasingly effective use of resources while improving results;
- ❖ Recommending upgrades and/or replacement of components, software or other elements that create/cause faults;
- ❖ Improving fault detection and reporting to reduce the time between fault occurrence and taking corrective action;
- ❖ Reporting on performance impact(s); and,
- ❖ Periodically re-assessing logging requirements.

6.10.6 Computer clocks shall be synchronized for accurate reporting. a) Synchronization b) Checking and Verification

Purpose: To ensure the integrity of *information system* logs.

6.10.6 a) Synchronization

System administrators must synchronize information system clocks to:

- ❖ the local router gateway; or,
- ❖ PEI Government clock host.

6.10.6 b) Checking and Verification

System administrators must confirm system clock synchronization:

- ❖ Following power outages or brownouts;
- ❖ As part of incident analysis and audit log review; and,
- ❖ At least semi-annually in conjunction with Daylight Savings Time.

Chapter 7 – Access Control

This chapter identifies the mechanisms that restrict access to Government information and information assets. Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by legislation that protects particular types of information (e.g., personal, sensitive or cabinet confidential) and by business requirements. Mechanisms for access control include password management, user authentication and user permissions.

Access control policies provide the blueprint for the management of user access, authorizations and control mechanisms for computer networks, operating systems, applications and information. This chapter identifies security best practices and responsibilities for administrators and personnel.

7.1 Business requirement for access control
7.1.1 Access control policy Access to information systems and services must be consistent with business needs and be based on security requirements.
7.2 User access management
7.2.1 User registration There must be a formal user registration and de-registration process for granting access to all information systems.
7.2.2 Privilege management The allocation and use of system privileges must be restricted and controlled.
7.2.3 User password management The issuance of authentication credentials must be controlled through a formal management process.
7.2.4 Review of user access rights Information Owners and Information Custodians must formally review user access rights at regular intervals
7.3 User responsibilities
7.3.1 Password use Users must follow good security practices in the selection and use of passwords.
7.3.2 Unattended user equipment Users must ensure unattended equipment has appropriate protection.
7.3.3 Clear desk and clear screen policy Users must ensure the safety of sensitive information from unauthorized access, loss or damage.
7.4 Network access control
7.4.1 Policy on use of network services Users must only be provided access to the information systems they have been specifically authorized to use.
7.4.2 User authentication for external connections Access by remote users must be subject to authentication.
7.4.3 Equipment identification in the network

Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment.
7.4.4 Remote diagnostic and configuration port protection Physical and logical access to diagnostic ports must be securely controlled.
7.4.5 Segregation in networks Groups of information services, users and information systems must be segregated on networks.
7.4.6 Network connection control The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system.
7.4.7 Network routing control Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system.
7.5 Operating system access control
7.5.1 Secure log-on procedures Access to information systems must use a secure logon process.
7.5.2 User identification and authentication All users must be issued a unique identifier for their use only, and an approved authentication technique must be used to substantiate the identity of the user .
7.5.3 Password management system A password management system must be in place to provide an effective, interactive facility that ensures quality passwords.
7.5.4 Use of system utilities Use of system utility programs must be restricted and tightly controlled.
7.5.5 Session time-out Inactive sessions must be shut down after a defined period of inactivity.
7.5.6 Limitation of connection time Restrictions on connection times must be used to provide additional security for high value applications.
7.6 Application and information access control
7.6.1 Information access restriction Access to information systems functions and information must be restricted in accordance with the access control policy.
7.6.2 Sensitive system isolation Information systems managing data of a sensitive nature must have an isolated dedicated computing environment.
7.7 Mobile computing and teleworking
7.7.1 Mobile computing and communications Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.
7.7.2 Teleworking Teleworking must employ security controls to ensure that information resources are not compromised.

7.1	**Access Control – Business requirement for access control**
7.1.1	Access to information systems and services must be consistent with business needs and be based on security requirements. a) Access control policy b) Access control policy management c) Review of access control policy

Purpose: To ensure that *information* and *information systems* are available for authorized use and protected from unauthorized use.

7.1.1 a) Access control policy

Information Owners and Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- ❖ Support and enable business requirements identified in *Privacy Impact Assessments*; and
- ❖ Be based upon Threat and Risk Assessment.

Access control policies must additionally:

- ❖ Consider both physical and logical access to assets;
- ❖ Apply the "*need to know*" and "*least privilege*" principles;
- ❖ Set default access privileges to "deny-all" prior to granting access;
- ❖ Require access by unique user identifiers or system process identifiers to ensure that all accesses are auditable;
  - ✓ Have permissions assigned to roles rather than individual user identifiers.

The relevant portions of the access control policy must be communicated to personnel as part of awareness training.

7.1.1 b) Access control policy management

Information Owners and Information Custodians are responsible for establishing processes to manage the access control policies, including:

- ❖ Ensuring the process is communicated to all personnel;
- ❖ Documenting processes for user registration and deregistration;
- ❖ Segregating roles and functions (i.e. access requests, access authorization, access administration);
- ❖ Defining rules for controlling access to privileged system functions;
- ❖ Identifying roles and/or functions which require multi factor authentication; and,
- ❖ Identifying and justifying exceptional cases where there is a need for enhanced personnel security screening for sensitive assets.

7.1.1 c) Review of access control policy

Information Owners and Information Custodians must conduct periodic reviews of the access control policy as part of an ongoing process for *risk* management, security, and privacy. Reviews must be conducted:

- Annually;
- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise; and,
- Following significant Government or Departmental re-organization as appropriate.

7.2	**Access Control – User access management**
7.2.1	There must be a formal user registration and de-registration process for granting access to all information systems. a) Registration b) Deregistration

Purpose: To ensure that all access actions are traceable to an identifiable individual or process.

7.2.1 a) Registration

Information Owners and Information Custodians are responsible for managing access to the assets under their control and must implement registration processes which:

- Depending on the asset, Owners or Custodians must approve all access rights. This process should:
  - ✓ ensure access requests are approved by the supervisor/manager of the *user* requesting access, and,
  - ✓ ensure the reasons for requesting access are consistent with job responsibilities;
- Maintain records of access right 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 the approved *Privacy* Impact Assessment;
- Ensures accesses are traceable to an identifiable individual or process;
- Ensures each user is assigned a single unique identifier for accessing information systems.
- Ensures the responsibilities for authorizing access are segregated from the responsibilities for granting access;
- Restricts access by using predefined role permissions; where possible;
- Provides secure and separate transmission of the user identifier and password to the user; and,

- In exceptional cases, where warranted by the sensitivity of the asset and supported by a *Threat and Risk Assessments*, ensures enhanced user security screening or background checks are completed prior to authorizing access.

7.2.1 b) Deregistration

Information Owners and Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization within 5 working days;
- Promptly review access rights whenever a user changes duties and responsibilities;
- Promptly review access rights whenever the user's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended absence or temporary assignments within 10 working days of the change of status;
- Remove access privileges for employees terminated for cause concurrent with notification to individual; and,
- Quarterly check for and remove inactive or redundant user identifiers.

7.2.2 The allocation and use of system privileges must be restricted and controlled.
a) Managing, restricting and controlling the allocation and use of system privileges

Purpose: To prevent unauthorized access to multi-user information systems.

7.2.2 a) Managing, restricting and controlling the allocation and use of system privileges

Information Owners and Information Custodians are responsible for authorizing *system privileges* and 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 access to system privileges;
- Ensure use of system privileges is recorded in audit logs which are unalterable by the privileged user;

- ❖ Implement processes for ongoing *compliance checking* of the use of system privileges; and,
- ❖ Implement processes for regular review of authorizations in place to confirm that access is still needed and that the least number of users needed have access.

User identifiers with *system privileges* must only be used for performing privileged functions and not used to perform regular activities. User identifiers established to perform regular activities must not be used to perform privileged functions.

Guidelines:

- ❖ The design of information systems should include processes for performing regular maintenance activities which avoid the requirement of *system privileges*.
- ❖ Whenever possible system routines should be used to execute system privileges rather than granting system privileges to individual users.
- ❖ System acquisition and development should encourage use of programs which minimize the need for users to operate with system privileges.

Privileged *users* should:

- ❖ Not be able to read the data of an information asset;
- ❖ Be able to alter user permissions for an information asset; and,
- ❖ Be permitted to view user activity logs as part of security safeguards.

7.2.3 The issuance of authentication credentials must be controlled through a formal management process. a) Managing the issuance of passwords

Purpose: To define the formal management processes for issuing passwords.

7.2.3 a) Managing the issuance of passwords

Designated individuals have the authority to issue and reset passwords. The following applies:

- ❖ Passwords shall only be issued to users whose identity is confirmed prior to issuance;
- ❖ Individuals with the authority to reset passwords must transmit new or reset passwords to the user in a secure manner (e.g., using encryption, using a secondary channel);
- ❖ Whenever technically possible temporary passwords must be unique to each individual and must not be easily guessable;
- ❖ Passwords must never be stored in an unprotected form; and,
- ❖ Default passwords provided by technology vendors must be changed to a password compliant with Government standards during the installation of the technology (hardware or software).

7.2.4 Information Owners and Information Custodians must formally review user access rights at regular intervals. a) Circumstances and criteria for formal access right review b) Procedure for formal access right review

Purpose: To ensure that access rights only exist for users with a defined "need to know".

7.2.4 a) Circumstances and criteria for formal access right review

Information Owners and Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When a user's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a user's need to access information assets; (See GISP 4.3.3 for requirements at termination of employment or contract);
- As part of a major reorganization, or the introduction of new technology or applications; and,
- When Information Owners and Information Custodians change the access control policy the access rights must be reviewed.

7.2.4 b) Procedure for formal access right review

Review of access rights must include the following:

- Confirmation that access rights are based on the "need to know" and "least privilege" principles;
- Confirmation that all members of the group/role have a need to know;
- Reviews and verification of access control lists are dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights is logged and auditable.

Access control logs and reports are Government records and must be retained and disposed of in accordance with approved record management retention schedules.

7.3 Access Control – User responsibilities
7.3.1 Users must follow good security practices in the selection and use of passwords. a) Selection of passwords b) Password change c) Privileged accounts d) Protection and use of passwords

Purpose: To maintain the integrity of the unique identifier (user id) by ensuring users follow

good security practices.

