Northwest Territories **Standards**

GNWT
INFORMATION TECHNOLOGY
Electronic Information Security

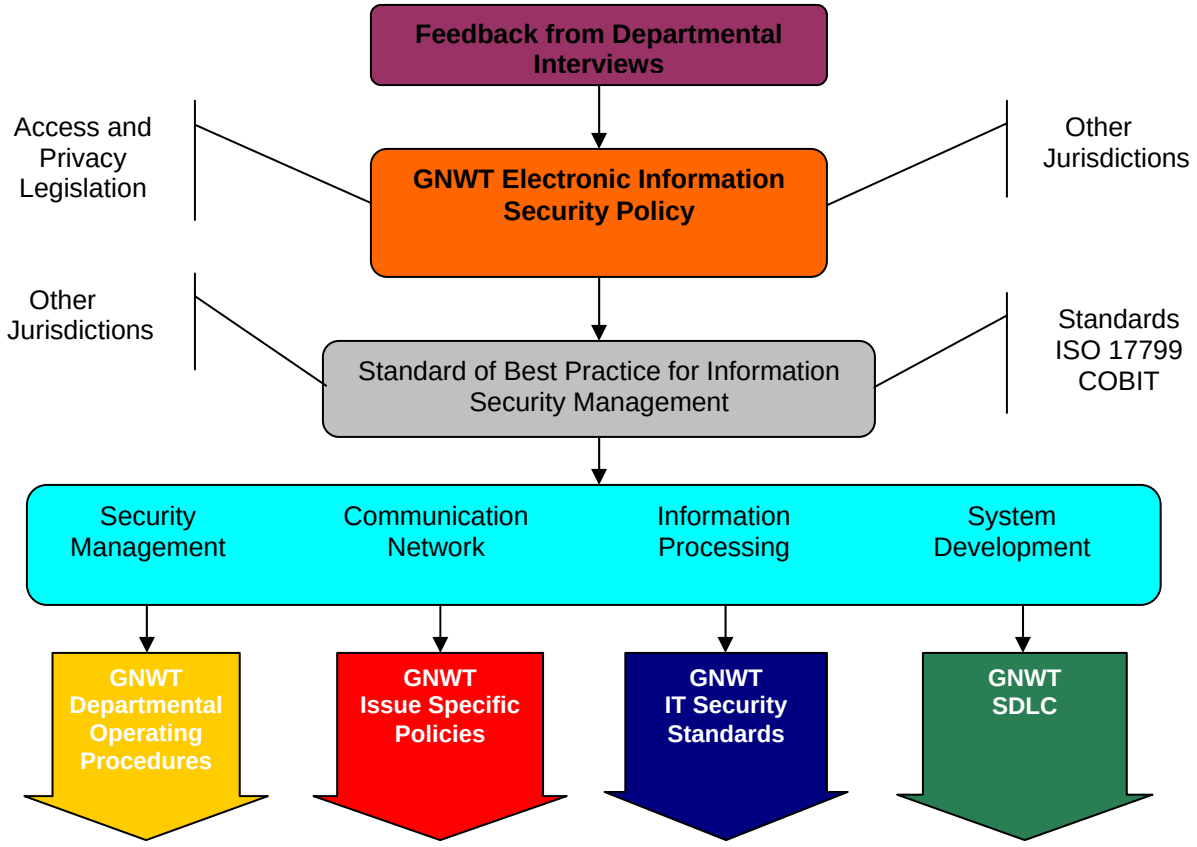
Table of Contents

INTRODUCTION

This document sets out the Government of the Northwest Territories [**GNWT**] Standard of Best Practice for Information Security Management. The Electronic Information Security Community of Interest group adopted this document from Government of Manitoba. The new Electronic Information Security Committee will be responsible for revisions as required. It is a guide for IT Security management in the GNWT.

The Standard of Best Practice is based upon industry standards for IT Security management including ISO17799 and COBIT (Controlled Objects for IT). This document will assist GNWT departments in improving their IT Security environments. This document provides a framework for the IT Security Policy, Standards, Procedures, and Guidelines. Figure 1.0 shows how the Standard of Best Practice supports the Government's IT security framework.

Figure 1.0: Best Practice Relationship to IT Security Policy



Northwest Territories **Standards**

GNWT
INFORMATION TECHNOLOGY
Electronic Information Security

The GNWT Standard of Best Practice provides a practical, business focused standard for information security all government departments can achieve.

The GNWT Standard of Best Practice has four main areas. They are:

- **Security Management (SM)** – which describes how information security should be managed
- **Communications Networks (CN)** – which concentrates on the security of the data networks
- **Information Processing (IP)** – which covers computer environments that support business applications
- **Systems Development (SD)** – which addresses the development of business applications

This document is for individuals required to understand what constitutes best practices in information security management. These include:

- Senior Management
- IT Security Officers
- IT Staff
- Contractors & Consultants
- Business owners and managers
- Other specialists involved in information security

Each main area of the Standard of Best Practice includes a number of sections. Each section includes an objective and standard of best practice. Some sections appear in more than one area.

The Standard of Best Practice specifies what security practices should be considered when managing IT assets. Controlling risks requires information security to be managed in a consistent way. Best practices must be observed when planning, developing, installing, running, using, and maintaining information systems. By applying the Standard of Best Practice, departments can implement systems that take into account confidentiality, integrity, and availability requirements.

SECURITY MANAGEMENT

The GNWT requires clear direction and commitment from senior management, the allocation of adequate resources, and effective arrangements for promoting good information security practices to limit risks associated with information systems under its control.

SM 1.0 High Level Direction

Senior management must give clear direction to achieve a consistent standard of best practice for information security across the GNWT. This section covers management's direction on, and commitment to, information security. It specifies how this direction and commitment will be communicated to individuals with access to the GNWT's information and systems.

SM1.1 Management Commitment

Objective

To set the GNWT's direction on, and commitment to, information security as outlined in the Knowledge Management Study.

Standard of Best Practice

The GNWT has established a security policy.

Senior management including Deputy Ministers, Directors or equivalent are committed to:

- achieving high standards of IT governance
- treating information security as a critical business issue and creating a positive security environment
- demonstrating to third parties that the organization deals with information security in a professional manner
- applying fundamental principles such as assuming ultimate responsibility for information security, implementing controls proportionate to risk and achieving individual accountability

Senior management has shown their commitment to information security by:

- becoming directly involved in high-level information security arrangements, such as an information security policy
- providing high-level control
- allocating sufficient resources to information security

SM1.2 Security Policy

Objective

To document the GNWT's direction on, and commitment to information security and communicate it to all individuals with access to the Government's information and systems.

Standard of Best Practice

The GNWT's direction on and commitment to information security is established in a high-level information security policy applying across Government.

The policy includes a:

- statement of direction from senior management supporting the goals and principles of information security
- highlight of business risks associated with breakdowns in information security
- definition of information security, responsibilities, and the high-level principles to be observed
- list of key activities to be undertaken, including carrying out data classifications and risk analyses, safeguarding important records and reporting suspected security weaknesses
- requirement that information is protected in terms of its requirements for availability, integrity and confidentiality
- statement on the need to comply with software licenses and other legal, regulatory and contractual obligations
- statement prohibiting unauthorized or personal use unacceptable under the Network Usage Policy of the GNWT
- statement prohibiting obscene, racist or otherwise offensive statements (for example via e-mail or over the Internet
- statement that disciplinary action may be taken against individuals who violate its provisions

The policy document, ratified by Informatics Policy Committee (IPC), will be made available to all individuals with access to GNWT information or systems. The policy will be reviewed every five years and revised should circumstances change.

SM1.3 Personnel Policies

Objective

Personnel policies are consistent with, and support, the GNWT information security policy.

Standard of Best Practice

Personnel policies should require:

- terms and conditions of employment, including the Code of Conduct, specify security responsibilities
- contracts of employment include signing "Use of Electronic Mail", "Internet Guidelines" and Oath of Office
- external personnel with authorized access to the organization's information or systems to sign non-disclosure/confidentiality agreements
- revocation of access privileges when authorized users change jobs or leave the Government
- screening of applicants for specific groups of jobs for employment

Personnel policies related to information security are available to all individuals either through the GNWT's website or from Departmental Human Resource staff.

SM 2.0 Security Organization

Safeguarding information and systems requires information security activities be organized efficiently across the GNWT. This section covers organizational arrangements for managing information security across Government.

SM2.1 High-level Control

Objective

To provide a management structure and a practical mechanism for coordinating information security activity across the GNWT.

Standard of Best Practice

The Electronic Information Security Committee should exercise high-level control.

Membership of the group should include:

- two (2) representatives from the Recorded Information Management Committee
- two (2) representatives from Information Technology Advisory Committee
- two (2) representatives of Access & Privacy Coordinator group
- a representative from the Northwest Territories Archives
- a representative from the Office of the Chief Information Officer
- a representative from the Technology Service Centre
- a representative from Systems & Communications
- others as designated by IPC

The group should meet regularly to review the security condition of the Government, provide direction (by approving information security standards and procedures) and co-ordinate information security activity.

SM2.2 Driving Force

Objective

Actively promote best practices in information security and ensure they are applied effectively throughout the GNWT.

Standard of Best Practice

A Chief Security Officer specializing in information security should be established in the Office of the Chief Information Officer.

The Chief Security Officer should:

- define security mechanisms and supporting standards
- provide support and expertise to business managers, users, IT staff, and others to fulfill their information security responsibilities
- measure the effectiveness of Government-wide information security
- provide support for data classifications, threat and risk assessment, audits, third party agreements, and business continuity plans
- monitor general business trends, technological developments, new threats/vulnerabilities and new solutions
- have the knowledge, skills, resources and management support needed to fulfill their role

The Chief Security Officer should have direct access to management throughout the GNWT and maintain contact with counterparts in business, other governments, law enforcement agencies, and external security experts.

SM2.3 Local Co-ordination

Objective

Promote information security best practices within departments, and ensure they are applied effectively.

Standard of Best Practice

Deputy Ministers are responsible for information security within their departments.

A Departmental Security Officer (DSO) should be appointed to coordinate information security activity within each department. They should have the knowledge, skills, time, tools, contacts and authority needed to fulfill their role. Departmental security officers should have access to the GNWT's Chief Security Officer and be supported by standards/procedures for day-to-day security activities.

The condition of information security in all parts of the GNWT should be reported to the Chief Security Officer, or other Government Officials, in a consistent and regular manner.

SM2.4 Security Awareness

Objective

Ensure business owners, IT Staff, users and others with access to information and systems of the GNWT understand information security, why it is needed, and their personal responsibilities.

Standard of Best Practice

Awareness programs should be directed at all individuals with access to information or systems within the GNWT.

Employees (including contractors) should receive guidance to help them understand information security, the importance of complying with policies/standards and to be aware of their own personal responsibilities.

Formal awareness programs should be:

- coordinated by the Chief Security Officer
- use structured training programs and specialized awareness material focusing on general security and policy specific security information
- supported by departmental senior management
- kept current with best practices, standards, and guidelines
- provided to all individuals with access to information or systems

The level of awareness within the government should be measured and reviewed periodically to assess the effectiveness of the security awareness program.

SM2.5 Security Education

Objective

Ensure personnel controlling, using, running, developing and securing GNWT information and systems have the knowledge and skills required to fulfill their responsibilities.

Standard of Best Practice

Education/training should be provided to all personnel with control over GNWT information and systems. The training should provide the knowledge required to assess security requirements, propose security controls and ensure controls function effectively.

Education/training should ensure that:

- business users use systems correctly and apply security controls
- IT staff develop systems following the GNWT System Development Life Cycle (SDLC)
- IT staff understand the Government's business, and can communicate effectively with all levels of Government

SM3.0 Risk Assessment

Ensuring safeguards applied to information and systems are proportionate to their importance to the GNWT is a critical part of sound security practices. This sections covers identifying risk and control requirements.

SM3.1 Data Classification

Objective

To determine the criticality of information and systems within the GNWT in order to communicate how they should be treated and to enable attention to be focused on those that are most critical.

Standard of Best Practice

A data classification system that applies across the GNWT should be used to classify information and systems.

The information security classification scheme should:

- specify that information and systems should be classified according to their criticality, sensitivity, and vulnerability to particular threats
- take into account the business impact of a loss of confidentiality, integrity and availability
- apply to all information in electronic and paper form, all software and hardware, and to services provided by external parties
- be applied to new systems at their development stage, as well as to established systems
- provide guidance on how to resolve conflicting classifications

Critical information and systems should be:

- distinguished from other information and systems
- recorded in an inventory at the departmental level
- signed-off by the business 'owner'
- protected in line with their classification

For more information on classifying data assets, refer to the Government's guideline on "Threat and Risk Assessment (TRA) of Information Technology Assets".

SM3.2 Ownership

Objective

Achieve individual accountability for all information and systems within the GNWT

Standard of Best Practice

'Ownership' of all information, software and associated computer and network facilities within government should be assigned to the person(s) in charge of the business processes or organizational units most dependent on them. An 'owner' could be an individual or a collective within a business unit.

Owners' responsibilities should be clearly defined, documented and accepted.

Responsibilities should include:

- determining business requirements (including information security requirements)
- classifying information and systems by their criticality, sensitivity and vulnerability
- defining access and disclosure policies
- establishing and maintaining service agreements
- participating in information security reviews
- protecting information and systems in line with business risk

Owners should reassign 'ownership' to fulfill these responsibilities when they are unavailable.

SM3.3 Risk Analysis

Objective

Enable individuals responsible for information and systems to identify key risks and determine the controls required to keep those risks within acceptable limits.

Standard of Best Practice

Threat and Risk Assessment is required for information or systems which are important or critical to the GNWT, including those under development. Deputy Ministers, and individuals in charge of business applications, information processing environments, communications networks and systems under development should understand the need to perform risk analyses.

Business risks associated with GNWT information and systems will use formal risk analysis methods. They should be consistent across Government to allow comparison of the risk results. Risk analysis methods should be documented, flexible, understandable, approved by senior management and reviewed regularly to ensure they meet business needs.