7.3.1 a) Selection of passwords

When selecting passwords users must:

- Select complex passwords, i.e., a mixture of characters
- Avoid using the same password for multiple accounts.

The effectiveness of access control measures is strengthened when users adopt good security practices for selecting passwords.

7.3.1 b) Password change

Passwords must be changed:

- During installation of computer hardware and or software which is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If compromise has taken place or is suspected the incident must be reported in accordance with GISP 9.1.1; and,
- Comply with password change instructions issued by an automated process (e.g., password lifecycle replacement) or an appropriate authority.

7.3.1 c) Privileged accounts

Privileged accounts have wider and more powerful access rights to information assets. In addition to 7.3.1 a) and b) users authorized to create or who hold privileged accounts must:

- Use passwords which are at least 15 characters where technically feasible; and,
- Change passwords more frequently than a password for normal account.

7.3.1 d) Protection and use of passwords

Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing passwords;
- Permitting anyone to view the password as it is being entered;
- Writing down a password;
- Storing other personal identifiers, access codes, tokens or passwords in the same container as the token;
- Keeping a file of passwords on any computer system, including Personal Digital Assistants, smart phones and other similar devices; and
- Employing any automatic or scripted logon processes for personal identifiers; and, not using personal identifiers, access codes, or passwords associated with Government accounts for personal or other purpose

Where a business need is defined to keep written records of passwords an exception may be granted.

For mobile devices connecting to the Government messaging server, the following password rules apply:

- Passwords must contain a minimum of 6 characters;
- Controls should be in place to prevent the use of overly simple passwords; and,
- The use of complex passwords is not mandatory; however, the use of a combination of numbers, symbols, upper and lower case characters is highly recommended to increase the password strength.

7.3.2 Users must ensure unattended equipment has appropriate protection.
a) Protection of unattended equipment

Purpose: To reduce *risk* of unauthorized access, loss or damage to *information* and *information systems*.

7.3.2 a) Protection of unattended equipment

Information Owners and Information Custodians must ensure that *users* prevent unauthorized access to information systems by securing unattended equipment*,* by:

- Locking or terminating information system sessions before leaving the equipment unattended;
- Enabling a password protection features on the equipment (e.g., screen savers on workstations);
- Shutting down and restarting unattended workstations at the end of each workday;
- Enabling password protection on mobile devices including *portable storage devices*; and,
- Being aware of their responsibility to report *security weaknesses* where the above controls have not been applied.

7.3.3 Users must ensure the safety of sensitive information from unauthorized access, loss or damage.
a) Securing the work space
b) Secure work habits

Purpose: To reduce *risk* of unauthorized access, loss or damage to information by ensuring users take reasonable security precautions.

7.3.3 a) Securing the work space

Users should secure their work space whenever it is not supervised by an authorized person, including during short breaks, attendance at meetings, and at the end of the work day.

Securing the work space includes:

- Clearing desk tops and work areas;
- Securing documents and *portable storage devices* in a locked desk or file cabinet;
- Ensure outgoing and incoming mail is appropriately secured;
- Having a password protected screen saver;
- Shutting down and restarting workstations at the end of each work day;
- Locking doors and windows; and,
- Checking fax machines and printers to ensure that no sensitive information is waiting to be picked up.

7.3.3 b) Secure work habits

Users must develop and implement security conscious work habits to reduce the likelihood of unauthorized viewing, access or disclosure of sensitive information. Security conscious work habits include:

- Ensuring sensitive information is protected from accidental viewing by persons passing through the work space;
- Ensuring that only the documents required for current work are out of their normal file cabinet;
- Covering up, filing or storing paper documents when visitors are present in the work area;
- Clearing, changing or turning off the computer screen (e.g., minimize open Windows, lock the PC) so that sensitive information is not displayed when visitors are present in the work area; and,
- Not discussing sensitive information in open work spaces or public areas.

7.4	**Access Control – Network access control**
7.4.1	Users must only be provided access to the information systems they have been specifically authorized to use. a) Access to network services b) Management controls and processes c) Means for accessing networks and network services

<u>Purpose: To support the information system access control policy by limiting network access to authorized users of specific information systems.</u>

7.4.1 a) Access to network services

Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems,

using the principle of least privilege, as defined in the access control policies for the information system.

7.4.1 b) Management controls and processes

Information Custodians must document processes for management of network access, including:

- Documentation and review of implemented network access controls;
- Identification of threats, *risks* and mitigation factors associated with network services;
- Testing of network access controls to verify correct implementation; and,
- Assisting Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

7.4.1 c) Means for accessing networks and network services

Information Custodians must define and implement:

- Permitted network access methods for each network zone (e.g., direct connection, Virtual Private Network, dial-up); and,
- Minimum security controls required for connection to networks (e.g., patch levels, anti-virus software, firewalls, user and system authentication requirements).
-

7.4.2 Access by remote users must be subject to authentication.
a) Remote access to the Government networks or services

Purpose: To identify and authenticate users and systems accessing the Government network from remote locations.

7.4.2 a) Remote access to Government networks or services

Providers of remote network access services for individuals must:

- Perform a *Threat and Risk Assessments* for each *remote access service* to determine the authentication methods to be implemented. Factors to be considered include sensitivity of network services, information and information systems accessible from the remote access service;
- Require remote users to connect through Government designated remote access services or security gateways (e.g., Virtual Private Network, Desktop Terminal Services (DTS), GroupWise Web Access); and,
- Require user identification and authorization prior to permitting each remote network connection.

Providers of remote network access services for interconnection of networks must:

- ❖ Perform a Threat and Risk Assessments for each remote network interconnection to determine the user and system authentication methods to be implemented. Factors to be considered include:
  - ✓ sensitivity of network services, information, and information systems accessible from the remote access service, and,
  - ✓ the strength of security controls implemented in the remote network;
- ❖ Notify Information Owners of every information system accessible from remotely connected networks prior to interconnectivity; and,
- ❖ Require remote network interconnections to connect through Government designated remote access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

7.4.3 Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment. a) Authentication of connections

Purpose: To increase assurance of system identification where required by system sensitivity.

7.4.3 a) Authentication of connections

Information Owners must use automatic equipment identification if the requirement is identified by a Threat and Risk Assessment. Factors to consider include:

- ❖ The sensitivity of information that may be accessed or stored;
- ❖ The physical security of information, information technology assets and location;
- ❖ Unauthorized information access by people at the location, either inadvertent or deliberate; and,
- ❖ Remote access threats if remote access is utilized.

7.4.4 Physical and logical access to diagnostic ports must be securely controlled. a) Protection of diagnostic ports

Purpose: To prevent unauthorized use of maintenance or diagnostic facilities

7.4.4 a) Protection of diagnostic ports

Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems for diagnostic, maintenance and monitoring activities to prevent bypassing of information system access controls.

Physical and logical access controls to be considered for implementation include: physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed, and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized by agreements, contracts and conditions of use.

Use of diagnostic ports must be logged and monitored for suspicious activity.

7.4.5 Groups of information services, users and information systems must be segregated on networks. a) Segregation based on risk and requirements

Purpose: To isolate *information systems*, users and networks based on *risk* and business connectivity requirements to control information flow, minimize unauthorized connection attempts and limit the spread of damage in case of compromise.

7.4.5 a) Segregation based on risk and requirements

Information Custodians must segregate services, information systems and users to support business requirements for information system connectivity and access control based on the principles of *least privilege*, management of risk and segregation of duties.

Information Custodians 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.

The techniques and technologies selected for *network segregation* must be based on *Security Threat and Risk Assessment* findings and industry best practices. Factors to consider include:

- The information and information system security ;
- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks and sensitivity to eavesdropping (e.g., the Internet is a less trusted network than a controlled server network zone);
- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

7.4.6 The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system. a) Logical and physical network connection control b) Wireless networks

Purpose: To control network connection in support of the access control policy and limit opportunity for unauthorized access.

7.4.6 a) Logical and physical network connection control

Information Custodians must restrict the ability of users to physically and logically connect to networks according to the access control policy defined by Information Owners. Techniques may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuing network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to *information systems* must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to segregate it from direct network connections by user workstations.

7.4.6 b) Wireless networks

Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as determined by a *Threat and Risk Assessments* and industry best practices.

7.4.7 Networks must have routing controls to ensure that computer connections and information flows do not breach the access control policy of the information system. a) Network address control b) Control of routing information

Purpose: To control network routing to prevent unauthorized access or bypassing of security control points.

7.4.7 a) Network address control

Information Custodians must implement mechanisms to prevent *network address spoofing* and routing of spoofed network traffic (e.g., through use of router access control lists).

Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

7.4.7 b) Control of routing information

Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

7.5	**Access Control – Operating system access control**
7.5.1	Access to information systems must use a secure logon process. a) Information displayed during logon b) Unsuccessful logon attempts c) Password transmission

Purpose: To ensure access to *information systems* is limited to authorized users and processes.

7.5.1 a) Information displayed during logon

Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access. This includes:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Displaying a general warning notice that the Information System be accessed only by authorized users;
- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

7.5.1 b) Unsuccessful logon attempts

If supported by the system, Information Owners must ensure that Information Custodians configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure. If exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

7.5.1 c) Password transmission

Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

7.5.2 All users must be issued a unique identifier for their use only, and an approved authentication technique must be used to substantiate the identity of the user. a) Allocation of unique identifier b) Authentication of identity c) Shared user identifiers

Purpose: To ensure that access to information systems requires use of unique authenticated *user identifiers.*

7.5.2 a) Allocation of unique identifier

Information Owners and Information Custodians must ensure *users* are issued unique user identifiers (userids) for their use only except as specified in 7.5.2 (c). The documented and approved process for allocating and managing unique identifiers must include:

- A single point of contact to:
- manage the assignment and issuance of user identifiers,
- ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
- record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

7.5.2 b) Authentication of identity

Information Owners and Information Custodians must ensure that user identifiers are authenticated by an approved authentication mechanism.

User identifiers authenticated by means other than a password must use a mechanism approved by the Office of Information Protection.

7.5.2 c) Shared user identifiers

In exceptional circumstances, where there is a clear business benefit identified by the Information Owner or Information Custodian, the use of a *positional user identifier* for a group of users or a specific job can be used, provided:

- ❖ Positional user identifiers are not used for privileged users

7.5.3 A password management system must be in place to provide an effective, interactive facility that ensures quality passwords. a) Enforcing quality password rules

Purpose: To support the operating system access control policy through use of *password management systems* to enforce the password standard.

7.5.3 a) Enforcing quality password rules

Information Owners and Information Custodians must ensure password management systems:

- ❖ Enforce the use of individual user identifiers and passwords;
- ❖ Support user selection and change of passwords using the Complex Password Standard;
- ❖ Enforce user change of temporary passwords at first logon and after password reset by an Administrator;
- ❖ Enforce regular user password change, including advance warning of impending expiry;
- ❖ Prevent re-use of passwords for a specified number of times;
- ❖ Prevent passwords from being viewed on-screen;
- ❖ Store password files separately from application system data;
- ❖ Ensure password management systems are protected from unauthorized access and manipulation; and,
- ❖ Store and transmit passwords in protected (e.g., encrypted) form.

The password management system standard for Government systems requires that users must be:

- ❖ Prevented from reusing the same password within 12 months; and,
- ❖ Provided with notification at least 10 days before their password will need to be changed.

7.5.4 Use of system utility programs must be restricted and tightly controlled. a) Restriction and control of system utility programs

Purpose: To restrict and tightly control the use of utility programs, which may be used to override system and application controls.

7.5.4 a) Restriction and control of system utility programs

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

- ❖ Defining and documenting authorization levels;

- Restricting the number of users with access to system utility programs;
- Annually reviewing the status of users with permissions to use system utility programs;
- Ensuring that the use of system utilities maintains segregation of duties;
- Requiring a secure logon process to be used to access system utilities;
- Ensuring that all system utility programs are identified and usage logged;
- Segregating system utilities from application software where possible; and,
- Removing or disabling unnecessary and obsolete system utilities and system software.

7.5.5 Inactive sessions must be shut down after a defined period of inactivity.
a) Session time-out

Purpose: To ensure unattended *information system* sessions are automatically terminated.

7.5.5 a) Session time-out

Information Owners and Information Custodians must define and implement automatic termination or re- authentication of active sessions after a pre-determined period of inactivity.

Government *information systems* must have session time-outs managed by operating system access, application or Government infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the:

- *Risks* related to the security zone;
- Sensitivity of the information being handled; and,
- Risks related to the use of the equipment by multiple users.

7.5.6 Restrictions on connection times must be used to provide additional security for high value applications.
a) Limiting access hours
b) Limiting connection duration

Purpose: To limit opportunities for inappropriate and unauthorized access to high value applications by restricting access hours and connection duration.

7.5.6 a) Limiting access hours

Information Owners and Information Custodians must restrict access hours for high value applications.

Restricting operating hours includes:

- ❖ Limiting access to pre-determined times (e.g., when Departmental support staff are available); and,
- ❖ Establishing restrictions for access from high *risk* public or external locations which are outside the control of the Department.

7.5.6 b) Limiting connection duration

Information Owners and Information Custodians must limit the duration of connection times for high value applications.

Restricting connection duration includes:

- ❖ Limiting session length; and,
- ❖ Requiring re-authentication of the user when a session has been inactive for a pre-defined period of time.

7.6	**Access Control – Application and information access control**
7.6.1	Access to information systems functions and information must be restricted in accordance with the access control policy. a) Information access controls b) System configuration c) Publicly accessible information

Purpose: To restrict access to application systems functions and information to authorized individuals or systems.

7.6.1 a) Information access controls

Information Owners and Information Custodians are responsible for ensuring the implementation of the access control policy for their business applications.

The application and information section of the access control policy must specify:

- ❖ The information to be controlled;
- ❖ The system functions to be controlled; and,
- ❖ The roles authorized to access the resources/information and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

The access control policy must identify the information and system functions accessible by various classes of users.

7.6.1 b) System configuration

Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

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

7.6.1 c) Publicly accessible information

Information that is publicly accessible must be physically segregated from non-public information.

7.6.2 Where possible, Information systems managing data of a sensitive nature must have an isolated dedicated computing environment. a) Segregation of sensitive information systems

Purpose: To ensure that sensitive *information systems* are segregated from non-sensitive information systems and are not compromised by sharing *information technology resources* with non-sensitive information systems.

7.6.2 a) Segregation of sensitive information systems

Information Owners and Information Custodians must conduct a *Threat and Risk Assessments* to determine the information system sensitivity level. The information system sensitivity level determines which network security zone the information system must reside.

Security zones must be established using physical or logical methods, which may include separate network segments, separate servers, firewalls, access control lists and proxy servers.

7.7	**Access Control – Mobile computing and teleworking**
7.7.1	Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices. a) Information protection paramount b) Service-specific risks and practices c) Protection of credentials d) Protection of network endpoint and physical device e) Human factors f) Risk assessment factors

Purpose: To protect information stored on *portable storage devices* from loss or unauthorized

access.

7.7.1 a) Information protection paramount

Information Owners and Information Custodians must ensure that use of portable storage devices is managed and controlled to mitigate the inherent *risks* of portable storage devices.

The use of portable storage devices such as laptops, tablets and smart phones to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity a *Threat and Risk Assessments* must be performed prior to permitting subscription or use of *mobile computing services.*

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

7.7.1 b) Service-specific risks and practices

Providers of mobile computing services must perform annual risk assessments to identify service-specific risks. Policies, standards, practices and guidelines that treat these risks must be developed, documented and maintained by the service provider.

7.7.1 c) Protection of credentials

User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets.

In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places. See GISP 7.3.1

7.7.1 d) Protection of network endpoint and physical devices

Portable storage devices are typically used to store information or remotely access Government *networks* and services. The policies and procedures governing *remote access* apply to mobile devices. See GISP 6.6.1, GISP 7.4.1, GISP 7.4.2, GISP 7.4.5 and GISP 7.4.6. Where Remote Access services are used, the portable storage device must be configured to prevent its use as a conduit between the non-Government and Government networks (e.g., VPN split tunneling must be disabled).

Network access to portable storage devices from non-Government networks must be blocked

by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).

Portable storage devices must be protected against *mobile* and malicious code.

Portable storage devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

7.7.1 e) Human factors

Information Owners and Information Custodians must provide users of mobile computing services with security awareness training, to ensure that Users are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using portable storage devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with security event reporting procedures.

7.7.1 f) Risk assessment factors

The Threat and Risk Assessments must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of the portable devices to remotely access Government networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information sensitivity levels must be considered in the risk assessment.

Minimum information protection safeguards for the use of portable storage devices include:

- **Encryption of stored data** to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- **Access control permissions on a portable storage device** must be applied to prevent unauthorized access to information by system users, particularly for multi-user mobile systems;
- **Regularly maintained data backups** of information stored on portable storage devices using Government backup facilities to protect against information loss;
- To provide **information availability** portable storage devices must not be used to

store the only copy of a Government record;

- **Physical security of the device** must be maintained to protect against asset and information loss; and,
- **User authentication** to the portable storage device and **user authentication** for remote access from the device must be implemented in accordance with authentication policies.

7.7.2 Teleworking must employ security controls to ensure that information resources are not compromised. a) Teleworking security controls based on risk assessment b) Teleworking agreement c) *Ad hoc teleworking* policy

Purpose: To protect information accessed through *teleworking* arrangements from loss or unauthorized access.

7.7.2 a) Teleworking security controls based on risk assessment

Information Owners and Information Custodians must ensure that Government information and information technology assets are adequately protected by implementing security controls supported by a *Threat and Risk Assessments* prior to granting permission for employees to enter into a teleworking arrangement.

The Threat and Risk Assessment must consider:

- The sensitivity of information that may be accessed or stored at the teleworking location;
- The physical security of information, information technology assets and the teleworking location;
- Unauthorized information access by people at the teleworking location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.

Security controls that must be considered include:

- Restriction of permitted *information t*ypes at the teleworking location;
- Provision of Government-managed equipment, if appropriate, due to information sensitivity or volume;
- Provision of locking cabinets, shredders and other physical security equipment;
- Encryption of data stored at the teleworking location;
- Security awareness training for protection of information and information assets, including clear desk policy, information handling rules, physical security issues and remote access training; and,
- Monitoring and review of teleworking equipment for security events and incident response.

7.7.2 b) Teleworking agreement

Teleworking arrangements must be formally authorized and documented.

A documented teleworking agreement between the employer and employee must exist that specifies the following user responsibilities, terms and conditions:

- The expectation that the user will actively protect information and information technology assets;
- Restrictions on the information types permitted at the teleworking location;
- The requirement to protect information from inadvertent or deliberate disclosure to people at the teleworking location by use of locking cabinets, passwords, locked rooms or shredders;
- The authorized teleworking location and contact information;
- Information backup requirements;
- What equipment and software is supplied by the employee and what is supplied by the employer;
- The terms of use for remote access, if applicable;
- The requirement to meet or exceed specified wireless networking security controls, if wireless networking will be used at the teleworking location;
- The requirement to report security events or unusual activity;
- The right of the province to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking;
- The right of the province to inspect the physical location of the teleworking office;
- The requirement to establish and maintain security controls as determined in the Threat and Risk Assessments;
- Arrangements for technical support; and,
- The start date, end date, expected work hours and provision for termination of the teleworking arrangement.

7.7.2 c) Ad hoc teleworking policy

Departments must develop and publish policy that governs ad hoc *teleworking*, in particular the practice of removing material from the workplace. Controls required for an ad hoc teleworking policy are:

- Restriction of the information types that may be accessed or utilized while teleworking;
- Use of locking cabinets, shredders and other physical security equipment;
- Minimum technical security controls required for non-Government computing equipment, in particular current anti-virus, personal firewall and current software patches; and,
- Subject to applicable law, the right of the province to monitor and investigate security events at the teleworking location, including access to employee owned equipment used for teleworking.

Chapter 8 – Information Systems Acquisition, Development and Maintenance

This chapter establishes requirements for incorporating security measures into the life cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

8.1 Security requirements of information systems
8.1.1 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.
8.2 Correct processing in applications
8.2.1 Input data validation Data input to an information system must be validated to ensure that it is correct and appropriate.
8.2.2 Control of internal processing Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.
8.2.3 Message integrity Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content.
8.2.4 Output data validation Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
8.3 Cryptographic controls
8.3.1 Policy on the use of cryptographic controls The use of cryptographic controls must be based on the risk of unauthorized access of the information or information system that is to be protected.
8.3.2 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.
8.4 Security of system files
8.4.1 Control of operational software The implementation of software on operational information systems must be operational information systems.
8.4.2 Protection of system test data Test data must be protected and controlled using the same procedures as for data from operational information systems.
8.4.3 Access control to program source code Access control must be maintained for program source libraries.