Risk analysis methods should:

- require involvement from representatives such as business 'owners', key user representatives, IT professionals and, for critical business applications, a Risk Management specialist
- take into account the criticality of the application, the business impact of a loss of confidentiality, integrity or availability, key threats and vulnerabilities
- take into account all controls needed to keep risks within acceptable limits including their costs

The results of risk analysis should include a clear indication of risks, an assessment of potential business impacts and recommendations to reduce risk to an acceptable level.

SM 4.0 Secure Environment

A consistent standard of best practice in information security across the GNWT can be achieved by introducing a common framework at the government level.

This section explains the arrangements required for consistency across the GNWT.

SM4.1 Standards/procedures

Objective

Provide a consistent framework of information security disciplines across the GNWT.

Standard of Best Practice

The GNWT should develop and apply comprehensive and formal standards/procedures for information security.

Formal standards/procedures should be based on business requirements, practical experience and focused on issues that cause the most harm.

Formal standards/procedures should address:

- security management including organization, security awareness and education, security audit/review, data classification, risk analysis, building security into systems during system development, security monitoring and business continuity
- government-wide initiatives including electronic commerce, electronic mail, data privacy, security architecture and the use of cryptography
- general information security activity including system administration, change management, incident management, back-up, physical security, and protection against malicious code
- control of access to information and systems including Internet usage, remote access and external access by third parties
- processes for dealing with evidence required for investigations

Formal standards/procedures should be documented, kept up-to-date, supported by more detailed guidelines and standards for technical or special topics and approved by the Electronic Information Security Committee.

Relevant standards/procedures should be made available to all individuals with authorized access to the information and systems of the GNWT.

There should be lists of approved hardware and software products applicable to all Government departments.

SM4.2 Security Architecture

Objective

Facilitate the secure development and use of systems by implementing consistent, simple-to-use security functionality across multiple computer systems within the GNWT.

Standard of Best Practice

The GNWT should establish and apply Information Security Architecture.

Government-wide arrangements should be made to:

- encourage the use of consistent hardware and software
- integrate security controls at application, computer and network levels while eliminating redundancy
- implement common naming conventions for information and systems, including an integrated directory name service
- employ consistent security functionality including access controls, cryptographic techniques and 'role-based' access privileges
- support a consistent way of validating and authenticating users

Arrangements should be formalized into documented information security architecture.

The architecture should:

- define a set of security mechanisms and supporting standards that provide a complete range of security capabilities to users and system developers
- be applied when developing major new applications and to existing systems
- be approved by business and IT security

SM4.3 Data Privacy

Objective

Ensure compliance with legal and regulatory requirements for data privacy that includes, but is not limited to, the GNWT Access to Information and Protection of Privacy Act (ATIPP).

Standard of Best Practice

Departments should develop standards/procedures for dealing with data privacy issues. A Privacy Impact Assessment (PIA) checklist is available for all public bodies from the Office of the Chief Information Office. The PIA checklist should be utilized when considering new data collection systems or for reviewing existing or modified system. Additionally, an Access and Privacy Coordinator (or contact) should be designated within departments to ensure compliance with territorial legislation, national and international law and regulatory requirements.

Personal data should be:

- adequate, relevant and not excessive for the purposes for which it was collected
- accurate (i.e. recorded correctly and kept up-to-date) and held in a format that permits identification of data subjects for no longer than is necessary
- processed fairly and legally, kept confidential, and used only for specified, explicit and legitimate purposes

Individuals must be informed and consulted regarding their personal information before their personal data is stored, processed or disclosed to a third party. The ATIPP Act requires individuals to be informed of how personal data will be collected, used, and disclosed. Additionally the data systems should allow for the correction or removal of the personal data.

SM4.4 Physical Protection

Objective

Ensure that only authorized individuals have physical access to GNWT critical information and IT facilities.

Standard of Best Practice

All buildings housing critical GNWT IT facilities (including data centers and communications facilities) should be protected by a range of physical controls.

Physical controls should protect:

- buildings housing critical IT facilities against unauthorized access, by using locks, card access systems, employing security guards and/or providing video surveillance in areas requiring higher levels of security
- important papers and removable storage media such as CDs, diskettes, and tapes against theft or copying, providing password protected screensavers on unattended workstations and restricting physical access to important fax points
- easily portable computers and components against theft, by using physical locks and indelibly marking vulnerable equipment

SM4.5 Business Continuity

Objective

Equip the GNWT to withstand a prolonged unavailability of critical information and systems, for example due to a major disaster such as flood or fire, and continue to deliver services to its citizens.

Standard of Best Practice

A formal process for developing and maintaining effective business continuity plans and arrangements across the government should be established.

Standards/procedures for developing business continuity plans should specify that such plans are:

- documented for all critical parts of government
- based on the results of risk analyses
- developed in conjunction with user representatives
- distributed to all individuals who would require them in case of an emergency
- kept current, backed-up by a copy held off-site, and subject to formal change management

Business continuity plans should include a schedule of key tasks to be carried out, responsibilities for each task and a list of services to be recovered, in priority order.

Business continuity arrangements should:

- be based on a thorough analysis of risk and approved by the business 'owner'
- cover the prolonged unavailability of critical computer facilities or equipment, communications services, personnel, buildings or access to buildings
- be tested periodically, using realistic simulations, to demonstrate whether services can be resumed within critical timelines
- be the responsibility of a particular individual or working group
- be documented in a formal plan and updated following any significant changes

Checks should be performed to ensure that individuals responsible for critical environments have developed business continuity plans, provided contingency arrangements and tested them periodically.

SM5.0 Special Topics

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns that should be dealt with consistently across government. This section covers special security controls that apply to electronic commerce, electronic mail, remote working, use of cryptography and the provision of third party access. It also covers arrangements required to protect against malicious mobile code.

SM5.1 Protection from Malicious Code

Objective

Protect the GNWT against disruption caused by the introduction of malicious code, such as viruses or harmful mobile code downloaded from the web.

Standard of Best Practice

The GNWT should develop and distribute standards/procedures that specify methods of protecting against malicious code such as viruses or harmful mobile code (downloaded from the web).

The risk of virus infection should be reduced by specifying:

- minimum requirements for anti-virus software, such as scanning computer memory, files and storage media
- that anti-virus software should be run at all times computers are in use
- the use of automatic update mechanisms for anti-virus software
- a formal process to help users deal with virus attacks, warning them to stop processing, note symptoms, identify the source and inform a single point of contact for support
- that staff should disconnect suspected computers from the network before powering them up and transfer media or files to a dedicated quarantine computer

Strict disciplines should be imposed over the downloading of mobile code from the web, and should include:

- restricting the use of mobile code from undesirable sources
- preventing downloading of specific types of mobile code with known vulnerabilities
- screening mobile code in quarantine areas

SM5.2 Use of Cryptography

Objective

Provide a high level of assurance that cryptographic solutions are applied and managed in an effective and disciplined manner throughout the GNWT.

Standard of Best Practice

The GNWT should develop standards/procedures to govern the use of cryptography. Cryptography should be managed in an effective and disciplined manner in accordance with formal standards/procedures.

These standards/procedures should:

- define the circumstances when cryptography should be used
- specify the suitability of cryptographic solutions to be employed (including algorithms and key lengths)
- define methods for secure distribution, storage, and periodic updating of cryptographic keys
- define the process for revocation of cryptographic keys
- define a recovery process of cryptographic keys that are lost or corrupted
- define the management of keys that have been compromised
- address the selection of cryptographic algorithms, and the management of cryptographic keys including the changing of cryptographic keys and the retention of keys for data recovery purposes

An up-to-date inventory of cryptographic solutions applied in government should be maintained. Responsibilities for cryptographic key management and dealing with licensing issues should be clearly defined.

Business managers should have access to:

- Technical and legal advice on the use of cryptography
- a list of approved cryptographic solutions

Where a Public Key Infrastructure (PKI) is in use, standards/procedures should be established, which define the:

- purpose of the PKI
- Controls required to manage digital certificates/cryptographic keys within the PKI
- methods required to operate the PKI
- actions to be taken in the event of a compromise or suspected compromise of the PKI

Steps should be taken to provide very high levels of protection over the Certification Authority (CA) used by the GNWT, including:

- severely restricting access to the CA(s)
- removing all known vulnerabilities on the operating system(s) that supports the CA(s)
- Employing other general controls

Contingency plans for the application(s) supported by the PKI should include methods of recovering the PKI in the event of a disaster.

SM5.3 Electronic Mail

Objective

Ensure that electronic mail services are available when required, the risk of misuse is minimized and that the confidentiality and integrity of messages is protected in transit.

Standard of Best Practice

Mail servers should be configured to protect the availability of electronic mail (e-mail) systems, by limiting the size of messages, user mailboxes, restricting the use of large distribution lists and preventing e-mail 'loops'.

E-mail messages should be scanned for:

- known malicious code, including attachments where code could be hidden
- key phrases, such as those commonly used in hoax viruses or chain letters

E-mail systems should be protected by:

- blocking messages that originate from undesirable web sites or e-mail list servers to help prevent 'spamming'

Confidential Internet e-mail should be protected by:

- hashing messages to help maintain integrity and encrypting confidential messages
- ensuring non-repudiation of messages by using mechanisms such as digital signatures
- encrypting sensitive messages and/or documents

Users of GNWT e-mail systems should be warned that contents of e-mail messages may be legally binding, messages sent or received may be monitored and misuse of e-mail facilities can result in disciplinary action as outlined in the GNWT Guidelines to the Use of Electronic Mail and the Internet.

SM5.4 Remote Access

Objective

Ensure that computers used by GNWT staff working in remote locations operate as intended, remain available and do not compromise the security of facilities to which they can be connected.

Standard of Best Practice

Computers to be used by GNWT staff working in remote locations (typically desktop or laptop PCs) must have purchases authorized by the Technology Service Centre (TSC), tested prior to use, supported by effective maintenance arrangements, and protected by physical controls.

Computers used in remote locations should be:

- equipped with standard configurations of system and application software
- protected by a comprehensive set of system management tools, access control mechanisms and up-to-date virus protection software
- automatically logged-off after a set period of inactivity

Staff working in remote locations, including public areas, such as trains, airports or from home, should be:

- authorized to work in specified locations
- have the skills to perform required security tasks
- made aware of the additional risks associated with remote working, including the increased likelihood of theft of equipment or disclosure of confidential information
- made aware of approved GNWT enhanced security options
- provided with technical support
- be in compliance with legal and regulatory requirements

SM5.5 Third Party Access

Objective

Ensure that access to GNWT information and systems by third parties (i.e. external organizations, such as business partners, contractors and members of the public) is only provided following rigorous review and formal approval.

Standard of Best Practice

Third parties (i.e. external organizations, such as business partners, contractors and members of the public) should only receive access to government information or systems following rigorous review.

Before Third Party access is allowed to information systems containing personal information, a Privacy Impact Assessment should be considered. Privacy Impact Assessments, allow for an objective evaluation of the impact that a new program is likely to have on the privacy of individuals. The PIA process is designed to ensure that project managers evaluate their new programs to ensure compliance with the ***Access to Information and Protection of Privacy Act.***

Once a data connection from a third party is approved, all data connections should be uniquely identified, documented by business owners, have formal approval obtained from Public Works and Services, The Technology Service Centre and be agreed to by both parties in a formal data agreement contract. A risk assessment should be carried out, agreed controls implemented, and rigorous testing performed.

Standards/procedures for third party access should specify methods of:

- ensuring controls over third parties are commensurate with business risks
- making third parties accountable for their actions
- limiting liabilities and protecting ownership rights
- complying with legal or regulatory obligations such as the Access to Information and Protection of Privacy Act

Standards/procedures for third party access should address arrangements for:

- achieving technical compatibility, logging activity and providing a single point of contact for dealing with problems
- restricting methods of connection and the type of access granted
- subjecting third party users to strong authentication and monitoring
- terminating connections no longer required

Individuals responsible for managing third party connections should be aware of the risks associated with third party access, guidelines on how to secure connections, supporting tools such as checklists and sources of expertise for technical/specialist advice.

SM5.6 Electronic Commerce

Objective

Keep risks associated with the development and deployment of electronic commerce within the GNWT to acceptable limits.

Standard of Best Practice

A high-level committee should coordinate all GNWT electronic commerce (e-commerce) initiatives. A top-level government business manager should chair the committee. It should include representatives from a wide range of disciplines including business units, finance, audit, legal, security, and Risk Management.

Risk assessments should be performed early in the development of e-commerce initiatives, using a specialized risk analysis method specially designed to evaluate e-commerce, and focused on key risks such as overload or divulgence of sensitive citizen data.

Standards/procedures should require that:

- security practices are not sacrificed in the interests of speed
- initiatives are driven by business requirements (i.e. they are not technology-led)
- dependence on immature technology is minimized
- security implications of implementing vendor solutions are assessed

A process should be established to ensure that key decision-makers:

- understand security requirements of business owners
- are aware of the risks associated with e-commerce and have not overlooked the main threats
- formally sign-off residual risks
- have acquired staff with the security skills required to support e-commerce initiatives

Prior to going live, e-commerce initiatives should be formally approved by senior management, tested rigorously using very large numbers of users, and undergone a vulnerability assessment by the Office of the Chief Information Officer or their designate.

SM5.7 Electronic Commerce Applications

Objective

Ensure risks associated with applications supporting electronic commerce are minimized.

Standard of Best Practice

Web servers that support applications should be prevented from running with high level privileges on a day-to-day basis, initiating network connections to the Internet, or uploading unknown files.

Interfaces between web servers and back end systems (i.e. database systems) should be restricted to those services required by the application, channeled through documented application programming interfaces (APIs) and supported by mutual authentication.

Key system configuration information, that could be useful to hackers (i.e. prompts that identify operating system versions), should not be inadvertently made available to third parties over the Internet.