8.5 Security in development and support processes
8.5.1 Change control procedures Changes to software must be controlled by the use of formal change control procedures.
8.5.2 Technical review of applications after operating system changes Information systems must be reviewed and tested when operating system changes occur.
8.5.3 Restriction on changes to software packages Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.
8.5.4 Information leakage Controls must be applied to limit opportunities for information leakage.
8.5.5 Outsourced software development Controls must be applied to secure outsourced information system development.
8.6 Vulnerability Management
8.6.1 Control of vulnerabilities Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks.

8.1	**Information Systems Acquisition, Development and Maintenance – Security requirements of information systems**
8.1.1	Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems. a) Security requirements for information systems b) Security requirements at implementation c) System Security Plan

Purpose: To integrate system security requirements into business processes supporting the development, maintenance and acquisition of *information systems*.

8.1.1 a) Security requirements for information systems

Information Owners must conduct a Threat and Risk Assessments during the requirements phase when developing, implementing major changes to, or acquiring an information system, to identify the security requirements necessary to protect the information system. The Information Owner must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common Government processes and services (e.g., authentication, access control, financial management).

8.1.1 b) Security requirements at implementation

Information Owners and Information Custodians must ensure that sufficient controls are in place to mitigate the *risk* of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing a security certification.

8.1.1 c) System Security Plan

A System Security Plan must be documented and maintained for each information system.

The System Security Plan includes:

- A summary of risks identified in the Threat and Risk Assessments;
- Results of the system certification;
- Roles and responsibilities for information system security management;
- Specific procedures and standards used to mitigate risks and protect the information system;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures.

8.2	**Information Systems Acquisition, Development and Maintenance – Correct processing in applications**
8.2.1	Data input to an information system must be validated to ensure that it is correct and appropriate. a) Input data validation

Purpose: To maintain the integrity of *information* in *information systems* by preventing the introduction of invalid or incomplete data.

8.2.1 a) Input data validation

Information Owners must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and;
- Using *control balances* to verify complete input and processing.

8.2.2	Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity. a) Internal processing

Purpose: To prevent errors, loss, unauthorized modification or misuse of *information* in *information systems*.

8.2.2 a) Internal processing

Information Owners must require that information systems include internal processing checks to:

- Detect unauthorized or incorrect changes to information;
- Prevent information from being accidentally overwritten;
- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);
- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;
- Maintain audit trails; and,
- Provide error and exception reports.

8.2.3	*Message integrity* controls must be used for information systems where there is a security requirement to protect the authenticity of the message content. a) Message integrity

Purpose: To prevent errors, loss, unauthorized modification or misuse of *information* in *information systems*.

Message integrity

Information Owners must determine message integrity requirements during the requirements definition phase of system development or acquisition.

8.2.4	Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. a) Output data validation

Purpose: To verify correct information processing for output data.

8.2.4 a) Output data validation

Information Owners must require that processes are documented to validate the data output from an information system by:

- Reconciling *control balances* to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, and precision of the information;
- Maintaining audit trails; and,
- Providing error and exception reports.

8.03	**Information Systems Acquisition, Development and Maintenance – Cryptographic controls**
8.3.1	The use of cryptographic controls must be based on the risk of unauthorized access of the information or information system that is to be protected. a) Cryptographic controls - Roles and responsibilities b) Acceptable use of cryptography

Purpose: To manage the use of cryptography for protecting the confidentiality and integrity of electronic information.

8.3.1 a) Cryptographic controls - Roles and responsibilities

The Office of Information Protection provides Government direction and leadership in the use of

cryptography and the provision of cryptographic services, such as those used for user registration services and *key management* services, by:

- Establishing policy and providing strategic direction on the use of cryptography;
- Setting standards for cryptographic algorithms and key length; and,
- Approving the use of cryptographic services.

The Office of Information Protection supports the use of cryptography in Government by:

- Maintaining an inventory of applications approved for use with cryptography; and,
- Providing technical advice on the use of cryptography.

Information Owners must document the use of cryptography in the *System Security Plan* for the information system.

8.3.1 b) Acceptable use of cryptography

The type and quality of cryptographic controls used in information systems must be based on a *Threat and Risk Assessment* and include consideration of:

- Confidentiality requirements, in accordance with sensitivity of the information;
- Integrity requirements (e.g., for financial payment instructions in excess of a specified dollar amount);
- Non-repudiation requirements (e.g., for proof of the occurrence or non-occurrence of an event);
- Authentication requirements (e.g., proof of identity);
- Other security measures (e.g., for 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* relating to the long-term storage of electronic information (e.g., recovery of encrypted data, long-term key maintenance).

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

Purpose: To provide trust-worthy *key management* processes for Government cryptographic services.

8.3.2 a) Management of cryptographic keys

The Office of Information Protection is responsible for approving key management standards and processes, including:

- Selection of cryptographic keys with sufficient lengths;
- Distribution, storage and periodic updating of cryptographic keys;
- Revocation of cryptographic keys (e.g., when a recipient changes job);
- Recovery of cryptographic keys that are lost, corrupted or have expired;

- ❖ Management of cryptographic keys that may have been compromised;
- ❖ Archival of cryptographic keys and the maintenance of cryptographic key history; and,
- ❖ Allocation of activation/de-activation dates.

8.4	**Information Systems Acquisition, Development and Maintenance – Security of system files**
8.4.1	The implementation of software on operational information systems must be controlled. a) Changes to operational information systems

Purpose: To prevent compromise of operational *information systems* from unauthorized software installation.

8.4.1 a) Changes to operational information systems

Information Owners and Information Custodians must implement procedures to control software installation on operational information systems to ensure that:

- ❖ Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- ❖ Operations personnel and end users have been notified of the changes, potential impacts and if required have received additional training;
- ❖ New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- ❖ Modifications to operational software are logged;
- ❖ The number of personnel able to perform the updates is restricted and kept to a minimum;
- ❖ Development code or compilers are not present on operational information systems; and,
- ❖ Vendor supplied software is maintained at the supported level.

Guidelines:

a) Pre-Implementation

Before an updated or new information system is implemented into the operational environment, checks should be performed to ensure that:

- ❖ A Threat and Risk Assessments has been carried out;
- ❖ A *Privacy Impact Assessment* has been performed and approved;
- ❖ Limitations of security controls are documented;
- ❖ Performance and capacity requirements can be met and support organizations have the capacity to maintain the information system;
- ❖ Development problems have been resolved successfully;
- ❖ The effects on existing operational information systems are known; and ,

- ❖ Arrangements for fall-back have been established if the updated or new information system fails to function as intended.

Before the updated or new information system is implemented into the operational environment:

- ❖ Communicate changes to users who may be affected by the change;
- ❖ Error recovery and restart procedures should be established;
- ❖ Business continuity plans should be developed or updated;
- ❖ Operating procedures should be tested;
- ❖ Users should be educated to use the information system correctly and securely; and,
- ❖ Computer operators/system administrators should be trained in how to run the information system correctly and securely.

b) Implementation

The installation process should include:

- ❖ Validating the load or conversion of data files;
- ❖ Installing executable code only, and not source code;
- ❖ Providing ongoing technical support;
- ❖ Implementing new or revised procedures/documentation;
- ❖ Discontinuing old software, procedures and documentation;
- ❖ Arranging for fall-back in the event of failure;
- ❖ Informing the individuals involved of their roles and responsibilities;
- ❖ Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and,
- ❖ Recording installation activity.

c) Post-implementation

Post-implementation reviews should include:

- ❖ The efficiency, effectiveness and cost of security control;
- ❖ Lessons learned and scope for improvements of security controls; and,
- ❖ Security incidents and mitigation.

8.4.2 Test data must be protected and controlled using the same procedures as for data from operational information systems. a) Protection of test data

Purpose: To protect *information* from unauthorized access or use.

8.4.2 a) Protection of test data Information Owners must implement procedures ensuring Sensitive or personal data from operational *information systems* is not used as test data;

- ❖ Using test data extracted from operational information systems must be authorized and logged to provide an audit trail;

- Test data is protected with controls appropriate to the sensitivity of the information and information system; and,
- Data from operational information systems is removed from the test environment once testing is complete.

8.4.3	Access control must be maintained for program source libraries. a) Protection of program source libraries.

Purpose: To protect *information systems* from unauthorized access or modification.

8.4.3 a) Protection of program source libraries

Information Owners and Information Custodians must implement procedures to control access to program source code for information systems to ensure that:

- Program source code is isolated and stored separately from operational information systems;
- *Privileged users* do not have unrestricted access;
- A change control process is implemented to manage updating of program source libraries and associated items;
- Program source code contained on any media must be protected; and,
- Accesses and changes to program source libraries are logged.

8.5	**Information Systems Acquisition, Development and Maintenance – Security in development and support processes**
8.5.1	Changes to software must be controlled by the use of formal change control procedures. a) Changes to software during information systems development b) Changes to software for operational information systems

Purpose: To ensure that *information systems* are not compromised from unauthorized changes to software.

8.5.1 a) Changes to software during information systems development

Information Owners must implement a change control process during development which includes:

- Requiring that change requests originate from authorized personnel;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

8.5.1 b) Changes to software for operational information system

Information Owners must implement a change control process during the maintenance phase including:

- Requiring that change requests originate from authorized personnel;
- Performing an impact assessment considering items such as the *System Security Plan* and proposed modifications;
- Documenting fallback plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating the System Security Plan and other system, operations and user documentation with the details of changes in accordance with records management policy;
- Maintaining version control for all changes to the software; and,
- Logging all requests for change.

8.5.2 Information systems must be reviewed and tested when operating system changes occur. a) Changes to the operating system

Purpose: To ensure *information systems* will not be disrupted or compromised.

8.5.2 a) Changes to the operating system

Information Custodians must notify information system Information Owners and other affected parties of operating system changes to allow:

- Sufficient time for the review and testing of information systems prior to implementation;
- Information system testing with the changes to the operating system in a separate (i.e. test) environment; and,
- Update of business continuity plans if required.

8.5.3 Modification of *commercial-off-the-shelf* software is limited to essential changes that are strictly controlled and documented. a) Modifying commercial-off-the-shelf software b) Applying vendor supplied patches and updates

Purpose: To reduce the *risk* of *information system* functionality loss.

Modifying commercial-off-the-shelf software

Other than vendor supplied patches, commercial-off-the-shelf (COTS) software must not be modified except in exceptional circumstances when needed for a critical business requirement.

This requirement must be documented and approved by the *Information Owner* and *Information Custodian*.

If changes to COTS software are required, the Information Owners and Information Custodians must determine:

- The effect the change will have on the security controls in the software;
- If consent of the vendor is required;
- If the required functionality is included in a new version of the software; and,
- If Government will become responsible for maintenance of the software as a result of the change.

If changes are made to COTS software the original software must be kept unaltered and 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 continues to operate as intended.

8.5.3 b) Applying vendor supplied patches and updates

A software update management process must be maintained for COTS software to ensure:

- The most up-to-date approved patches have been applied; and,
- The version of software is vendor supported.

8.5.4 Controls must be applied to limit opportunities for information leakage.
a) Preventing information leakage

Purpose: To protect *information* and *information systems* from unauthorized access, theft or misuse.

8.5.4 a) Preventing information leakage

Information Owners and Information Custodians must implement processes to reduce the opportunity for information leakage in information systems by:

- Scanning for malicious code;
- Monitoring resource usage in information systems;
- Identifying and limiting the trusted connections in and out of the Government network;
- Controlling third party network connections (e.g., only authorized traffic permitted);
- Using software that is considered to be of high integrity; and,
- Regular monitoring of information systems.

8.5.5	Controls must be applied to secure outsourced information system development. a) Outsourced information system development

Purpose: To ensure *information systems* perform as expected and meet security requirements.

8.5.5 a) Outsourced information system development

Information Owners and Information Custodians must consider the following when outsourcing information system development:

- Procurement policy for licensing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

Information Owners and Information Custodians must ensure that certification and accreditation requirements are met, including testing of the information system for common vulnerabilities and malicious code.

8.6	**Information Systems Acquisition, Development and Maintenance – Vulnerability management**
8.6.1	Regular assessments must be conducted to evaluate information system vulnerabilities and the management of associated risks. a) Vulnerability response processes

Purpose: To mitigate damage to Government operations resulting from exploitation of published vulnerabilities.

8.6.1 a) Vulnerability response processes

Vulnerabilities which impact Government *information systems* must be addressed in a timely manner to mitigate or minimize the impact on Government operations. Information Custodians 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 Chief Information Security Officer on progress in responding to vulnerabilities.

The Chief Information Security Officer must:

- Evaluate vulnerabilities and provide advice on appropriate Government responses;
- Monitor progress in responding to vulnerabilities;
- Publish summary reports on vulnerability response activities and costs; and,
- When required, initiate incident response processes to address vulnerabilities.

Chapter 9 – Information Security Incident Management

This chapter establishes requirements for reporting a possible breach of information security as quickly as possible. This includes establishing procedures and processes so that personnel understand their roles in reporting and mitigating security events.

Information security incident management policies identify mechanisms to detect and report when information security events occur and the directives for the consistent management of such events. The information collected about the events can be analyzed to identify trends and to direct efforts continually improve and strengthen the information security infrastructure of the Province.

9.1 Reporting information security events and weaknesses
9.1.1 Reporting information security events Information security events must be reported through appropriate management channels immediately.
9.1.2 Reporting security weaknesses Personnel using information systems must note and report any observed or suspected security weaknesses in those systems.
9.2 Management of information security incidents and improvements
9.2.1 Responsibilities and procedures Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.
9.2.2 Learning from information security incidents The types, volumes and costs of information security incidents must be quantified and monitored.
9.2.3 Collection of evidence Investigations into information security incidents must ensure evidence is collected, retained and presented in conformance with the rules for collection of evidence.

9.1	**Information Security Incident Management – Reporting information security events and weaknesses**
9.1.1	Information security events must be reported through appropriate management channels immediately. a) Information security event reporting

Purpose: To enable prompt response to information security event*(s)* and identify Government Information wide trends.

9.1.1 a) Information security event reporting

Employees must immediately report all suspected or actual information security events to the Office of Information Protection and to t their Departmental Manager/Director. Requirements for reporting events must be included in contracts and service agreements.

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

Purpose: To assist in maintaining the security of information systems all personnel must report observed or suspected *security weaknesses* in information systems.

9.1.2 a) Reporting security weaknesses

Departments must follow the Information Incident Management Process for responding to suspected or actual security weaknesses which includes:

- Reporting to the Chief Security Information Officer, Risk Management and Insurance Branch and the Office of Information Protection as appropriate. The response process must:
  - ✓ ensure all reports are investigated and handled in a secure, confidential manner, and,
  - ✓ ensure the individual who reported the weakness is advised of the outcome when the investigation is complete: and
- A user awareness program on information security advising personnel that:
  - ✓ They have a responsibility to report observed or suspected weaknesses to the Ministry point- of-contact,
  - ✓ Suspected or observed weakness must not be tried or tested, and,
  - ✓ Weaknesses should not be discussed, or made known, except through approved reporting channels.

9.2	**Information Security Incident Management – Management of information security incidents and improvements**
9.2.1	Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents. a) Information security incident management and response b) Information security incident investigation c) Monitoring and evaluating information security incident management and response

Purpose: To enable quick and orderly management of *information security incidents*.

9.2.1 a) Information security incident management and response

Departments must follow the Information Incident Management Process for reporting, managing, responding to and recovering from information security incidents. The process must include:

- A reporting process that includes the Chief Information Security Officer, Risk Management and Insurance Branch and the Office of Information Protection as appropriate;
- During the incident process, the Office of Information Protection will notify senior management of the incident and mitigation activities at the earliest possible time;
- Staff with incident management responsibilities must be appropriately trained and qualified, and their authorization for access to live systems and data delineated formally;
- Processes are established for handling different types of information security incidents, including immediate action for containment, response escalation and contingency plans; and,
- Incident response processes must be documented, tested and rehearsed regularly to evaluate their effectiveness.

9.2.1 b) Information security incident investigation

Information security incident investigation should be formalized and practiced in accordance with standard investigation techniques:

- Information security incident investigation processes include:
  - ✓ identification of the incident's cause,
  - ✓ planning of corrective action,
  - ✓ implementation of corrective action to prevent recurrence, and,
  - ✓ reporting action taken;
- Staff with responsibilities for information security investigations (investigating officer) must be aware of processes for securing potential evidence such as technology assets (e.g., PCs), audit logs, audit trails, voice mail and e-mail accounts for analysis and as potential evidence in legal proceedings;

- ❖ Inappropriate use of information and technology resources requires that within 48 hours the investigating officer contact:
  - ✓ in the case of an employee the individual's excluded Manager and PEI Public Service Commission Labour Relations, and,
  - ✓ in the case of a contractor or business partner the contract manager or relationship manager;
- ❖ When criminal activity is suspected, the investigating officer must ensure that the appropriate law enforcement authorities are contacted.;
- ❖ On resolution of an information security incident or weakness, the investigating officer must prepare a report that includes a detailed problem analysis, action(s) taken, and recommendations for corrective action or improvements; and,
- ❖ Information security incident reports must be submitted to Information Owners, Information Custodians, senior management, and Risk Management and Insurance Branch as part of security program management.

9.2.1 c) Monitoring and evaluating security incident management and response

The Information Security Branch, Office of Information Protection, is the centre of expertise and an essential capability in security incident protection, detection, response and correction where staff assigned responsibility for Information incident management receive special training in managing crises across the spectrum of potential incidents.

Information sharing with stakeholder and partner organizations, other provincial security incident response centres and national incident response centres should also be fostered. Information security incident response must be integrated within the broader requirements for business continuity and disaster recovery. Integration will simplify processes, maintain consistency and eliminate duplication.

Continuous improvement of security incident management processes includes:

- ❖ Monitoring incidents using statistical analysis of frequency, types and locations of security incidents;
- ❖ Analysis of incidents, responses and successful containment;
- ❖ Determining requirements for user awareness and training;
- ❖ Improving the security of information systems through monitoring and reporting; and,
- ❖ Integrating automated alarms and other security incident detection technology with user reporting, checking logs and auditing systems.

9.2.2 The types, volumes and costs of information security incidents must be quantified and monitored. a) Monitoring and evaluating information security incident management and response

Purpose: To identify and use information security incident trends to update the Government and supporting security processes.

9.2.2 a) Monitoring and evaluating information security incident management and response

The Chief Information Security Officer 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 Information Custodians and Ministry Information Security *Officers* of evolving security exposures and mitigation strategies;
- Evaluating the effectiveness of incident management, response and reporting; and,
- Evaluating the effectiveness of information security technologies.

The Chief Information Security Officer must provide incident information to the Office of Information Protection, Risk Management and Insurance Branch and the Office of the Comptroller; as appropriate.

9.2.3 Investigations into information security incidents must ensure evidence is collected, retained and presented in conformance with the rules for collection of evidence. a) Collection of evidence

Purpose: To ensure investigation processes preserve the integrity of evidence that may be required for legal or disciplinary action.

9.2.3 a) Collection of evidence

At the outset of an information security investigation it may not be known if legal or disciplinary actions will result. Evidence must only be collected by individuals authorized by the Chief Information Security Officer.

Investigative processes must follow the rules of evidence to ensure relevance, admissibility and materiality.

Information Owners and Information Custodians in receipt of a legal order to produce electronic

evidence must immediately contact the Chief Information Security Officer.

Chapter 10 – Business Continuity Management

This chapter provides direction from a security focus for planning the resumption of business or services where a man-made or natural disaster has occurred. Government organizations are required to be prepared and to re-establish business or services as swiftly and smoothly as possible. Business continuity plans include the evaluation of security risks in line with the directions set by the Office of Public Safety and the Department of Environment, Labour and Justice and government.