Web content should be reviewed to ensure that:

- vulnerabilities are not introduced by scripts or 'hidden' form fields
- it is accurate and up-to-date
- hyperlinks are valid and functional

SM6.0 Management Review

The GNWT must have an accurate understanding of its security posture (including the level of dependence on information and systems, its security status, incidents statistics, likely threats and improvement activity) to manage information security effectively.

Accordingly, this section covers the arrangements needed to provide decision makers with sound information on the security posture of GNWT information and systems.

SM6.1 Security Assessment/Review

Objective

Provide Deputy Ministers and other senior management, with an independent assessment of their department's IT environment security posture.

Standard of Best Practice

The information security status of IT environments should be subject to thorough, independent and regular security assessments/review by the Office of the Chief Information Officer or their designate.

Security assessments/reviews should consider business risks associated with the environment under review and should be performed for business applications, information processing environments, communications networks and system development activities.

Security assessments/reviews should be:

- agreed upon by the individual responsible for the environment
- performed by qualified individuals with sufficient technical skills and knowledge of information security
- conducted in a way to provide assurance that security controls function as required
- complimented by reviews conducted by or in consultation with the Internal Audit Bureau

Recommendations for improvement should be agreed upon with the individuals responsible for the environment under review, implemented and reported to senior management.

SM6.2 Security Monitoring

Objective

Provide senior management with an accurate, comprehensive, and coherent assessment of the security posture of the GNWT.

Standard of Best Practice

The GNWT should monitor its information security posture.

Information regarding the security posture of the GNWT's networks should be provided to senior management and individuals in charge of critical business applications, information security management and the Internal Audit Bureau.

Information about the security posture of the GNWT should:

- provide decision makers with an informed view of the adequacy of information security arrangements
- reveal areas where improvement is most needed
- identify information and systems subject to unacceptable risks
- highlight actions required to minimize risks
- set quantitative targets for improvement

COMMUNICATIONS NETWORKS

Communication networks convey information and provide access to information systems. By their nature, communication networks are vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well defined network services, and sound procedures for running the network and managing security. These factors apply equally to local and wide area networks.

CN1.0 Communications Management

The GNWT's computer networks are complex. They link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the technical and organizational issues involved requires sound management.

This section covers: the standards/procedures and organizational arrangements applied to the network, its design, configuration, documentation and the management of relationships with service providers and outsource contractors. These processes are designed for communications environments that are in-sourced, out-sourced, and combinations of both. The processes apply to vendors and/or GNWT staff who manage GNWT's communication networks.

CN1.1 Organization

Objective

Provide a sound management structure for personnel running the GNWT network.

Standard of Best Practice

Overall responsibility for activity on the GNWT network should be clearly assigned to a specific work group. Individuals within this work group should be equipped with the knowledge, skills and time to fulfill their roles.

Responsibility should be clearly assigned for:

- controlling the technical aspects of the network such as network design, configuration management, traffic management and network monitoring
- the general management of the network environment, such as day-to-day operations, incident management and change management
- establishing service agreements
- methods of coordinating information security activity

The risk of staff disrupting the running of the network either in error or by malicious intent should be reduced by:

- segregating the duties of staff running the network from those developing/designing the network
- reducing dependence on key individuals by automating key tasks, ensuring complete and accurate documentation and arranging alternative cover for key positions
- closely controlling activities of network staff, by supervision and recording of activity
- screening applicants for positions that involve running the network, by taking up references, checking career history/qualifications and performing background checks

CN1.2 Standards/procedures

Objective

Provide personnel running the communications network with a clear statement of the procedures they must follow.

Standard of Best Practice

Network staff should be provided with formal standards/procedures to follow..

Standards/procedures should specify:

- ways of controlling the technical aspects of the network including network design, resilience, configuration management, traffic management and network monitoring
- general management of the network environment, including day-to-day operations, incident management and change management
- the establishment of service level agreements, such as those with specific government program areas or external service providers/contractors
- information security responsibilities

Network standards/procedures should be documented, kept current, communicated to all network staff and reviewed regularly.

CN1.3 Network Design

Objective

Produce an operational communications network based on sound design principles that has security functionality built-in and enables additional controls to be incorporated easily.

Standard of Best Practice

The GNWT's communication networks should be designed in conformance with sound disciplines.

The communications network should be designed to:

- be compatible with other networks used throughout the GNWT
- cope with foreseeable developments in the government's use of IT (such as by performing growth projections and adopting open/non proprietary standards)

The design of the network should:

- incorporate clear technical standards, support consistent naming conventions and comply with statutory and industry regulations
- incorporate distinct sub-networks, protected by rule-based traffic filtering or firewalls
- minimize single points of failure and the number of entry points into the network
- allow the network to be centrally managed
- enable network management reports and audit trails to be maintained

Network design should be supported by formal documentation of service requirements.

CN1.4 Network Resilience

Objective

Ensure the communications network is supported by robust and reliable hardware and software.

Standard of Best Practice

Communications facilities that are critical to the continuity of network services should be identified. Single points of failure should be minimized by:

- automatic re-routing of communications should critical nodes or links fail
- routing critical links to more than one external exchange or switching centre
- the provision of duplicate or alternate secure gateways, such as firewalls, main switching nodes and critical power supplies in areas of high criticality

The risk of malfunction of critical communications equipment, software, links and services should be reduced by:

- giving high priority to reliability, compatibility and capacity in the acquisition process
- using only proven products, keeping them up-to-date and in good running order
- ensuring that key network components can be replaced quickly
- using modern protocols that can be updated quickly and withstand high capacity

CN1.5 Network Documentation

Objective

Ensure the network is supported by accurate, up-to-date, documentation.

Standard of Best Practice

Standards/procedures should be established, applying to network documentation.

Accurate documentation (in paper or electronic form) should be maintained for:

- the network configuration , including all nodes and connections
- communications equipment, software, links and services, including up-to-date inventories and labeling of equipment
- in-house cabling including identification of cable runs and labeling of cables

Network documentation (i.e. diagrams, inventories and schedules) should be:

- generated automatically, using software tools, and kept-up-to-date
- include, for historical purposes, archive copies of legacy diagrams and configurations
- readily accessible to authorized personnel, and subject to supervisory review
- checked periodically to ensure that no unauthorized changes have been made

CN1.6 Service Providers

Objective

Define the business requirements, including those for security, to be met by service providers who provide network communication services to the GNWT.

Standard of Best Practice

Network communication services obtained from reputable service providers should be defined in formal agreements, such as service level agreements or contracts.

Formal agreements with service providers should specify:

- responsibilities, capacity requirements, dates/times when network services are required and critical timescales of the network
- service windows for scheduled upgrades, repairs and outages
- points to be connected and methods of connection including types of network services or protocols
- restrictions on methods of connection and access to particular services

Formal agreements should specify requirements for security controls, including:

- arrangements for ensuring continuity of service and segregation of network components
- change management processes
- arrangements for incident management
- methods of detecting/recovering from service interruptions
- protecting confidential data in transit, for example using encryption

The terms of formal agreements should be enforced and reviewed periodically.

Arrangements should be made to:

- deal with service providers via a single point of contact
- restrict the use of services to those provided by reputable parties
- ensure an acceptable level of security
- obtain independent confirmation of security controls applied by service providers
- ensure that the service provider(s) have qualified IT Security Specialists

CN1.7 Outsourcing

Objective

Ensure GNWT's security requirements are satisfied if an outsourced contractor runs the network.

Standard of Best Practice

Prior to outsourcing responsibility for all or part of a network, the GNWT should:

- subject the selection of outsource contractors and the transfer of responsibilities to a formal process
- identify risks and assess security practices employed by outsource contractors
- agree to security controls, and establish formal agreements

Formal agreements should oblige contractors to:

- comply with good business practice, including those outlined in CRTC regulations, report incidents and provide regular reports on network performance
- maintain the confidentiality/integrity of information gained in the course of work, limiting access to authorized users
- maintain continuity of services in the event of a disaster
- apply agreed information security controls, ensuring legal and regulatory requirements (including those for data privacy) are met
- permit their activities to be audited and to provide compensation if service targets are not met

Arrangements should be made to:

- deal with a single point of contact within the outsource contractor
- provide sufficient resources to manage the relationship with the outsource contractor on an informed basis
- cover the possibility of network services being interrupted for a prolonged period
- ensure that the service provider(s) have qualified IT Security Specialists

A designated division within the GNWT with sufficient technical skills and knowledge should be responsible for managing the relationship with the outsource contractor.

CN2.0 Traffic Management

Communications networks can handle many types of network traffic from a wide variety of sources. To manage network traffic effectively, network devices must be configured correctly and particular types of network traffic denied access. This section covers the procedures required to ensure undesirable network traffic or unauthorized external users are prevented from gaining access to specified parts of the GNWT communications network.

CN2.1 Configuring Network Devices

Objective

Ensure important network devices function as required and do not compromise network security.

Standard of Best Practice

Network devices (including routers, concentrators, switches or firewalls) should be configured to:

- highlight overload or exception conditions
- log events in a form suitable for review, and write them to a separate logging system
- copy control information (including logs and tables) to removable media and integrate with access control mechanisms and security systems
- restrict use to authorized personnel, for example using access control software that supports individual accountability
- disallow inessential services not required for the standard operation of the network
- support encrypted communications for management functions
- approved standards through the use of master security templates or configurations

Network devices that route traffic should be configured to prevent unauthorized or incorrect updates by configuring them to:

- verify the source and destination of routing updates
- protect the exchange of routing information

Network devices should be reviewed regularly to verify configuration, by checking parameters and scrutinizing activity logs. All changes to network devices must follow approved change management processes.

CN2.2 Traffic Filtering

Objective

Ensure unauthorized or undesirable network traffic is not allowed access to specified parts of the GNWT network.

Standard of Best Practice

Network traffic should be routed through an effective filtering device, such as a firewall, before being allowed access to the network.

Network filtering devices should be configured to:

- filter specified types of traffic including IP addresses, TCP ports or information about the state of communications and users
- block or otherwise restrict particular types or sources of traffic
- limit the use of communications prone to abuse
- use authentication servers for management purposes (i.e. TACACS + or Radius)

Filtering of traffic should be based on pre-defined rules or tables that:

- consider a high-level security policy, and business requirements
- are developed by trusted personnel, and subjected to supervisory review
- are based on the principle of 'least access'
- are documented and kept up-to-date
- are verified to confirm strength and correctness and subject to strict change management disciplines prior to any changes being applied
- subject to security assessments by a designated centre

Steps should be taken to ensure that network filtering devices:

- cannot be bypassed
- can only be accessed from designated workstations or specified IP addresses
- are supported by a process for dealing with suspected vulnerabilities and failure

Divulgence of information about the network should be limited, for example by using network address translation and proxy servers.

CN2.3 External Access

Objective

Ensure only authorized and authenticated users are granted external access to the network.

Standard of Best Practice

All external access to the GNWT network should be individually identified, approved by a designated authority, recorded and assigned an owner.

The network should be configured to:

- verify the source of external connections
- restrict connections to defined entry points, such as via specific gateways
- route access through a network filtering device, such as a firewall, or VPN
- restrict access to only specified parts of the network
- restrict access to only specified service ports on the network, such as HTTP

Unauthorized access points should be identified by:

- performing manual audits of network equipment and documentation to identify discrepancies with records of known external connections
- employing network management and diagnostic tools, such as port probes and network 'discovery' tools

External access should be provided using a dedicated remote access server, running an authentication system such as Radius or TACACS+. The dedicated remote access server should log all connections, connection times, and sessions and help identify possible security breaches, for example by logging all events in a database and collating them centrally.

External access no longer required should be removed promptly and any dedicated components disabled or removed.

CN2.4 External Connections

Objective

Ensure only authorized individuals or organizations gain access to applications on the GNWT network via external network connections (i.e. Extranets).

Standard of Best Practice

External connections to GNWT applications, (including those used by staff working in remote locations or by authorized third parties) should be individually identified, formally approved and recorded.

Prior to granting external access to the GNWT network, steps should be taken to ensure that:

- the business owner has provided a business case outlining the requirements for the connection
- risks have been assessed
- agreed security controls have been implemented
- rigorous testing has been performed
- formal agreements are in place between the GNWT and the third party connecting to the network

Once permission to connect has been granted, external access to the application should be restricted by:

- subjecting external users to strong authentication, such as challenge/response devices featuring one-time passwords, smartcards or other tokens
- routing traffic through secure gateways such as firewalls
- limiting methods of connection
- granting access only to specified parts of an application, network, or host

All external connections should be periodically reviewed to ensure that no additional risks have been introduced to the environment due to technological change. External connections no longer required should be removed promptly and key components disabled or removed.

Business owners should provide a business case to the network owner outlining the requirement for the external connection.

CN3.0 Network Operations

Maintaining the continuity of the GNWT's communications network requires the network be run in accordance with sound procedures. This section covers the arrangements made to run the network, monitor performance and to manage changes and incidents. This section also covers the arrangements required to provide physical security, tape back-ups and ensure service continuity.

CN3.1 Day-to-day Operations

Objective

Ensure communications network staff are equipped to run the network under all conditions.

Standard of Best Practice

Staff who operate the communications network should:

- be aware of the existence and importance of information security controls
- have the necessary knowledge, skills and time to run the network under normal and peak conditions
- be able to deal with error, exception and emergency conditions
- report faults and other disruptive events

Staff who run the network should be supported by comprehensive, documented procedures that:

- help them run the network, administer network addresses, back-up key files such as router settings and provide network diagrams
- are readily accessible and approved by the person in charge of the network
- are kept up-to-date and supported by copies stored off-site

CN3.2 Network Monitoring

Objective

Assess the GNWT network performance, reduce the likelihood of network overload and detect potential or actual malicious intrusions.

Standard of Best Practice

The network should be continuously monitored.