10.1 Information security aspects of business continuity management
10.1.1 Including information security in the business continuity management process There must be a managed process to ensure that business continuity programs address information security requirements
10.1.2 Business continuity and risk assessment A risk assessment must be conducted to identify information security events that may interrupt business processes.
10.1.3 Developing and implementing continuity plans including information security Business continuity plans must be developed to resume and maintain business operations to the required level following interruption to, or failure of, essential services.
10.1.4 Business continuity planning framework A government-wide framework of business continuity plans must be maintained to ensure consistent handling of information security requirements.
10.1.5 Testing, maintaining and re-assessing business continuity plans Business continuity plans must be regularly exercised and updated.

10.1	**Business Continuity Management – Information security aspects of business continuity management**
10.1.1	There must be a managed process to ensure that business continuity programs address information security requirements. a) Management of business continuity

Purpose: To ensure government can continue to deliver essential services despite damage, loss, or disruption of business processes.

10.1.1 a) Management of business continuity

Information Owners and *Information Custodians* must ensure business continuity and recovery plans address information security requirements consistent with the sensitivity of the information. Processes for establishing business continuity and recovery plans are detailed in the Government of Prince Edward Island Business Continuity Program Manual.

The Information Custodian must maintain the business continuity and recovery plans for *information systems* as part of the *System Security Plan*.

10.1.2	A risk assessment must be conducted to identify information security events that may interrupt business processes. a) Business continuity risk assessment b) Business continuity strategy

Purpose: To ensure that business continuity planning processes consider information security *risks*.

10.1.2 a) Business continuity risk assessment

The process for analyzing and assessing business impacts, including those for information security risks, is detailed in the Government of Prince Edward Island Business Continuity Program Manual – section 2 – Understanding the Organization.

10.1.2 b) Business continuity strategy

The process for developing a business continuity strategy is detailed in the Government of Prince Edward Island Business Continuity Program Manual – section 1 – Business Continuity Program Management.

10.1.3 Business continuity plans must be developed to maintain and resume business operations to the required level following interruption to, or failure of, essential services. a) Business continuity plans

Purpose: To ensure that *essential services* can be restored after the damage, loss, or disruption of business processes.

10.1.3 a) Business continuity plans

Requirements for business continuity plans are defined the Government of Prince Edward Island Business Continuity Program Manual - section 4 – Developing and Implementing a Business Continuity Response. The process for developing and maintaining business continuity plans is detailed in the Government of Prince Edward Island Business Continuity Program Manual.

10.1.4 A government-wide framework of business continuity plans must be maintained to ensure consistent handling of information security requirements. a) Co-ordination of business continuity plans

Purpose: To ensure consistency and completeness of the information security components of business continuity plans.

10.1.4 a) Co-ordination of business continuity plans

Information Owners and Information Custodians must ensure business continuity plans:

- Include the sensitivity of information assets to identify critical business operations;
- Use government-wide frameworks and processes; and,
- Use information security processes which maintain approved security levels.

The Office of Public Safety and the Department of Environment, Labour and Justice must coordinate government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes.

The Office of Information Protection is responsible for protecting the privacy, confidentiality, integrity and availability of government's electronic information. This responsibility includes providing expert advice to Office of Public Safety and the Department of Environment, Labour and Justice on information security aspects of business continuity plans.

10.1.5 Business continuity plans must be regularly exercised and updated. a) Business continuity plan exercising and maintenance

Purpose: To ensure business continuity plans are current, functional and address information security requirements.

10.1.5 a) Business continuity plan exercising and maintenance

Requirements for exercising and maintaining the business continuity plan are defined in the Government of Prince Edward Island Business Continuity Program Manual – section 3 – Determining Business Continuity Strategy and Tactics.

Chapter 11 – Compliance

The chapter describes requirements for verifying that information systems comply with relevant statutory, regulatory, and information security contractual clauses. Compliance policies identify what to do to ensure that the Province is in compliance with applicable laws and policies. Processes to monitor the extent in which information systems follow policies include conducting security reviews, assessments and the systematic analysis of logged information.

11.1 Compliance with legal requirements
11.1.1 Identification of applicable legislation The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained
11.1.2 Intellectual property rights Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing
11.1.3 Safeguarding of organizational records Government records must be protected from loss, destruction and falsification.
11.1.4 Data protection and privacy of personal information Security controls must be applied to protect data and personal information in accordance with relevant legislation.
11.1.5 Prevention of misuse of information processing facilities Controls must be in place to deter misuse of information systems
11.1.6 Regulation of cryptographic controls Cryptographic controls must be used in conjunction with relevant agreements, laws and regulations.
11.2 Compliance with security policies and standards
11.2.1 Compliance with security policy and standards Management must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards.
11.2.2 Technical compliance checking Information systems must be regularly checked for compliance with security policies and standards.
11.3 Information systems audit considerations
11.3.1 Information systems audit controls Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.
11.3.2 Protection of information systems audit tools Access to system audit tools must be controlled to prevent misuse or compromise

11.1 Compliance – Compliance with legal requirements
11.1.1 The statutory, regulatory and contractual requirements for each information system must be explicitly defined, documented and maintained. a) Legal requirements

Purpose: To ensure that the legal requirements of information systems are documented.

11.1.1 a) Legal requirements

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

- Identified and documented when commencing a system development or enhancement initiative;
- Reviewed prior to, or concurrent with, changes to legislation, regulation or policy; and,
- Explicitly identified in contracts and service agreements, and included in:
  - ✓ Privacy Impact Assessments,
  - ✓ Threat and Risk Assessments,
  - ✓ System Security Plans,
  - ✓ Risk Management Plans, and,
  - ✓ Business Continuity Plans.

11.1.2 Controls must be implemented to ensure compliance with legal, regulatory and contractual restrictions on the use of material with respect to intellectual property rights and proprietary software licensing. a) Intellectual property rights of external creators and owners b) Intellectual property rights for Government assets

Purpose: To protect the intellectual property rights of information and software creators and owners.

11.1.2 a) Intellectual property rights of external creators and owners

Information Owners and Information Custodians must protect intellectual property by:

- Ensuring that information and software is only acquired from reputable vendors;
- Maintaining proof or evidence of ownership or right to use;
- Adhering to the terms and conditions of use associated with intellectual property;
- Ensuring the maximum number of users permitted is not exceeded;
- Implementing processes to detect unlicensed information (e.g., ISO standards documents) and software or expired licenses;
- Requiring the removal of unlicensed information and software from Government information systems;
- Informing personnel of Government policies including those pertaining to appropriate use of Government resources;

- ❖ Ensuring licensed intellectual property is securely removed from electronic media prior to media disposition; and,
- ❖ Complying with terms and conditions for information and software obtained from public networks (e.g., "free for personal use only", open source).

11.1.2 b) Intellectual property rights for Government assets

Policy for the intellectual property of Government information assets is in Core Policy and Procedures Manual 6.3.4 – Corporate Supply and Disposal Arrangements which is managed by the Office of Information Protection.

11.1.3 Government records must be protected from loss, destruction and falsification a) Records management

Purpose: To ensure the Government policy and supporting processes enable compliance with legal and policy requirements for Government *records*.

The *Archives and Records Act* speaks to requirements for the disposal of Government records.

11.1.4 Security controls must be applied to protect data and personal information in accordance with relevant legislation. a) Data and personal information protection

Purpose: To ensure the Government policy and supporting processes enable compliance with legislation.

11.1.4 a) Data and personal information protection

The *Freedom of Information and Protection of Privacy Act* requires personal information to be protected using 'reasonable security arrangements'.

Policy requirements for protecting data and personal information are found in FOIPP Guidelines and Practices located at http://www.gov.pe.ca/law/regulations/index.php3#F.

The Government Information Security Policy includes detailed controls which enable and support the protection of Government information and information systems.

11.1.5 Controls must be in place to deter misuse of information systems. a) Deterring unauthorized and inappropriate use of information systems

Purpose: To ensure *personnel* do not create security exposures through unauthorized or inappropriate use of information systems.

11.1.5 a) Deterring unauthorized and inappropriate use of information systems

Information Owners and *Information Custodians* must monitor *information system* usage to prevent, detect and respond to unauthorized or inappropriate use by:

- Ensuring audit logs contain sufficient detail to detect and trace inappropriate usage;
- Implementing processes to analyze audit logs to identify potential misuse of information systems;
- Implementing system rules to prevent access to undesirable Internet sites;
- Implementing content inspection and filtering tools (e.g., for e-mail and web traffic);
- Ensuring that security incidents are investigated in accordance with policy; and,
- Determining, in consultation with the Public Service Commission, if disciplinary action, including dismissal, cancellation of contract and/or other legal remedies are warranted for personnel who have made unauthorized or inappropriate use of information system resources.

Prior to implementing *information system* monitoring processes Information Owners and Information Custodians must ensure:

- Monitoring activities will be compliant with legal, policy and contractual requirements and obligations;
- Personnel are informed that specific activities may be monitored; and,
- Access to data gathered through monitoring processes is restricted on a 'need to know' and '*least privilege*' basis to the fewest possible number of users.

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

a) Regulation of cryptographic controls

Purpose: To prevent inappropriate use and unregulated importing or exporting of cryptographic controls.

11.1.6 a) Regulation of cryptographic controls

When cryptographic controls are used, Information Owners and Information Custodians must:

- Ensure that the use of cryptographic control(s) is supported by an Information *Security Threat and* Risk Assessment;
- Consult with the Office of Information Protection 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 Security Officer; and,
- When 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.

The Office of Information Protection will:

- Develop and document cryptographic key management processes;
- Provide guidance and assistance to departments and agencies in the selection and use of cryptographic controls; and,
- Establish and publish cryptographic standards.

11.2 Compliance – Compliance with security policies and standards
11.2.1 Management must ensure security procedures are followed in their areas of responsibility and facilitate regular reviews to ensure compliance with security policies and standards. a) Compliance with security policies and standards b) Review of controls c) Review of implementation of information incident report recommendations

Purpose: To ensure compliance of *information systems* with Government policy, requirements and standards.

11.2.1 a) Compliance with security policies and standards

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

- Conducting periodic self assessments;
- Ensuring personnel receive regular information security awareness updates; and,
- Initiating independent assessments, reviews or audits to assess compliance to policy.

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

- Determine cause(s);
- Assess the threats and *risks* of non-compliant processes;
- Document the marginal risks; and where required; and,
- Develop plans to implement corrective action.

11.2.1 b) Review of controls

Departments must develop an annual plan which identifies information systems scheduled for a security review in each fiscal year. The information systems to be reviewed in each year should be:

- Determined in conjunction with and endorsed by the Standing Committee on

Corporate Management.

Departments must ensure that mission critical information systems are reviewed at least every three years.

11.2.1 c) Review of implementation of information incident report recommendations
Information Owners and Information Custodians must ensure that recommendations from information incident reports are addressed.

Chief Information Security Officer may perform compliance reviews or audit of the implementation of recommendations from information incident reports, when necessary. Ministry Chief Information Officer must ensure that Information Owners and Information Custodians support the audit activities.

11.2.2 Information systems must be regularly checked for compliance with security policies and standards.
a) Technical compliance checking
b) Authorization to conduct technical compliance checking
c) Reporting results

Purpose: To determine if technical controls meet established Government standards.

11.2.2 a) Technical compliance checking

Information Custodians must regularly test information system technical control compliance by using automated tools to:

- Detect network intrusion;
- Conduct penetration testing;
- Determine if information system patches have been applied;
- Confirm that system technical controls have been implemented and are functioning as designed; and,
- Perform technical compliance checking as part of the system change management process to verify that unauthorized connections and/or systems changes have not been made.

11.2.2 b) Authorization to conduct technical compliance checking

Managers responsible for technical compliance checking and Information Custodians must ensure that:

- *Information Owners* and operations personnel are consulted prior to initiating tests;
- The Chief Information Security Officer is notified prior to testing to prevent triggering false security alarms from the infrastructure; and,

- Automated testing of operational systems are conducted by authorized personnel.

11.2.2 c) Reporting results

Managers responsible for technical compliance checking and Information Custodians must:

- Assess results of testing and promptly develop action plans to investigate and mitigate identified exposures in consultation with the Office of Information Protection;
- Provide Information Owners and the Chief Information Security Officer with copies of test results and action plans; and,
- Maintain records, in accordance with established records schedules, of tests for subsequent review by internal and external auditors.

Guidelines:

The Chief Information Security Officer should:

- Develop and maintain testing processes for authorizing/conducting tests, storing results and building on previous testing experience; and,
- Provide summarized quarterly reports to the Chief Information Officer on the status and results of testing.

Departments must consult with the Departmental Information Technology Architects prior to issuing Requests for Proposal or contracts for technical compliance checking.

11.3 Compliance – Information systems audit considerations
11.3.1 Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes. a) Management of information systems compliance checking

Purpose: To prevent *compliance checking* activities from causing unplanned disruptions to operational *information systems*.

11.3.1 a) Management of information systems compliance checking

Prior to commencing compliance checking activities such as audits*, risk and controls reviews, monitoring* or *security reviews* of operational information systems, the Manager responsible for the compliance checking activity, Information Owners and Information Custodians must define, document and approve the activities by:

- Determining the scope, duration and level of detail of the compliance checking activity;
- Limiting access rights to operational information systems for compliance checking personnel to “read only”;
- Determining handling requirements for copies of files made by compliance checking personnel including:

- ✓ establishing a separate environment for the analysis of files,
- ✓ restricting access to those files,
- ✓ logging the accesses made to those files, and,
- ✓ erasing files at the conclusion of compliance checking activities unless needed to support report findings;

❖ Identifying special testing or processing which may impact the operational information system (e.g., network penetration tests, server vulnerability assessments) and by:

- ✓ notifying the Chief Information Security Officer prior to compliance checking activities to prevent triggering false security alarms from the infrastructure, and,
- ✓ scheduling tests to minimize disruption; and,

❖ Requiring that personnel conducting compliance checking activities maintain a segregation of duty from the operational information systems being checked.

11.3.2 Access to system audit tools must be controlled to prevent misuse or compromise. a) Protection of information system audit tools

Purpose: To minimize *risks* to information and information systems from inappropriate use of audit tools.

11.3.2 a) Protection of information system audit tools

Managers responsible for compliance checking activities and Information Custodians must control the use of audit tools by:

❖ Restricting access to authorized personnel who have a *need-to-know*;

❖ Installing or enabling specialized audit tools for the duration required by the compliance checking activity;

❖ Removing information system access at the conclusion of the compliance checking activities; and,
Notifying the Chief Information Security Officer

Appendix A – Glossary

1. ***Ad hoc timework*** – occasional telework that may not have a formal agreement in place. (See: ***telework***)

2. ***Application*** (business application) – a collection of computer hardware, computer programs, databases, procedures and knowledge workers that work together to perform a related group of services or business processes.

3. ***Assets*** – for the purposes of Government information in all forms and media, networks, hardware, software and application systems.

4. ***Audit*** – is an examination of the facts to render an opinion and would include testing evidence to support the opinion.

5. ***Audit logs*** – includes all types of event logs including (but not limited to) security, audit, application, access and network across all operating system platforms.

6. ***Authentication*** – the verification of the identity of a person or process.

7. ***Availability*** – information or information systems being accessible and usable on demand to support business functions.

8. ***Business Continuity Plan*** (BCP) – the procedures and information necessary for the timely recovery of essential services, programs and operations, within a predefined timeframe. The BCP includes the recovery following an emergency or a disaster that interrupts an operation or affects service or program delivery.

9. ***Business information systems*** – internal administrative and productivity information systems that support the organization such as e-mail, calendars and financial systems.

10. ***Capacity management*** – the process of determining the system capacity needed to deliver specific performance levels through quantification and analysis of current and projected workload.

11. ***Certification*** – See: ***security certification***

12. ***Chief Information Security Officer*** – responsible for protecting the confidentiality, integrity and availability of Government information.

13. ***Commercial-off-the-shelf*** (COTS) – commercially available products that can be purchased and integrated with little or no customization.

14. ***Compliance checking*** – includes: an audit; risk and controls review; security review; and monitoring of an information system.

15. ***Confidentiality*** – information is not made available or disclosed to unauthorized individuals, entities or processes.

16. ***Control*** – (of a record) means the power or authority to manage the record throughout its life cycle, including restricting, regulating and administering its use or disclosure. Where the information in a record directly relates to more than one public body, more than one public body may have control of the record. (Contact your departmental FOIPP Coordinator for further information.)

17. ***Cryptographic Keys*** – a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of data into encrypted data and the transformation of encrypted data into data during decryption. The cryptographic algorithm ensures that only someone with knowledge of the key can reproduce or reverse the transformation of data.

18. ***Cryptography*** – the discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.

19. ***Custody*** – (of a record) means having physical possession of a record, even though the public body does not necessarily have responsibility for the record. Physical possession normally includes responsibility for access, managing, maintaining, preserving, disposing and providing security.

20. ***Data*** – See: ***Information***.

21. ***Digital signing*** – refers to an attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the users' private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the 'digitally signed' document) that can only be decrypted by applying the user's public key. (Also digitally signing, digital signature)

22. ***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. The DRP is part of a ministry's overall business continuity plan (Business Continuity Plan or BCP).

23. ***Disposition*** – the actions taken regarding information that is no longer needed to support on-going administrative and operational activities in accordance with

an approved Records Management Schedule. Directions may include destroy, transfer to the Provincial Archives, transfer to inactive records storage space, or retain permanently in unit. (Contact your departmental Records Liaison Officer for further information).

24. ***Electronic agent*** – a computer program, or other electronic means, used to initiate an activity or to respond to electronic information, records or activities in whole or in part without review by an individual at the time of the response or activity.

25. ***Electronic commerce*** – the exchange of information between Government and internal and external stakeholders independently of either participant's computer system. E.g., electronically accessing forms, obtaining payments, sending invoices, receiving tax returns, placing orders and receiving transaction acknowledgements.

26. ***Electronic messages*** – includes all forms of electronic messaging such as e-mail, voice mail, instant messaging etc.

27. ***Employee*** – is a person appointed under the Public Service Act.

28. ***Essential services*** - Essential business processes are those processes defined as mission-critical and business- priority and essential to delivery of outputs and achievement of business objectives. Business activities and resources are the essential elements that combine to make up each essential business process.

29. ***Event*** – is an identified occurrence of a system or service state indicating a possible breach or failure of safeguards, or a previously unknown situation that may be security relevant.

30. ***External Party*** – a person external to "Government" as defined within the Financial Administration Act.

31. ***Fault*** – an error or failure in either software or hardware.

32. ***Firmware*** - programming that is inserted into programmable read-only memory becoming a permanent part of a computing device.

33. ***Government information*** – means all recorded information, regardless of physical format, that is received, created, deposited or held by or in any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of Prince Edward Island. Government records include machine-readable records, data stored in information systems, film, audio and audiovisual tapes, etc. Government records include cabinet ministers' records that are created and/or accumulated and used by a Minister (or a Minster's office) in developing, implementing and/or administering programs of Government. Government records do not include legislative records (records created and/or

accumulated and used by an individual or an office in the administration of the Legislative Assembly of Prince Edward Island by a Member of the Legislative Assembly). The retention and final disposition of most Government records is governed by the *Archive and Records Act.*

34. ***Government network*** – See: ***Network Infrastructure***.

35. ***Government records*** – See: ***Government information***

36. ***Hardware*** – includes (but not limited to) servers, desktop computers, printers, scanners, fax machines, photocopiers, multi function devices, routers, communications and mobile equipment, cell phones, PDAs, BlackBerries, removable media.

37. ***Information*** – the data in context. The meaning given to data or the interpretation of data, based on its context, for purposes of decision making. (See: ***Government Information***).

38. ***Information asset*** – includes all data, information and intellectual property.

39. ***Information classification label*** – a designation indicating the information classification, e.g., "Public", "Normal", "High". (As per Treasury Board section 16.02 Security Policies, attachment 16.02-1)

40. ***Information Custodians*** – maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

41. ***Information Owners*** – have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

    Within the Government of Prince Edward Island, information ownership flows from the Crown to Government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

42. ***Information processing facilities*** – the physical location housing any information processing system, service or infrastructure; this includes storage facilities for equipment not yet deployed or awaiting disposal.

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

44. ***Information security activities*** – management and technology programs to protect Government information assets.

45. ***Information security architecture*** – a strategy that consists of layers of policy, standards and procedures and the way they are linked to create an environment in which security controls can be easily established.

46. ***Information Security Event*** – See: ***event***.