Monitoring activities should include:

- monitoring service level agreements
- reviewing service levels with user representatives and reporting them to the Technology Service Centre (TSC)
- formal investigation of current and projected volumes of network traffic, utilization of network facilities and any potential bottlenecks or overloads
- checking whether powerful utilities/commands have been disabled on attached communications equipment
- logging key network activities and reviewing them regularly, investigating any unusual entries

Intrusion detection mechanisms should be employed that include:

- detection of known attack characteristics
- a process for regular update to incorporate new or updated attack characteristics
- provision of alerts when suspicious activity is detected, and formal procedures for responding to suspected intrusions

The use of powerful analysis/monitoring tools, such as protocol analyzers should be restricted to authorized users. The Technology Service Centre (PWS) should approve the use of protocol analyzers on the GNWT communications network.

CN3.3 Incident Management

Objective

Identify and resolve incidents effectively, minimize their business impact and reduce the risk of similar incidents occurring.

Standard of Best Practice

All incidents on the GNWT communication network (including malfunctions, loss of power/communications services, overloads, mistakes by users or computer staff, access violations) should be dealt with through a formal process.

The incident management process should:

- ensure incidents are reported to a single point of contact
- specify requirements for recording incidents
- include categorizing incidents by type and prioritizing them according to their impact/urgency
- define procedures for dealing with incidents (including investigation, planning of remedial action, resolution, communication with users, supervising activity and documenting actions taken)
- be recorded and documented in a formal incident report

Incidents should be reported to the Office of the CIO or their designate, who should assess their business impact. Patterns of incidents (including number and frequency) should be reviewed to diagnose common problems and minimize their recurrence.

CN3.4 Change Management

Objective

Ensure changes to the GNWT communications network do not affect its availability or compromise the confidentiality/integrity of network traffic and target systems.

Standard of Best Practice

Changes affecting the network should be made through a formal process. The process should apply to all changes, such as:

- the roll-out of new services to users or the introduction of new services from service providers
- adding or deleting network nodes
- upgrades of communications equipment or software
- revisions to parameter settings in communications controllers
- temporary or emergency fixes to any part of the network

Changes should be rigorously tested and their impact assessed before being implemented. Network changes should be supervised, documented and formally accepted by management. Once made, changes should be reviewed to ensure that they have been made according to specification.

Versions of equipment, software, and firmware should be kept consistent across the network.

CN3.5 Physical Security

Objective

Ensure only authorized individuals have physical access to GNWT network facilities, and prevent services being disrupted by loss of or damage to communications equipment, power or facilities.

Standard of Best Practice

Physical access to communications equipment and facilities should be restricted to authorized personnel. Vendors or service engineers should be supervised when given access to communications equipment.

Critical areas, such as network operation centre or equipment rooms, including those at remote sites, should be protected from:

- natural hazards, such as fire and flood
- power failure, such as by the use of uninterruptible power supplies
- unauthorized access, such as by locks on doors and shutters on windows

Communications cables should be protected by concealed installation, armored conduit, locked inspection/termination points, alternative feeds or routing and avoidance of routes through public areas.

Fibre optic cables should be used to reduce the risk of data in transit being intercepted.

CN3.6 Back-up

Objective

Prevent the loss of essential network configurations, information and/or software.

Standard of Best Practice

Back-up versions of essential network information and software (including communications software and utilities, network configurations/settings, configuration diagrams and inventories) should be taken, according to a defined cycle.

Steps should be taken to verify back-up versions are readable and can be restored within the critical timescale of the network (i.e. the point beyond which unacceptable loss would be suffered).

Back-ups should be protected from loss, damage and unauthorized access. They should be stored in a fireproof safe on-site and copies kept off-site in a secure and controlled environment.

CN3.7 Service Continuity

Objective

Enable network services to continue in the event of a disaster.

Standard of Best Practice

Arrangements should be made to enable services to continue in the event of a disaster affecting the GNWT network.

The arrangements should:

- be the responsibility of a particular individual or working group
- be based on a thorough analysis of risk
- comply with government-wide standards/procedures set forth by Risk Management
- be reviewed by business owners and approved by the person in charge of the network and subject to a formal change management process
- cover prolonged unavailability of network operation centre, critical communications equipment, links, services, facilities, personnel, buildings or access to buildings
- be documented in a formal plan and updated following significant changes (such as to network services/facilities and legal, regulatory or contractual obligations)

To ensure that services can continue within the critical timescale of the network (i.e. the point beyond which unacceptable loss would be suffered) periodic tests or rehearsals should be carried out using realistic simulations, involving network personnel.

Key components of the network should be covered by insurance arrangements and/or liability clauses in outsource agreements. These arrangements should address key risks, such as loss of data, business interruption, or liabilities to third parties and provide adequate protection against likely threats, for example fire, theft, fraud or malicious damage.

CN3.8 Remote Maintenance

Objective

Prevent unauthorized access to the network through the misuse of remote maintenance facilities.

Standard of Best Practice

Remote maintenance facilities should be tightly managed by:

- defining and agreeing on the objectives of the planned remote maintenance
- restricting access rights and logging all activity
- revoking access rights and changing passwords regularly
- authorizing sessions individually and providing independent supervision of all activity
- providing access using a dedicated remote access server running an authentication system such as Radius or TACACS+

Diagnostic ports on network equipment should be protected by access controls, such as passwords and physical locks.

CN4.0 Local Security Management

The GNWT's communication networks play an essential role in many critical business applications. They convey information that needs to be protected, and are valuable assets in there own right. Both these roles need to be considered to achieve network security. Accordingly, this section covers the arrangements made to ensure that information security is managed and coordinated for the network as a whole.

CN4.1 Security Organization

Objective

Provide a management structure and a practical mechanism for coordinating the security arrangements of the GNWT communications network.

Standard of Best Practice

The person in charge of a network should be personally accountable for the information security of the network. Departmental Security Officers should be made responsible for coordinating departmental information security arrangements of the network, and acting as a single point of contact on information security issues within departments.

The Departmental Security Officer should:

- have a sound understanding of their information security roles
- have the knowledge, skills, time, tools, contacts and authority needed to carry out their assigned role
- be supported by procedures for day-to-day security administration and up-to-date information on issues related to information security
- have a communication channel with security officers in other departments and a reporting line to the Office of the CIO, or their designate
- coordinate business partner (i.e. extranet) connections within their departments through Public Works & Services, Systems & Communications
- ensure that departmental network communication circuits are provisioned through Public Works & Services, Systems & Communications

The Departmental Security Officers should meet periodically with the person responsible for the network to review the status of communications security.

CN4.2 Security Awareness

Objective

Maintain awareness of information security among personnel who run the network.

Standard of Best Practice

GNWT network staff, and contractors, should be aware of the high-level information security policy that applies across the government, and comply with it.

Network staff should be made aware of:

- the meaning of information security and why it is needed
- the importance of complying with information security policies and applying associated standards/procedures
- their personal responsibilities for information security
- particular security threats to the network

Network staff should be made aware that they are prohibited from:

- using any part of the network without authorization or for purposes that are not acceptable under the GNWT Network Usage Policy
- installing network analyzers or other devices capable of capturing network traffic without prior approval from the person in charge of the communication network
- disclosing confidential information (such as network designs or IP addresses) or compromising passwords (such as writing them down or disclosing them to others)

CN4.3 Risk Analysis

Objective

Identify key risks associated with the GNWT network and determine the controls required to keep risks within acceptable limits.

Standard of Best Practice

A formal risk analysis should be carried out periodically for networks that support critical business applications and for all network connections established with business partners (extranets), contractors, or third parties.

The risk analysis technique used should:

- include identifying critical business applications supported by the network and a review of associated service level agreements
- involve representatives of key areas, such as business 'owners' of critical business applications, the person in charge of the network, associated IT staff, and representation from a specialist in Risk Management
- determine the risk to the GNWT (considering the criticality of the network, the business impact from a loss of confidentiality, integrity, availability, key threats and vulnerabilities)
- consider the full range of controls needed to keep risks within limits acceptable to the GNWT
- account for the security posture of business partners connecting to the GNWT network

The results of the risk analysis should include a clear indication of key risks, an assessment of the potential impact to the GNWT, and recommendations for the actions required to reduce risks to an acceptable level. The results (including any residual risk) should be reviewed and agreed to by the person in charge of the network, the Office of the CIO or their designate, and communicated to the 'owners' of critical business applications supported by the network. Agreed actions should be implemented and a process established to ensure that this is done effectively.

CN4.4 Security Assessment/Review

Objective

Provide senior management and the person in charge of the communications network with an independent assessment of the security of the communication network.

Standard of Best Practice

The information security status of the communication network should be subject to thorough, independent and regular security assessment/review. Security assessments/reviews should cover network management, traffic management, network operations and security management.

Security audits/reviews should assess the business risks associated with the network by:

- reviewing the information security requirements of the business applications supported by the network
- evaluating the network's vulnerability to key threats

Security audits/reviews of the network should be:

- conducted in consultation with the Internal Audit Bureau
- agreed with the person in charge of the network
- defined in scope and documented
- performed by qualified individuals and checked by competent personnel
- supported by the use of automated software tools

Agreed recommendations from Security assessments/reviews should be implemented, reported to senior management, and validated.

INFORMATION PROCESSING (IP)

The GNWT computer environment supports a number of critical business applications and safeguarding them is a high priority. Since the same information security principles apply to any information processing activity regardless of where, or what scale or type of computer it takes place on, a common standard of best practice for information security must be applied. All systems, regardless of the sensitivity of the data contained within, should have the standards of best practice applied to them before they are brought online for the first time and throughout the life cycle of the system.

IP1.0 Installation Management

Computers used for data processing need to be well managed. Accordingly, this section covers the organization of people involved in running computer environments within government, the procedures they are expected to follow, agreements made with business users, documentation and monitoring of systems.

IP1.1 Organization

Objective

Provide a sound management structure for personnel running IT environments within government.

Standard of Best Practice

Overall responsibility for information processing activity should be assigned to an individual within the department. Responsibilities for key tasks should be assigned to individuals with the knowledge, skills and time to fulfill their roles.

Responsibilities should be clearly assigned for:

- controlling the technical aspects of the environment, such as installation design, host or workstation configuration, access control, and virus protection
- general management of the environment, such as day-to-day operations, incident management, change management, system monitoring and service continuity
- establishing service agreements with business owners of applications supported by the organization
- coordinating information security activity within the department

The risk of staff disrupting the operations of the environment either in error or by malicious intent should be reduced by:

- segregating the duties of personnel running the production environment from those developing new systems
- reducing dependence on key individuals by automating tasks, ensuring complete and accurate documentation and arranging alternative cover of key positions
- closely controlling activities of IT staff, by supervision and recording of activity
- ensuring systems are not connected to the network until they have been adequately secured including the application of required security updates
- screening applicants for positions that involve running the environment, by taking up references, checking career history/qualifications

IP1. 2 Standards/procedures

Objective

Provide personnel running the environment with a clear statement of the procedures they are required to follow.

Standard of Best Practice

Government staff running computer environments should receive formal, comprehensive and up to date standards/procedures to comply with.

Standards/procedures should specify:

- methods of controlling the technical aspects of the environment, such as installation design, host or workstation configuration, access control and virus protection
- general management of the environment, such as day-to-day operations, incident management, change management, system monitoring and service continuity
- the service level agreements with the business owners of applications supported by the IT environment
- information security responsibilities including minimum baseline standards

Standards/procedures must be consistent with policies across the GNWT, for example the high-level information security policy. They should be documented, kept current, made available to all IT staff and reviewed periodically.

IP1.3 Service Agreements

Objective

Define the business requirements for services provided by IT resources.

Standard of Best Practice

Service requirements should be classified to identify their criticality to the business owner and documented in formal agreements, such as contracts, memorandum of understandings, or service level agreements. These agreements apply to in-sourced and out-sourced environments.

Service agreements should specify:

- who is in charge of the business application(s) supported within the environment, and who is responsible for delivering the required service
- capacity requirements, maximum processing response times, dates/times when services are required and critical timelines
- the level of criticality of the service

Formal agreements should specify requirements for security controls, including:

- segregation of operational duties
- authentication methods and access restrictions
- change and incident management procedures
- protection against malicious code, including viruses and malicious mobile code downloaded from the web
- back up, retention and archiving
- arrangements for ensuring continuity of service

Service agreements should be signed-off by all parties and their terms should be enforced and reviewed periodically.

IP1.4 System Documentation

Objective

Ensure GNWT computer environments are supported by accurate and current system documentation.

Standard of Best Practice

Standards/procedures should be established for system documentation. Accurate system documentation should be maintained within departments for:

- the design of the environment, including configuration of all hosts/servers and attached devices
- software employed
- parameter settings
- communications links/services

System documentation should include copies of formal agreements with business owners.

Details of environment components (including business information, software, computers and related documentation, equipment, facilities and services) should be recorded in inventories, or equivalent, and should contain the:

- identity of the component(s), such as a description or a unique identifier
- classification of the data contained within the application
- identity of the 'owner' (i.e. the individual responsible for specific components)
- location of the component(s)
- software and hardware version in use including applicable service updates
- license conditions, such as the number of permissible users, and the license expiration date(s)

Access to system documentation should be restricted to authorized personnel as it provides a significant amount of information on the configuration of the system and could be used by a malicious user to gain access to a system. Inventories of system documentation should be protected against unauthorized change, kept current, periodically checked against physical assets and independently reviewed.

IP1.5 System Monitoring

Objective

Assess the performance of the IT environment, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

Standard of Best Practice

Systems associated with the computer environment should be continuously monitored.

Monitoring activities should include:

- monitoring service levels against agreed targets
- reviewing service levels with user representatives and reporting them to the asset 'owner' and the 'owners' of business applications supported by the environment
- recording current and projected volumes of work, utilization of systems facilities and any potential bottlenecks or overloads
- checking whether powerful utilities, commands, and services have been disabled on attached hosts

System availability (i.e. response and up-time) should also be measured from the perspective of business owners.

IP1.6 Outsourcing

Objective

Ensure security requirements are satisfied when an outsource contractor is running a computer environment and or application environment.

Standard of Best Practice

Before outsourcing responsibility for the environment, IT resources within government should:

- subject the selection of the contractor and the transfer of responsibilities to a formal process
- identify risks and assess security practices employed by outsource contractors
- agree to security controls, approve transfer and establish formal agreements

Formal agreements should oblige contractors to:

- comply with good business practice, including the standards outlined in the GNWT Standard of Best Practice and other GNWT IT Policy and Standards
- report incidents and provide regular reports on system performance
- maintain the confidentiality/integrity of information gained in the course of work
- limit access to authorized users
- maintain continuity of services in the event of a disaster
- apply agreed information security controls, ensuring legal and regulatory requirements, including those for data privacy, are met (i.e. ATIPP)
- permit their activities to be assessed
- provide compensation if service targets are not met

Arrangements should be made to:

- deal with a single point of contact within the outsource contractor
- provide sufficient technical resources to manage the relationship with the outsourced contractor on an informed basis
- cover the possibility of services being interrupted for a prolonged period

Responsibility for managing the relationship with the outsource contractor should be assigned to a designated individual with sufficient technical skills and knowledge.

IP2.0 Production Environment

Service levels are more likely to be achieved if computer environments are well designed. This section covers the design of the environment and the configuration of any related hosts and/or workstations. It also covers the resilience of the environment and its protection from physical loss or damage.

IP2.1 Environment Design

Objective

Ensure the computer environment as a whole is designed using sound principles and processes.

Standard of Best Practice

The IT environment should be designed to be consistent with other environments within the department and/or government, and cope with current and future information processing requirements.

The environment should be designed to:

- support consistent naming conventions, such as computer addresses, device locations and user identifiers
- be managed from a central point
- enable users to be able to gain access to multiple systems within the environment via a single sign-on and be administered from central points.
- minimize the need for manual intervention
- isolate production environments from development and acceptance testing activity, by using different staff and systems

Key components of the environment should be protected by:

- segregating critical business applications from all other business applications, as agreed with their business ‘owners’
- storing source code in a secure location away from the production environment and restricting access to source code to authorized personnel
- segregating different types of software and data, for example by storing them in separate directories
- permitting only execute access to executable software
- keeping all systems clocks synchronized and accurate through the use of centralized network time source

IP2.2 Host Configuration

Objective

Ensure host systems within the GNWT operate as intended and do not compromise the security of the environment.

Standard of Best Practice

Hosts on the GNWT networks should be configured in accordance with formal standards/procedures.

Hosts should be configured to:

- disable or otherwise restrict particular functions or services, such as inessential or redundant services, communications that are inherently susceptible or prone to abuse, and powerful utilities or commands
- restrict access to powerful system utilities/host parameter settings to particular users or defined circumstances, logging their use

Hosts should be protected against unauthorized access by:

- changing default parameters set by suppliers prior to use
- disabling unnecessary or insecure user accounts, such as ‘guest’ for UNIX or Windows NT, and renaming the default Windows NT/2000/ Server administrator account
- consolidating all access and activity logs to enable focused review
- invoking time-out facilities that automatically log-out or invoke password protected screen savers on workstations and/or servers after a set period of inactivity, clear screens and require users to sign-on again before restoring screens

The Technology Service Centre has been established to help departments identify new technical vulnerabilities in operating systems and ensure proven countermeasures are implemented quickly. Software updates such as patches or security fixes must be applied in a timely manner and subjected to a change management process.

IP2.3 Workstation Configuration

Objective

Ensure workstations operate as intended and do not compromise the security of the systems to which they are connected.

Standard of Best Practice

Workstations connected to the environment should be purchased from approved suppliers as identified by the Technology Service Centre, tested prior to use, supported by effective maintenance arrangements and protected by physical controls.

Each workstation should be:

- equipped with standard configurations of system and application software
- protected by the use of a comprehensive set of system management tools, access control mechanisms and up-to-date virus protection software
- automatically logged-off or have a password protected screen saver invoked after a set period of inactivity

Additional controls should be implemented on workstations with the capability of connecting to the Internet, including:

- use of standard web browsers, with key software updates applied, and configured to prevent users from disabling security options
- warning users of the dangers of downloading files or programs from the Internet

IP2.4 Resilience

Objective

Ensure the GNWT computer environment is supported by a robust and reliable set of hardware and software.

Standard of Best Practice

The GNWT should identify components critical to the functioning of computer environments. Single points of failure should be minimized or reduced by considering:

- processors, for example using fault-tolerant systems including high availability servers
- on-line storage and file/database servers
- points from which the environment can be run
- processing locations
- the recovery of transactions following a system failure
- duplicating data storage, for example using disk mirroring or RAID
- protecting power supplies using redundant and uninterruptible power supplies (UPS)

The resilience of critical communications equipment, software, links and services should be improved by:

- giving high priority to reliability, compatibility and capacity in the acquisition process
- using only proven products, keeping them up-to-date and in good running order
- ensuring key equipment can be replaced quickly, and service agreements ensure timely repairs that meet business owners' requirements

IP2.5 Hazard Protection

Objective

Prevent services being disrupted by damage to computer equipment or facilities as a result of natural hazards.

Standard of Best Practice

Computer equipment and facilities should be protected against fire, flood, and environmental and natural hazards.

Computer equipment and facilities should be:

- situated in locations that have a low risk of fire, flood, explosion, civil unrest and damage from neighboring activities or natural disasters
- located in rooms that are free from intrinsic fire hazards (such as paper or chemicals), protected against the spread of fire and fitted with fire detection and suppression systems

The impact of hazards should be minimized by:

- training staff in the use of fire extinguishers (which should be located nearby) and other emergency/safety equipment
- establishing and testing emergency evacuation procedures

Fire alarms should be monitored, tested periodically and serviced in accordance with manufacturer specifications. The temperature/humidity of computer rooms should be monitored.

IP2.6 Power Supplies

Objective

Prevent services from being disrupted by loss of power.

Standard of Best Practice

Critical computer equipment and facilities should be protected against power outages.

Power cables within the computer environment should be protected by concealed installation, include locked inspection/termination points, and avoid routes through public areas.

Uninterruptible power supply (UPS) devices should protect critical computer equipment. Emergency equipment such as UPS equipment should be serviced in accordance with manufacturers' recommendations and tested periodically.

IP2.7 Physical Access

Objective

Ensure only authorized individuals have physical access to the environment and prevent services being disrupted by loss of or damage to equipment or facilities.

Standard of Best Practice

Physical access to the GNWT information processing environments should be restricted to authorized personnel by:

- fitting intruder alarms and locks activated by swipe cards, key pads, or manual locks
- requiring personnel to wear visible means of identification and encouraging them to challenge strangers
- recording the arrival/departure of visitors and supervising them at all times
- employing security guards and/or video surveillance in areas requiring high security
- issuing authorizations for physical access in accordance with formal standards/procedures, reviewing them periodically and revoking them when no longer needed, for example when staff leave the organization

Physical controls should be provided to protect:

- important papers and removable storage media (such as CDs and diskettes) by locking them away when not in use, for example in compliance with a ‘clear desk’ policy
- post/fax points and equipment used for sensitive printed material
- easily portable computers and components by using physical locks and indelibly marking vulnerable equipment

IP3.0 System Operation

Achieving service levels within the GNWT requires that IT organizations be run in accordance with sound procedures. This section covers day-to-day operations, basic procedures (i.e. handling computer media, back-up) and arrangements for identifying and resolving incidents (i.e. incident management, virus protection).

IP3.1 Day-to-day Operations

Objective

Ensure GNWT IT staff can run the computer environment under all conditions.

Standard of Best Practice

GNWT staff who operate computer systems or environments should be:

- equipped with the necessary knowledge, skills and time to run the network under normal and peak conditions
- competent to deal with error, exception and emergency conditions
- required to report faults and other disruptive events

Government staff who operate computer systems should be supported by operating procedures that cover:

- start-up/shut-down and restart/recovery processes
- scheduling routines and exception conditions
- handling of electronic business information and physical computer media
- restrictions on the use of system utilities
- back up, recovery and retention
- change management
- incident management
- management/safety of the environment

Operating procedures should be:

- comprehensive
- documented
- readily accessible to authorized staff
- approved by the person in charge of the environment
- reviewed periodically
- protected against unauthorized access
- kept current and backed-up by copies stored off-site

Activities of individuals running the environment should be logged in sufficient detail and reviewed to enable swift diagnosis and resolution of incidents.

IP3.2 Handling Computer Media

Objective

To protect computer media in line with its information data classification.

Standard of Best Practice

Computer media (including magnetic tapes, disks, CD, and printed results) should be handled in accordance with sound procedures.

The information held on data storage media should be protected by:

- keeping identifying labels free from descriptive information that might give unauthorized individuals information regarding their contents
- providing secure storage arrangements in compliance with manufacturers' storage recommendations including written authority for removal and recording of movements
- erasing the content of reusable storage media when no longer needed

Heightened protection should be provided for sensitive material by:

- labeling it with the correct data classification allowed under ATIPP
- minimizing distribution and confirming receipt of media
- utilizing bonded couriers that specialize in transporting computer media
- recording authorized recipients, marking media with the recipient's identity, and periodically reviewing records of authorized recipients
- ensuring all information is input/processed and that there is proper accounting for all computer media
- using fire-resistive safes for storage that have heat resistance ratings that meet or exceed the requirements of the media
- disposing of it securely by erasure, incineration or shredding and recording its disposal
- encrypting information while in transit

IP3.3 Back-up

Objective

Prevent the loss of essential GNWT information or software.

Standard of Best Practice

Back up versions of essential information including source code, data, and other software used by or within the computer operation should be taken, according to a defined cycle.

Back-up processes should be approved by business 'owners' and comply with:

- government wide policies and standards/procedures
- business continuity plans
- legal, regulatory and contractual obligations
- long-term archiving requirements as set forth by the Territorial Archivist
- manufacturers' recommendations for reliable storage, such as maximum 'shelf-life'

Back ups should be taken by government departments of master files/databases, transaction files, system programs/utilities, application software, parameter settings and system documentation. Backups should also include copies of system or application software updates required to return systems to normal operational state.

Back-ups should be:

- done in accordance with a defined back up/retention cycle that reflects data classifications, importance and time-criticality
- done so that individual files can be recovered
- time stamped, reconciled to live versions
- verified periodically to ensure recovery is possible
- clearly and accurately labeled, and protected from accidental overwriting
- stored in readily accessible locations on-site and supported by copies stored off-site
- protected in transit, for example by packing them in locked, robust containers and using only reputable bonded couriers
- signed for upon pickup and delivery

IP3.4 Incident Management

Objective

Identify and resolve incidents effectively and minimize the business impact and reduce the risk of similar incidents.

Standard of Best Practice

All types of incidents (including malfunctions, loss of power, overloads, mistakes by users or computer staff, access violations) on the GNWT network should be dealt with through a formal process.

The incident management process should:

- ensure incidents are reported to a single point of contact within the department
- ensure security incidents are reported to the Chief Security Officer within the Office of the CIO, by the Departmental Security Officer
- specify requirements for the recording of incidents
- include categorizing incidents by type and prioritizing them according to their impact/urgency
- define procedures for dealing with incidents (including investigation, planning of remedial action, resolution, and communication with users, supervising activity and documenting actions taken)

Significant incidents should be reported to the asset 'owner' who should assess their business impact. Patterns of incidents (including number and frequency) should be reviewed to diagnose common problems and to minimize their recurrence.

IP3.5 Virus Protection

Objective

Prevent disruption of the GNWT computer environment by computer viruses.

Standard of Best Practice

Software and procedures should be implemented to prevent virus infection for computer networks that contain systems susceptible to viruses.

Individuals running such systems should be made aware of the dangers posed by computer viruses, and the arrangements for dealing with suspected virus attacks.

The risk of virus infection on the government's data network should be reduced by:

- using standard anti-virus software, that runs at all times on computers in use, to scan computer memory, files and storage media
- applying automatic update mechanisms for anti-virus software, at least on a weekly basis
- a formal process to help users deal with virus attacks, warning them to stop processing, note symptoms, identify the source and inform a single point of contact for support
- issuing directives that investigators should disconnect suspected computers from the network before powering them up and transfer suspect media, such as diskettes, to a dedicated quarantine computer

IP4.0 Access Control

Maintaining sound procedures, enforced by effective access control mechanisms, can reduce the risk of unauthorized access to GNWT information and systems. This section covers the access control procedures applied to users and the steps taken to control access to GNWT information and systems.

IP4.1 Access Control Policies

Objective

Restrict access to GNWT information and systems in accordance with defined policies.

Standard of Best Practice

Access to the capabilities of an IT asset should be restricted according to formal, clearly defined access control policies.

Formal access control policies should consider:

- other policies that apply government-wide, for example a high-level information security policy
- the principle that access should be provided in line with business risk
- formal agreements with business 'owners' and requirements set by the asset 'owner'
- legal, regulatory and contractual obligations
- the need to achieve individual accountability, promote segregation of duties and apply additional controls over users with special access privileges

Access control policies should be:

- applied rigorously
- supported by formal standards/procedures and clearly-defined responsibilities for business 'owners', users and IT staff within the GNWT
- reviewed periodically and upgraded in response to new threats, capabilities, business requirements or access violations

IP4.2 Access Control Arrangements

Objective

Provide mechanisms to restrict access by users to specified components of the asset.

Standard of Best Practice

Arrangements should be made to control access to information and systems within the GNWT's computer network.

Access control arrangements should:

- cover access by business users, individuals running the system and IT staff, such as technical support staff
- cover information, application/system software, access control data, back-up files and system documentation
- restrict access in line with access control policies set by business 'owners' that reflect the business processes and policies of the business owner

Access control arrangements should provide technical mechanisms to:

- restrict the system capabilities that can be accessed, for example by providing restricted menus
- prevent users from gaining access to system prompts, for example by making systems menu-driven
- prevent misuse of passwords, for example by using encryption, avoiding the use of clear text passwords, one-time passwords or stronger authentication, such as token-based authentication on applications that require higher levels of security
- minimize the need for special access privileges

High-level administration activities should be limited to the system console only or through approved remote access mechanisms.