47. ***Information Security Incident*** – is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (ISO/IEC TR 18044:2004) Information security incidents may include but are not limited to:
    Inappropriate use of Government resources causing a service disruption;
    Breaches of privacy and/or confidentiality;
    Denial of service;
    Detection of network probing;
    Detection of malicious code, e.g., virus, worm or Trojan horse;
    Errors due to incomplete or inaccurate data;
    Outgoing network traffic not associated with typical business processing;
    Repeated attempts of unauthorized access;
    Repeated attempts to e-mail unknown internal accounts;
    System activity not related to typical business processing; and,
    System failures and loss of service.

48. **Information System –** any equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and that includes computer software, firmware and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems and associated equipment.

49. ***Information technology asset*** – includes owned and leased technology hardware (i.e. physical items), owned or licensed software and related or supporting services.

50. ***Information technology resources*** – information and communications technologies, including data, information systems, network services (e.g., Web services; messaging services); computers (e.g., hardware, software); telecommunications networks and associated assets (e.g., telephones, facsimiles, cell phones, laptops, personal digital assistants).

51. ***Information type*** – information classes or groupings based on function, usage, attributes or other commonality. E.g., personnel records, invoices, or system

documentation are information types. Address, name, or birth date are examples of discrete data elements.

52. ***Integrity*** – the characteristic of information being accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

53. ***Intellectual property*** – intellectual property refers to the category of intangible (non-physical) property consisting primarily of rights related to copyrighted materials, trademark, patent and industrial design.

    Intellectual property rights are associated with a wide range of products of the human intellect, such as training manuals, publications, map products, videos and computer software. It is important to keep clear the distinction between the items that give rise to intellectual property, such as the manuals and software, and the intellectual property itself, which is the set of rights arising from the creation and development of the items. Simply put, the items are the copies of a particular book, whereas the intellectual property is the copyright in that book.

54. ***Key Management*** – the processes for the generation, exchange, storage, safeguarding, use, vetting and replacement of cryptographic keys.

55. ***Least Privilege*** – a security principle requiring that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

56. ***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 can include viruses, worms, Trojans, spyware and denial of service attacks.

57. ***Media*** – Material that information is written to and stored on. See: Records.

58. ***Message integrity*** – the assurance of unaltered transmission and receipt of a message from the sender to the intended recipient to maintain the completeness, accuracy and validity of the information contained in the message.

59. ***Mission Critical*** – processes that, should they not be performed, could lead to loss of life (“safety”), personal hardship to citizens, major damage to the environment, or significant loss in revenue and/or assets.

60. ***Mobile code*** – multiplatform computer code that can be downloaded or transmitted across a network that runs automatically on a computer with little or no user interaction.

61. ***Mobile code technology*** – software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, VBScript, ActiveX).

62. ***Mobile computing service*** – a service that provides access to Government systems from Mobile Computing Devices. Distinct from Remote Access Services in that the mobile computing service provides product-specific access to limited applications rather than full standard network access (e.g., BlackBerry® Enterprise Server service).

63. ***Mobile devices*** – portable self-contained electronic devices, including portable computers (e.g., laptops), personal digital assistants (PDAs), cell phones, digital cameras, etc.

64. ***Monitoring*** – a regular/ongoing check on aspects of operations to identify and correct deviations from policies and standards.

65. ***Multi factor authentication*** – this is combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret - something the person knows Token - something the person has Biometric - something the person is.

66. ***Need to Know principle*** – a privacy principle where access is restricted to authorized individuals whose duties require such access. Individuals are not entitled to access merely because of status, rank or office. The need- to-know principle may be implemented in various ways. These include physically segregating and controlling access to certain records, listing individuals who may access certain records, or installing access controls on automated information systems. The need-to-know principle is especially important in protecting the privacy of individuals as required by the Freedom of Information and Protection of Privacy Act.

67. ***Network Address Spoofing*** – forging or faking source network addresses with the intent to obscure, hide or impersonate the actual source device.

68. ***Network infrastructure*** – the equipment, information systems and cabling systems used to establish a communication network between Information Systems. Includes routers, switches, hubs, firewalls, transmitters, fibre optic cable and copper cable.

69. ***Network management information*** – the information used to manage network infrastructure, including traffic statistics, counters and logs.

70. ***Network pathways and routes*** – the physical and logical pathways that comprise the connections within the network infrastructure.

71. ***Network security boundary*** – the logical or physical boundary between networks of differing security protection requirements. Network access control devices demark the network security boundaries.

72. ***Network security zone*** – a logical entity containing one or more types of services and entities of similar security requirements and risk levels.

73. ***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.

74. ***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.

75. ***Network service provider*** – a provider of network services to Government which may be internal or external to Government.

76. ***Non-repudiation*** - the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

77. ***Non-retrievable*** – unable to recover the data from any media in any form.

78. ***Outside authorities*** – include law enforcement, fire departments, other emergency response authorities, utilities and telecommunications providers.

79. ***Password management system*** –An automated process which enforces password rules.

80. ***Personnel*** – includes employees and other individuals (e.g., contractors, consultants, volunteers, third-party organizations).

81. ***Portable storage devices*** – electronic media including but not limited to laptop and notebook computers, removable hard drives, USB mass storage devices (flash drives, jump drives, memory sticks, memory cards, thumb drives, MP3 players, iPODs and PDAs), zip drives, CDs, DVDs, tapes and diskettes.

82. ***Positional user identifier*** (userid) – is a unique system userid assigned to a persistent function or job in circumstances where the personnel filling the job are transitional. Positional userids are issued to a Manager or supervisor who is accountable for the day to day management and assignment of the userid to

individuals. E.g., a positional userid could be used if a receptionist position was temporarily filled by short term staff from an employment agency. In these limited circumstances use of positional userids can avoid creating new userids for short term staff.

83. ***Privacy*** – the right of an individual to be secure from unauthorized disclosure of information about oneself that is contained in documents.

84. ***Privacy Impact Assessment*** – an assessment that is conducted to determine if a new enactment, system, project or program meets the requirement of Part 3 of the Freedom of Information and Protection of Privacy Act.

85. ***Privileged operations*** – permissions which allow the user to alter access rights and structures of information systems and/or services.

86. ***Privileged users*** – 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.

87. ***Privileges*** – See: ***privileged operations***.

88. ***Reception Zone*** – an area where the initial contact between the public and the ministry occurs, where services are provided, information exchanged and access to restricted zones is controlled.

89. ***Record*** – includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise.

90. ***Remote access*** – the act of using a remote access service to connect to the Government network or Government systems.

91. ***Remote access service*** – a service that provides network access to the Government network or Government systems from a remote location, e.g., the Government VPN service.

92. ***Requirements phase*** – one component of the System Development Life Cycle. Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable, testable and related to the business need or opportunity.

93. ***Restricted Access Operations Zone*** – a controlled area where access is limited to persons who work there and to escorted visitors. It is usually a standard working area and offices.

94. ***Restricted Access Security Zone*** – a strictly controlled area where access is limited to authorized persons and to properly escorted visitors.

95. ***Risk*** – Potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.

96. ***Screening*** – to verify facts about individuals related to their identity, professional credentials, previous employment, education and skills.

97. ***Secured Path*** – a network path that has been protected from eavesdropping, intrusion and data tampering.

98. ***Security categories*** – inform employees how to handle records in order to protect them and determine requirements for marking, storage, transport, transmittal and destruction.

99. ***Security certification*** – a comprehensive assessment of the management, operational and technical security controls in an information system, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

100. ***Security infrastructure*** – the complete set of information security-related systems, policies, standards, guidelines, procedures, resources and physical implementations of information security administration.

101. ***Security Management Systems*** – systems that collect, store and manage configuration and operational information about network devices. Includes configuration management databases and log management systems.

102. ***Security posture*** – the security status of the technical infrastructure and information systems to known vulnerabilities and attacks.

103. ***Security review*** – an independent review with the scope focused on the security framework over the business processes, application and operating environment. Reviews are distinguishable from audits in that the scope of a review is less than that of an audit and therefore the level of assurance provided is lower.

104. ***Security Threat and Risk Assessment*** – a component of a risk analysis specifically aimed at identifying security exposures.

105. ***Security weakness*** – a weakness in an application, procedure or process that may result in a security incident.

106. ***Security zone*** – See: ***reception zone***, ***restricted access operations zone***, ***restricted access security zone***.

107. ***Software*** – includes (but not limited to) application and system software, development tools, utilities.

108. ***Status Accounting*** – a comparison of configuration data stored in a configuration database to actual device configuration. Used to ensure that recorded configuration data matches actual device configuration.

109. ***System Security Plan*** – repository to document security information and controls (management, operational and technical) regarding an application system.

110. ***System Utility Programs*** – Tools that when misused can subvert system, access and application controls E.g. network sniffers, password crackers, port scanners, root kits and vulnerability assessment scanners.

111. ***Systems documentation*** – detailed information about a system's design specifications, its internal workings, and its functionality including schematics, architectures, data structures, procedures and authorization processes.

112. ***Systems privileges*** – permissions which allow the user to alter access rights and structures of information systems.

113. ***Telework*** – a working arrangement where employees work away from their official workplace for a portion of their regular work week (BC Public Service Agency, Flexible Work Options). (See: ***ad hoc telework***)

114. ***Third party*** – includes external party and includes a person outside the direct reporting structure of the Information Owner or Information Custodian. E.g., an individual, a business or organization, personnel from another branch of Government, or another level of Government.

115. ***Threat*** – in the security context, any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate, accidental or of natural origin. (See: ***vulnerability*** and ***event***).

116. ***Trusted path*** – See: ***secured path***

117. ***Two person access control*** – a system of requiring the presence of two authorized persons to perform an action, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. For example, a locked cabinet or safe which has two locks requiring action by two persons, each with a unique key or code and which requires the presence of two persons to access or open.

118. ***Uninterruptible power supply*** – a backup power source for computers and computer networks to insure on- going operation in the event of a power failure.

119. ***User*** – all persons authorized to access the Government electronic mail service including employees and contractors.

120. ***User identifier*** – is the unique personal identifier that is authorized to access the Government computers and information systems.

121. ***Vulnerability*** – in the security context, a weakness in security procedures, processes, or controls that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

122. ***Wireless Local Area Network*** – a Local Area Network that uses wireless transmission media.

123. ***Zone*** – See: ***reception zone***, ***restricted access operations zone***, ***restricted access security zone***.