IP4.3 Third Party Access

Objective

Ensure access to applications owned by the GNWT is provided to third parties only when risk assessments have been performed and a formal agreement, such as a Memorandum of Understanding has been established.

Standard of Best Practice

Third parties (i.e. external organisations, such as governments, government agencies, crown corporations, contractors, and business partners) requiring access to applications are subject to additional controls. They will only receive access on completion of a satisfactory risk assessment and if supported by a formal data sharing agreement.

Risk assessments of third party access arrangements should consider the:

- criticality and sensitivity of information and systems to be accessed
- relationship with prospective third parties (including the strength of their security practices) and the nature of the associated business process
- technical aspects of connection (including the effectiveness of IT infrastructure, access control mechanisms, methods of connection and any vulnerability in third party networks)
- obligations implicit in any agreements such as providing a third party with a reliable service or timely and accurate information

Data sharing agreements should be documented formally and approved by the business 'owner'.

The contract should:

- require third parties to comply with good security practices and provide information about any security incidents
- clearly state the services to be provided such as the business practices to be adopted, timeframes for completion of transactions and an agreed process for resolving disputes
- specify agreed security arrangements, such as those for managing changes/incidents, restricting access and preserving the confidentiality of important business information
- include arrangements for ensuring that transactions cannot be repudiated
- protect intellectual property rights
- include the right to audit third party security arrangements

Third party access arrangements should be reviewed periodically to ensure risks remain within acceptable limits.

IP4.4 User Authorization

Objective

Ensure all users of GNWT computer assets are authorized through a sound process.

Standard of Best Practice

All users of GNWT IT assets should go through an authorization process before receiving access privileges.

The process for authorizing users on GNWT assets should:

- be formally defined, controlled by one or more designated individuals and applied to all users
- associate access privileges with defined users, for example with UserIDs rather than passwords
- issue default access privileges of 'none' (i.e. rather than 'read')
- ensure redundant UserIDs are not re-issued for use

A file or database containing details of all authorized users should be created and reviewed regularly.

Details of authorized users should be:

- maintained by designated 'owners' such as system administrators
- protected against unauthorized change or disclosure
- segregated from other information in the production environment
- held in a way that facilitates user identification and authentication
- recorded so specific information and systems to which users have access can be identified
- recorded so that users of specific information and systems can be identified
- reviewed to ensure access privileges are set at the right level and are still required

IP4.5 Access Privileges

Objective

Provide authorized GNWT users with access privileges sufficient to allow them to perform their duties but do not permit them to exceed their authority.

Standard of Best Practice

All users of GNWT IT assets should be assigned a set of access privileges that allow them to adequately perform their duties. Access privileges should be assigned by business 'owners' and specialized technical privileges assigned by the person in charge of the asset.

Before access privileges come into effect:

- authorizations should be checked to confirm access privileges are appropriate
- details of UserIDs should be recorded
- users should be advised of their access privileges and associated conditions and required to confirm their understanding of those conditions

Access privileges should not be assigned collectively (i.e. generic or shared UserIDs).

Additional controls should be applied to special access accounts, including high-level accounts (such as 'Root' in UNIX or 'Administrator' in Windows NT), powerful utilities and privileges that provide access to sensitive application capabilities.

These controls should include:

- specifying the purpose of special access privileges
- restricting the use of special access privileges to narrowly defined circumstances and requiring individual approval for their use
- requiring users with special access privileges to sign-on using identification codes or tokens different from those used in normal circumstances

A process for terminating access privileges of users should be established to ensure:

- authentication details and access privileges are revoked promptly on all systems to which the user had access
- access profiles/accounts are deleted
- components dedicated to providing access, such as tokens, modems, and remote access UserIDs, are disabled or removed

IP4.6 Sign-on Process

Objective

Ensure users of GNWT assets follow a rigorous sign-on process before gaining access to information or systems.

Standard of Best Practice

Rigorous sign-on processes should be established for all systems on the government's data network.

Sign-on mechanisms should be configured so they:

- display no identifying details until after sign-on is successfully completed
- warn only authorized users are permitted access and access is recorded and logged
- validate sign-on information only when it has all been entered
- limit the number of unsuccessful sign-on attempts (for example a re-try limit of three) and disconnect users after the limit is reached
- record all unsuccessful sign-on attempts
- record all successful system sign on attempts
- limit the duration of any one sign-on session and automatically re-invoke sign-on after an interruption of the process, for example when a connection is broken
- do not store authentication details in clear text, such as in scripts, macros or cache memory

The approval of the Office of the CIO or their designate must be obtained before any important features of the sign-on process are bypassed, disabled or changed.

IP4.7 User Authentication

Objective

Ensure all users are identified and authenticated before gaining access to any information or systems on the GNWT's data network.

Standard of Best Practice

All users should be authenticated, either by UserIDs and passwords or by stronger authentication such as 'smartcards', tokens, or biometric devices.

GNWT employees should be advised of best practice for selecting, using and protecting passwords. They should be warned to keep passwords confidential (i.e. avoid disclosing them to anyone or writing them down) and change passwords that may have been compromised.

User authentication should be enforced by automated means that:

- ensure UserIDs, passwords and their combinations are unique
- issue temporary passwords to users that must be changed on first use
- ensure users set their own passwords
- ensure passwords are a minimum number of characters in length, differ from their associated UserIDs, contain no more than two identical characters in a row and are not made up of all numeric or alpha characters and/or dictionary based words
- ensure passwords are changed frequently for users with special access privileges
- restrict the re-use of passwords within a set period or set number of changes

Processes for issuing new or changed passwords should ensure that:

- passwords are not sent in the form of clear text e-mail messages
- the person to whom the password uniquely applies is directly involved
- the identity of the target user is verified, such as via a special code or through independent confirmation

Strong authentication, such as token-based authentication, should be considered for users with access to critical business applications, sensitive information, special access privileges or users with remote access capabilities.

IP4.8 Access Logging

Objective

Ensure individual accountability and enable incidents, such as access violations, to be investigated and resolved.

Standard of Best Practice

Access to information on IT assets on the GNWT's data network should be logged. The person in charge of the asset and the asset owner should determine which access events are to be logged (including sign-on and files accessed) and the review process to be followed (including frequency and responsibility).

Access logs should be turned on at all times and protected from accidental or deliberate overwriting. Mechanisms should be established so systems are not halted when logs become full and logging continues with little or no disruption. Archive polices for access control logs must meet or exceed regulatory and legal requirements as identified by the business owner. Access logs should be archived in accordance with archiving policies defined by the Territorial Archivist. Access logs should be archived for security purposes for a minimum of two (2) years.

Logs should include details of access by all types of users, servicing activities, failed and successful sign-on attempts and error/exception conditions.

Sufficient information should be recorded to identify:

- individual UserIDs, particular capabilities accessed (such as software, commands or files) and the dates/times of access
- access paths (including computers/ports from which access was gained)
- patterns of access to enable tracking of transactions or particular user activity
- changes to access logging parameters

Logs should be reviewed periodically, based on the business impact of potential or actual access violations by authorized IT staff.

IP5.0 Change Management

Changes to the GNWT computer environment (i.e. enhancements, software fixes, data adjustments, hardware/software upgrades) often have unforeseen effects, and may accidentally or deliberately impact service levels or compromise security controls. Sound management can reduce the risk of such incidents occurring. This section covers the procedures applied throughout the change management process.

IP5.1 Change Management Standards/procedures

Objective

Ensure changes within the GNWT computer environment are made in conformance with sound procedures.

Standard of Best Practice

Changes to the computer environment should be made in accordance with formal standards/procedures.

Formal change management standards/procedures should cover changes of all types, including software or equipment upgrades, software fixes, changes to business information, updating of parameter settings and correction of erroneous information.

Formal change management standards/procedures should cover changes to:

- custom-made software, integrated application packages, desk-top products, and emergency fixes
- systems software including operating systems and utilities
- revisions to parameter tables and settings
- file/database formats and structures
- modification of business information, such as data tables, files and databases
- changes to user or operating procedures
- computers and related equipment
- communications networks, including new methods of connection and new data circuits

IP5.2 Change Management Process

Objective

Ensure changes do not affect the availability of the computer environment or compromise the confidentiality/integrity of GNWT data.

Standard of Best Practice

Changes affecting the computer environment should be made through a formal process.

Prior to promotion to the production environment, arrangements should be made to ensure that:

- change requests are documented, for example using a change request form, only accepted from authorized individuals, and approved by a business 'owner' before work commences
- the impact of changes is assessed, and reviews performed to ensure that changes do not compromise security controls
- changes are rigorously tested, and synchronized across all key components of the environment
- changes are checked and authorized by all relevant individuals
- software is checked to ensure it does not contain malicious code
- the environment can recover from, or roll back, failed changes

Changes made to the GNWT computing environment should be performed by individuals with adequate skills, knowledge and tools, under the supervision of a departmental IT specialist. Changes should be made to a copy of the software prior to use in the production environment.

Arrangements should be made to ensure that once changes have been applied:

- version control is maintained, documentation is updated and details of changes are communicated to all relevant users
- a record is maintained showing what was changed, when and by whom
- checks are performed to confirm that only intended code has been changed
- 'before and after' contents of key records, (for example within database master files) have been scrutinized

IP5.3 Acceptance Criteria

Objective

Ensure rigorous acceptance criteria are met before new, or significantly modified systems, are placed into production within the GNWT environment.

Standard of Best Practice

Formal criteria should be established to cover the implementation of new or significantly changed systems.

Government departments should ensure before accepting new systems or significant changes in the production environment checks are made to ensure:

- security assessments have been carried out and limitations of security controls documented
- performance and capacity requirements can be fulfilled
- all development problems have been successfully resolved
- there will be no adverse effect on existing production systems
- the system can be supported on a continuing basis
- arrangements for fall-back have been established in the event the changes made failed to function as intended
- sign-off has been obtained from the business owner
- error recovery and restart procedures have been established and computer contingency plans have been developed/updated
- operating procedures have been tested
- users have been educated in the use of the system and computer staffs are trained to run the system correctly

Old software, procedures and documentation should be updated.

Acceptance checks should ensure only tested and approved versions of software are accepted into the production environment and new/upgraded software is successfully distributed without unauthorized change. Responsibility should be transferred to individuals running the systems once the installation is complete.

IP5.4 Emergency Fixes

Objective

Enable unforeseen problems to be addressed in a timely yet disciplined manner.

Standard of Best Practice

Formal standards/procedures should be established by government departments covering emergency fixes to computer equipment, business application software, systems software, parameter settings, business information and system details.

Formal standards/procedures should cover emergency access by business 'owners' or users, system administrators, systems development staff and suppliers of equipment, software or services.

Emergency fixes should be consistent with formal standards/procedures, logged, and approved by the most senior manager present.

Once fixes are made, authorization for emergency access should be revoked immediately.

Emergency fixes should be documented, subjected to normal change management disciplines, and reviewed by the asset 'owner'.

Steps should be taken to ensure that emergency fixes are not left permanently in place.

IP6.0 Local Security Management

A computer environment typically supports one or more critical business applications, holds information needing to be protected, and is an important asset in its own right. Each role must be considered to provide appropriate protection. This section covers the arrangements made to ensure information security is managed and coordinated for the environment as a whole.

IP6.1 Security Organization

Objective

Provide a top-down management structure and practical mechanism for coordinating the GNWT information security activities.

Standard of Best Practice

Deputy Ministers are responsible for IT Security within their departments. The person in charge of the computer environment within the department should be personally accountable for the information security of the environment. One or more individuals (i.e. Security Officers) should be made responsible for coordinating and being the contact for the information security arrangements and issues.

Departmental Security Officers should:

- have a sound understanding of their information security roles
- have the knowledge, skills, time, tools, contacts and authority needed to carry out their assigned role
- be supported by procedures for day-to-day security administration and up-to-date information on issues related to information security
- maintain a communication channel with their counterparts in other departments and with the Chief Security Officer within the Office of the CIO

Departmental Security Officers should meet periodically with the person responsible for the departmental environment, and user representatives, to review the status of information security, review local security incidents, and agree on security activities to be performed.

IP6.2 Security Awareness

Objective

Maintain awareness of information security among individuals who run or use the GNWT computer environment.

Standard of Best Practice

Individuals involved in Information Technology activities should be aware of, and comply with the high-level information security policy that applies across the GNWT. These individuals should include, but are not limited to, business 'owners', users and personnel who run the IT environment.

Individuals involved in Information Technology activities should be made aware of:

- the meaning of information security and why it is needed
- the importance of complying with information security policies and applying associated standards and procedures
- their personal responsibilities for information security
- particular security threats to the environment

Individuals involved in Information Technology activities should be made aware that they are prohibited from:

- using any part of the environment without authorization or for purposes that are not acceptable under the network usage policy
- making obscene, racist or otherwise defamatory statements
- illicit copying of information or software that violates copyright laws
- disclosing confidential information in violation of ATIPP, or other relevant acts or legislation

IP6.3 Data Classification

Objective

Classify GNWT data according to its sensitivity to communicate how it should be treated.

Standard of Best Practice

The data contained within computer environments should be classified using the classification system set forth in the GNWT guidelines for “Threat and Risk Assessment”.

The classification scheme should consider the:

- business impact of a loss of confidentiality, integrity or availability
- sensitivity of information to be stored in or processed by the environment
- vulnerability of the environment to particular threats

Data classifications should be:

- used to establish the criticality of business applications supported by the environment
- applied to all information in electronic or paper form, all software and hardware, and to services provided by external parties
- approved by the person in charge of the environment
- reviewed by the Departmental Security Officer and the individuals in charge of the business applications supported by the IT branch of the department
- revised periodically in the light of changing circumstances
- recorded in formal agreements with users, such as service level agreements

Details of data classifications should be recorded in an inventory and include:

- the identity of the individual responsible for them
- unique identifiers such as descriptive titles
- the classification level of the data
- an access policy defining who is authorized to access the information
- the identity of the legal entity that owns the data

The computer environment should be protected in line with its security classification.

IP6.4 Risk Analysis

Objective

Identify key risks associated with the GNWT computer environment and determine the controls required to keep those risks within acceptable limits.

Standard of Best Practice

A formal risk analysis as outlined in the GNWT's guidelines for "Threat and Risk Assessment" should be carried out periodically for computer environments supporting critical business applications within government.

The risk analysis technique used should:

- include identifying critical business applications supported within the environment and a review of associated service level agreements
- involve representatives of key areas, such as business 'owners' of critical business applications supported by the IT organization, the person in charge of the IT environment, IT staff and an expert in risk analysis
- determine business risk (considering the criticality of the environment, the business impact of a loss of confidentiality, integrity or availability, key threats and vulnerabilities)
- consider the sensitivity of information to be stored in or processed
- consider the vulnerability of the environment to particular threats
- consider the full range of controls needed to keep risks within acceptable limits

The results of the risk analysis should include a clear indication of key risks, an assessment of their potential business impact and recommendations for actions required to reduce risk to an acceptable level.

The results (including any residual risk) should be reviewed and agreed to by the person in charge of the environment, and communicated to the 'owners' of business applications supported by the associated IT group. Agreed actions should be implemented and a process established to ensure that this is done effectively.

IP6.5 Security Assessment/Review

Objective

Provide Deputy Ministers, the person in charge of the computer environment, and senior management, with an independent assessment of the security of their environment.

Standard of Best Practice

The information security status of the computer environment of each department should be subject to thorough, independent and regular security assessment/reviews by the Internal Audit Bureau. Security assessments/reviews should cover installation management, the live environment, system operation, access control, change management, local security management and service continuity.

Security assessments/reviews should assess the business risks associated with the environment by:

- reviewing the information security requirements of the business applications supported within the environment
- evaluating the environment's vulnerability to key threats

Security assessments/reviews of the environment should be:

- conducted in consultation with Internal Audit Bureau
- agreed to by the person in charge of the IT environment
- defined in scope and documented
- performed by qualified individuals and checked by competent personnel
- supported by the use of automated software tools as approved by the Office of the CIO

Agreed upon recommendations from security assessments/reviews should be implemented and reported to senior management within the department**.** Recommendations from security assessments that cannot be implemented should be documented. Documentation should include the reason that the recommendation cannot be implemented and/or future actions to resolve the issue**.**

IP7.0 Service Continuity

A serious interruption to information processing, for example if a disaster occurs, can result in the computer environment being unavailable for a prolonged period. Considerable forethought is required to enable information processing to continue in these circumstances and keep the business impact to a minimum. This section covers the development and content of contingency plans, and the coverage and validation of contingency arrangements.

IP7.1 Contingency Plans

Objective

Provide departmental staff with a documented set of actions to perform in the event of a disaster, enabling information processing to be resumed within critical timelines.

Standard of Best Practice

Contingency plans should be formulated to ensure government staff are aware of the steps required in the event of a disaster affecting the computer environment.

The format and content of contingency plans should comply with government-wide standards/procedures as set forth by a specialist in Risk Management, form part of a wider business continuity plan and be distributed to all individuals who would require them in case of an emergency. Such individuals should be informed of their responsibilities and equipped to fulfill them.

Contingency plans should be developed in conjunction with user representatives based on:

- identification of the key business processes to be protected by the plan
- assessments of the business impact of such scenarios
- a set of scenarios for possible disasters

Plans should include:

- conditions for their invocation
- the critical timelines associated with the business applications supported by the environment
- a schedule of key tasks to be carried out, responsibilities for each task and a list of services to be recovered in order of priority
- information security controls applied during the recovery process
- arrangements for processing from last successful backup to time of disaster and then to resumption of normal service
- provisions for the clearance of any processing backlogs that may have built up during the system outage
- resuming processing using alternative facilities

- procedures specified in sufficient detail to be followed by individuals who do not normally carry them out

Custody of the contingency plan should be the responsibility of a specific individual or group and copies of the plan should be stored securely offsite.

IP7.2 Contingency Arrangements

Objective

Enable processing to continue in the event of a disaster.

Standard of Best Practice

Alternative information processing arrangements should be established to enable service continuity to the citizens of the Northwest Territories in the event of a disaster affecting a computer environment.

The arrangements should cover prolonged unavailability of:

- key individuals, buildings or access to buildings
- business information or system/application software
- essential services such as electricity, water, telephone lines and data communications
- system documentation

Contingency arrangements should cover all locations and users supported by the department. Key components of the environment should be covered by arrangements that address key risks (such as loss of data, business interruption, or liabilities to third parties) and provide adequate protection against likely threats (such as fire, theft, fraud or malicious damage).

IP7.3 Validation and Maintenance

Objective

Ensure information processing can resume within critical timelines, using alternative facilities.

Standard of Best Practice

Regular tests should be conducted of the contingency arrangements for the computer environment.

Tests of contingency arrangements should:

- be carried out in accordance with a defined schedule
- be performed after significant changes are made to contingency arrangements
- be carried out periodically, and at least annually
- include realistic simulations involving both users and IT staff
- demonstrate information processing can resume within critical timescales

Contingency arrangements should be:

- the responsibility of a designated individual or working group
- updated following significant changes to business processes
- revised in response to problems encountered during tests/rehearsals

The need for changes should be considered at least monthly and contingency arrangements as a whole should be reviewed at least annually.

SYSTEMS DEVELOPMENT (SD)

Building security into GNWT systems during their development is more cost-effective and secure than attempting to add it on afterwards. It requires a structured approach to systems development, and sound procedures to be observed throughout the development cycle. Ensuring information security is addressed at each stage of the cycle is critical.

SD 1.0 Approach

Producing secure, robust systems, on which the GNWT can depend, requires a sound approach to systems development. This section covers the roles and responsibilities of systems development staff, the methodologies used in developing systems, arrangements made for assuring quality, the security of the development environment and the arrangements needed to ensure outsource contractors satisfy the GNWT's security requirements.

SD1.1 Roles and Responsibilities

Objective

Provide a sound management structure over the personnel involved in systems development activity.

Standard of Best Practice

Every system development project should have a designated individual responsible for development activity (for example a project manager) and a business 'owner' familiar with the Government's System Development Life Cycle (SDLC) methodology.

Each Government Department's IT Branch should have a designated individual with overall responsibility for system development.

Responsibility for key tasks (such as compliance with development standards, quality assurance, and definition of requirements, risk analysis, design/build, testing, implementation and change management) should be assigned to designated individuals.

Government staff involved in development projects should be:

- assigned clear responsibilities
- equipped with sufficient technical knowledge to develop systems correctly and securely
- sufficient in number to handle planned workloads
- competent to deal with error, exception and emergency conditions
- aware of information security principles, best practice and potential information security solutions
- aware of legislative acts dealing with privacy related issues (i.e. ATIPP)

Reliance on key individuals should be minimized by appointing designates, using standard techniques/technologies, maintaining complete and accurate documentation and ensuring segregation of duties.

SD1.2 Development Methodologies

Objective

Ensure development activity throughout the GNWT is carried out in conformance with sound procedures.

Standard of Best Practice

Development activity should be carried out consistent with the Government's System Development Life Cycle (SDLC) methodology.

Development methodologies should:

- be suitable for the types of project carried out
- cover definition of requirements, design and build activity, testing, implementation activity and change management
- require information security requirements to be formally documented and defined in terms of the need to maintain confidentiality, integrity and availability of information
- be kept current

All individuals involved in systems development should apply development methodologies. Compliance with methodologies should be monitored.

SD1.3 Quality Assurance

Objective

Provide assurance that systems developed meet the business and information security requirements of the GNWT.

Standard of Best Practice

Quality assurance activities should be applied to all systems under development.

Quality assurance activities should include an assessment of development risks. Such risks should be assessed at an early stage of the development process, documented, and reviewed at key stages during the development lifecycle.

Assessments of risk should cover project management, business requirements, benefits, resilience, technological compatibility, technical performance, costing and timescales.

Action should be taken to minimize development risks by considering alternative approaches, revising staffing arrangements, plans or timescales and canceling developments with unacceptable risks.

Development activity should be subject to supervisory review, and spot checks performed to ensure compliance with system development methodologies.

Quality assurance activities should:

- follow a structured approach
- cover all stages of development activity
- comply with a recognized standard for quality management
- produce specific recommendations for improvement

Results of quality assurance activities should be reviewed by the person in charge of development activity, (for example the project manager), and the business ‘owner’.

SD1.4 Development Environment

Objective

Provide a secure environment for development activities within the GNWT.

Standard of Best Practice

Systems development activities should be isolated from live systems. A system development environment should be created where systems can be developed securely.

The development environment should be protected from viruses and malicious mobile code by anti-virus software. Access control software should be used to protect development software/information and prevent development staff from making unauthorized changes to the live environment.

Program source code should be protected by:

- avoiding storage on live systems
- restricting access to designated development staff
- segregating source code under development from programs that are operational
- recording all access in an audit log
- archiving old versions periodically

Documentation of system development activity should be maintained (including development logs, approvals and project plans). System documentation should be kept up-to-date, held in accessible form and protected against loss or damage.

SD1.5 Outsourcing

Objective

Ensure security requirements of the GNWT are satisfied when systems development is entrusted to an outsource contractor.

Standard of Best Practice

Prior to outsourcing responsibility for some or all systems development activity, government departments should:

- identify risks and assess security practices employed by outsource contractors
- agree to security controls, approve transfer, and establish formal agreements

Formal agreements should oblige contractors to:

- comply with good business practice, report incidents and provide regular reports on systems development activity
- adhere to the GNWT IT Security Policies and Standards for IT Security
- maintain the confidentiality/integrity of information gained in the course of work, limiting access to authorized users
- maintain continuity of services in the event of a disaster
- apply agreed information security controls, ensuring legal and regulatory requirements including data privacy (i.e. ATIPP) are met
- assure the quality and accuracy of development activity undertaken
- permit their activities to be audited
- adhere to agreed upon service level agreements

Formal agreements should specify details of licensing arrangements, ownership of code and intellectual property rights.

Arrangements should be made to deal with a single point of contact within the outsource contractor. Sufficient resources should be provided to manage the relationship with the outsource contractor on an informed basis.

Responsibility for managing the relationship with the outsource contractor should be assigned to a designated individual, equipped with sufficient technical skills and knowledge.

SD2.0 Business Requirements

A thorough understanding of business requirements (including information security requirements) is essential if systems are to fulfill their intended purpose. This section covers the arrangements made for identifying the level of criticality of systems under development, conducting risk analyses, specifying business requirements and assessing the security controls needed to fulfill them.

SD2.1 Data Classification

Objective

Classify systems under development and the data contained within, according to its sensitivity in order to communicate how it should be treated.

Standard of Best Practice

The system under development should be classified using the classification system set forth by the Electronic Security Committee.
Data classification should consider important issues that may affect a system once it has gone live, such as the:

- business impact of a loss of confidentiality, integrity or availability
- sensitivity of information to be stored in or processed by the system under development and the period of time for which it remains sensitive
- vulnerability of the system to particular threats

Data classifications should be:

- used to establish the criticality of the system and data under development
- applied to all information to be processed in electronic or paper form, all software being developed, all hardware being acquired, and to all services to be provided by external parties
- approved by the person in charge of the system under development
- reviewed by the Departmental Security Officer and the individuals in charge of the business processes supported by the system under development
- revised periodically in the light of changing circumstances
- recorded in formal agreements with users, such as service level agreements

Data classifications for a system under development should be recorded in an inventory and should include:

- the identity of the individual responsible for them
- unique identifiers such as descriptive titles
- their data classification
- an access policy defining who is authorized to access the system
- the identity of the business 'owner'

Systems under development should be protected in line with their security classification

SD2.2 Risk Analysis

Objective

Identify key risks associated with systems under development and determine the controls required to keep risks within acceptable limits.

Standard of Best Practice

A formal risk analysis should be carried out for important or critical systems under development by the GNWT.

The risk analysis should:

- be carried out at an early stage of the system development process, in compliance with formal standards/procedures for risk analysis and using formal risk analysis methodologies
- be reviewed at key stages of the system development process
- involve representatives of key areas, such as the 'owners' of the system under development, the project manager, an IT specialist, key user representatives and, for critical systems, a specialist in Risk Management
- determine business risk (taking into account the criticality of the installation, the business impact of a loss of confidentiality, integrity or availability, key threats and vulnerabilities)
- take into account the full range of controls needed to keep risks within acceptable limits

The results of the risk analysis should include a clear indication of key risks, an assessment of their potential business impact and recommended actions to reduce risk to an acceptable level.

The results (including any residual risk) should be reviewed and agreed to by the person in charge of the system under development, and communicated to the 'owners' of business processes supported by the system under development. Agreed actions should be implemented and a process established to ensure that this is done effectively.

SD2.3 Specification of Requirements

Objective

Document and agree on the business requirements before detailed design/specification commences. Ensure information security requirements are treated as an integral part of business requirements and fully considered.

Standard of Best Practice

Business requirements for applications under development by the GNWT should be defined using a formal process.

Business requirements for the system under development should be clearly defined in terms of scope, resources, and roles/responsibilities. They should be documented and supported by an agreed process for handling changes to requirements.

The specification should include requirements for:

- system capacity, availability, continuity, flexibility, connectivity and compatibility
- information processing, storage and transmission (including requirements for protecting integrity and confidentiality)
- arrangements needed to support the system in the production environment
- compliance with contractual, legal and regulatory obligations
- access control arrangements, such as access by particular types of user or from particular locations
- segregation of duties

Business requirements should be signed-off by the business 'owner', the Departmental Security Officer or their designate, and the person in charge of development activity.

SD2.4 Security Controls

Objective

Ensure an appropriate set of security controls is identified when formulating business requirements.

Standard of Best Practice

The full range of controls should be assessed when formulating business requirements.

The assessment should include a review of the controls needed to ensure:

- the validity of information processed can be readily established
- the completeness and accuracy of information processed can be confirmed by comparison with control balances or original documentation and the rigorous checking of changes to key files and parameters
- accountability for actions can be determined
- the opportunity for error or abuse is minimized, such as by automating processes and the maintenance of a complete and reliable audit trail, including error and exception reports

The assessment should include a review of the general controls needed to ensure:

- responsibilities are assigned and duties segregated
- systems resilience is maintained, by minimizing single-points-of-failure, provision of adequate capacity and back-up/contingency arrangements
- the integrity/confidentiality of critical information is protected, by employing access control functionality, non-repudiation techniques and encryption of files stored or in transit
- compliance with contractual, regulatory or legal obligations

Proposed controls should be reviewed to ensure they are proportional to business risk.

SD3.0 Design and Build

Building systems to function as intended requires careful consideration of information security and the maintenance of sound procedures throughout the design and build stages of development. This section covers the arrangements made to address information security during design, acquisition and system build, including additional controls required for electronic commerce developments.

SD3.1 Design

Objective

Produce an operational system based on sound design principles with security functionality built in and/or easily enables controls to be incorporated y.

Standard of Best Practice

Information security requirements for systems under development by the GNWT should be considered when evaluating alternative designs.

The design phase should include:

- specification of a system architecture that supports technical system requirements
- identification of where security controls are to be applied
- documentation of control limitations and a review of designs to ensure controls are in place
- consideration of how individual controls work together to produce an integrated system of controls

The evaluation of alternative designs for the system under development should consider the:

- integration with existing information security architecture
- use of government wide security solutions
- cost of implementing controls
- skills needed to develop required solutions
- capability of the organization to develop and support the chosen technology

Before coding or acquisition work begins, system designs should be documented, verified to ensure that they meet business requirements, and reviewed by the Departmental Security Officer. System designs should be signed-off by the project manager and, for critical systems, by the person in charge of development activity within the department.

SD3.2 Acquisition

Objective

Ensure the software, hardware and services acquired from third parties provide the required functionality and do not compromise the security of systems under development by the GNWT.

Standard of Best Practice

The acquisition of system components should be in accordance with formal standards/procedures. All types of system components should be covered, including application packages, systems software, specialized security products (such as anti-virus software, encryption mechanisms and firewalls), computer/communications equipment and external services.

Controls over acquisition should include:

- selecting products and services from approved lists (with a high priority placed on reliability), assessing them against security requirements and supporting them by contractual terms agreed upon with suppliers
- addressing potential security weaknesses in products and services by considering external security ratings, identifying security deficiencies and implementing remedial measures
- meeting software licensing requirements by obtaining adequate licenses for planned use, maintaining software documentation as proof of ownership and recording details,

The acquisition of products should be reviewed by staff with the knowledge to adequately evaluate them.

SD3.3 System Build

Objective

Ensure systems are built correctly and security weaknesses are not introduced during the build process.

Standard of Best Practice

System build activities (such as coding programs, creating web pages, customizing packages or defining data structures) should be carried out in accordance with formal standards/procedures.

The build of the system under development should be documented, and inspected to identify unauthorized changes.

When building systems, steps should be taken to ensure that:

- system build activities are performed by individuals equipped with adequate skills, knowledge and tools
- staff comply with common industry standards
- system performance is optimized
- the use of insecure design techniques is prohibited
- automated tools are used to ensure adherence to programming standards
- system build activities are inspected to identify unauthorized modifications or changes that may compromise security controls
- staff are prohibited from making changes to the base code of software packages

Where modifications have to be made to the base code of software packages, a formal process should be applied, which:

- considers special risks, such as suppliers refusing to support or maintain modified software and incompatibility with future updates
- specifies changes can only be made following approval by a systems development manager, with written permission from the supplier and only to a copy of the original code

A responsible team leader should review system build activities to ensure individual components of the system function as intended (for example, by program testing) and to confirm no security weaknesses have been introduced (for example as a result of package customization).

SD3.4 Electronic Commerce Development

Objective

Ensure the risks associated with developing electronic commerce applications are minimized.

Standard of Best Practice

Additional controls should be employed when developing applications to support electronic commerce.

GNWT web site(s) should include a prominently displayed privacy policy reviewed and approved by the appropriate branch of the GNWT.

Web servers that support applications should be prevented from running with high level privileges on a day to day basis, initiating network connections to the Internet, or uploading unknown files.

Interfaces between web servers and back end systems (i.e. databases) should be restricted to those services required by the application, based on documented application programming interfaces (APIs), and supported by mutual authentication. Connectivity between web servers and back end systems should occur through security systems. (i.e. firewalls)

Web application sessions should be protected against being hijacked or cloned by ensuring session IDs cannot be easily predicted, for example by including a random element.

The disclosure of system configuration information (that could be useful to hackers) should be prevented by:

- suppressing the server field in http headers that identify the web server's brand and version
- ensuring directories of files on web servers are not indexed
- ensuring source code of server-side executables and scripts, such as Common Gateway Interface (CGI) scripts cannot be viewed by a browser
- ensuring the source of HTML, JavaScript and other client-side scripting languages do not contain unnecessary information, such as details of web CGI functions or comments

Server-side executables and scripts, such as CGI scripts, should be checked for potential vulnerabilities using automated tools, and configured to record actions performed.

Prior to going live, e-commerce initiatives should been formally approved by senior management, tested rigorously using very large numbers of users, and undergone a vulnerability assessment by the Office of the CIO or their designate.

SD4.0 Testing

Testing is a fundamental element of good practice in systems development. Well planned, and correctly performed, it provides assurance systems, including security controls, function as intended and reduces the likelihood of system malfunctions occurring. This section covers the arrangements needed to carry out thorough testing without disrupting other activities.

SD4.1 Testing Standards/procedures

Objective

Ensure testing is carried out in conformance with sound procedures.

Standard of Best Practice

New or changed GNWT systems should be tested thoroughly in accordance with formal standards/procedures.

Formal testing standards/procedures should require testing to cover:

- the full functionality of business requirements
- use under normal and exceptional conditions
- the impact of bad data
- interfaces with other systems
- the effectiveness of controls
- system performance when handling planned volumes of work (i.e. load testing with realistic numbers of users/volumes of transactions)
- identification of maximum system capacity
- fall-back arrangement to previous versions

Formal testing standards/procedures should require:

- new systems and significant changes to be tested prior to use in accordance with a documented test plan
- that the use of personal information for testing purposes complies with provincial and federal legislation and take into account requirements under ATIPP

SD4.2 Testing Process

Objective

Ensure GNWT systems are thoroughly tested.

Standard of Best Practice

All elements of a system (i.e. application software packages, system software, hardware and services) should be tested before promotion to the production environment of the GNWT.

New and significantly changed systems should be tested thoroughly in accordance with pre-defined, documented test plans. Test plans should be cross-referenced to the system design/specification to ensure complete coverage. Representatives of user groups should be involved in planning tests, and producing test data.

Tests should cover:

- the full functionality of business requirements
- use under normal and exception conditions
- the impact of bad data
- interfaces with other systems, such as program calls or hyperlinks
- the effectiveness of controls
- system performance when handling planned volumes of working (i.e. load testing with realistic numbers of users/volumes of transactions)
- identification of maximum system capacity
- fall-back arrangement to previous versions

Automated tools should be used to improve the testing process, for example to check the validity of system interfaces or simulate loading from multiple clients.

Final test results should be documented, reviewed (for example against expected results) approved by users and signed-off by the business ‘owner’ concerned.

SD4.3 Acceptance Testing

Objective

Ensure only rigorously tested systems satisfying user requirements are promoted to the production environment of the GNWT.

Standard of Best Practice

User acceptance tests (UAT) should be carried out in an environment isolated from the production environment and separated from other development activities (such as program coding or package customization).

Acceptance tests should:

- involve business users
- simulate the production environment
- involve running the full suite of system components, such as all application functionality, database management utilities and the underlying operating system
- feature testing to ensure that there will be no adverse effects on existing systems
- involve independent security assessments of critical code to detect vulnerabilities and insecure use of programming features
- include attempts to breach the security of the system, for example by performing a vulnerability assessment and/or a penetration test

Information copied from the production environment for the purposes of conducting acceptance tests should be protected by:

- requiring separate authorization each time information is copied from the live into the testing environment
- applying access controls in the testing environment
- erasing copies of business information once testing is complete
- logging the use of business information for testing purposes

SD5.0 Implementation

Sound procedures are required when new systems are transferred from the development environment into the GNWT production environment. This section covers the promotion of new systems from the development environment, their installation in the production environment, user procedures and training and post-implementation reviews.

SD5.1 Acceptance Criteria

Objective

Ensure rigorous acceptance criteria are met before new systems and significant changes are promoted into the GNWT production environment.

Standard of Best Practice

Formal acceptance criteria should be met before new systems and significant changes are promoted into the production environment.

Before accepting new systems and significant changes in the production environment, checks should be made to ensure:

- security assessments have been carried out and limitations of security controls documented
- performance and capacity requirements can be fulfilled
- all development problems have been successfully resolved and there will be no adverse affect on existing production systems
- the system can be supported on a continuing basis
- arrangements for fall-back have been established in the event of the changes made failing to function as intended
- sign-off has been obtained from the business ‘owner’
- error recovery and restart procedures are established and computer contingency plans are developed/updated
- operating procedures have been tested and documented
- users have been educated in use of the system and computer staff are trained in how to run the system correctly

Steps should be taken to ensure that only tested and approved versions of software are accepted into the production environment and new/upgraded software is successfully distributed without unauthorized change.

SD5.2 Installation Process

Objective

Ensure new or significantly changed systems are installed in the production environment of the GNWT without disruption.

Standard of Best Practice

New or significantly changed systems should be installed in the production environment in accordance with a formal, documented installation process.

The installation process should include:

- validating the load or conversion of data files
- restricting the installation of new or significantly changed software
- implementing new/revised procedures and documentation and discontinuing old versions
- arranging for fall-back in the event of failure
- informing the individuals involved of their roles and responsibilities
- handing over responsibility to staff running the live environment
- recording installation activity

The installation of systems into the production environment should be scheduled in advance to avoid disrupting information processing activities and enable installation to occur in a timely manner.

SD5.3 User Procedures and Training

Objective

Ensure users of GNWT systems are using systems correctly.

Standard of Best Practice

Users' responsibilities should be clearly defined. Users should be able to carry out their roles supported by documented procedures, help facilities and training.

Users of new or significantly changed systems should be:

- involved in - and contribute to - the development process
- equipped with the knowledge and skills to use systems correctly
- formally trained

User training should be carried out prior to systems going live and include information security tasks and responsibilities. User training programs should be signed-off by the project manager, the business 'owner' and the Departmental Security Officer or their designate.

SD5.4 Post-implementation Review

Objective

Verify system(s), and their information security controls function as intended.

Standard of Best Practice

Post-implementation reviews should be conducted for new or significantly changed systems.

Post-implementation reviews should cover:

- fulfillment of business (including information security) requirements
- efficiency, effectiveness and cost of controls
- scope for improvements of controls
- review of security incidents

Results of reviews should be signed-off by the project manager, the business 'owner' and the Departmental Security Officer or their designate. A copy of this report should be provided to the Internal Audit Bureau.

SD 6.0 Change Management

It is important for changes to the GNWT production environment be well managed. Changes to production systems (i.e. enhancements, software fixes, data adjustments, hardware/software upgrades) often have unforeseen effects, and may accidentally or deliberately impact service levels or compromise security controls. Sound management can reduce the risk of such incidents occurring. This section covers the disciplines applied throughout the change process.

SD6.1 Change Management Standards/procedures

Objective

Ensure changes to GNWT production systems are made in conformance with sound procedures.

Standard of Best Practice

Changes should be made in accordance with documented formal standards/procedures.

Formal documented change management standards/procedures should cover changes of all types, including software or equipment upgrades, software fixes, changes to business information, updating of parameter settings and correction of erroneous information.

Formal change management standards/procedures should cover changes to:

- in-house application software, integrated application packages and desk-top products
- systems software including operating systems and utilities
- file/database formats and structures
- computers and related equipment
- communications services, such as new methods of connection

SD6.2 Change Management Process

Objective

Ensure changes to GNWT production systems do not affect its availability or compromise the confidentiality/integrity of associated business information.

Standard of Best Practice

Changes affecting the production environment should be made in accordance with a documented formal process.

Prior to promotion to the live environment, arrangements should be made to ensure:

- change requests are documented, only accepted from authorized individuals, and approved by the business 'owner' before work commences
- the impact of changes are assessed, and reviews performed to ensure that changes do not compromise security controls
- changes are rigorously tested and synchronized across all key components of the live environment
- changes are checked and authorized by all relevant individuals
- software is checked to ensure it does not contain malicious code
- the system within the production environment can recover from failed changes

Changes should be performed by individuals equipped with adequate skills, knowledge and tools under the supervision of senior IT staff. Changes should be made to a copy of the software or data prior to use in the production environment.

Arrangements should be made to ensure that once changes have been applied:

- version control is maintained, documentation is updated and details of changes are communicated to all relevant users
- a record is maintained showing what was changed, when and by whom
- checks are performed to confirm that only intended code has been changed
- 'before and after' contents of key records (for example within databases) have been scrutinized

SD6.3 Emergency Fixes

Objective

Enable government departments to address unforeseen production problems in a timely yet disciplined manner.

Standard of Best Practice

Formal documented standards/procedures should be established for emergency fixes to computer equipment, business application software, systems software, parameter settings, business information and system details (such as back up files).

Emergency fixes should be made in accordance with formal standards/procedures, logged, and approved by the most senior IT manager present.

Once fixes are made, authorization for emergency access should be revoked immediately.

Emergency fixes should be formalized and reviewed by the person in charged of development activity.

Steps should be taken to ensure emergency fixes are not left permanently in place.