6003.00.26

Northwest Territories

Policy

GNWT
INFORMATION TECHNOLOGY
Electronic Information Security

1. Statement of Policy

The Government of the Northwest Territories recognizes that the increased use of information technologies to serve the public and to record its business requires that electronic information assets collected or made available electronically must be maintained in an environment that protects the confidentiality, availability, and integrity of the information over time and through technological change.

Taking into account this complex information technology environment, departments must maintain electronic information assets in their custody or under their control in a way that is consistent with this policy and complies with the *Access to Information and Protection of Privacy Act*, the *Archives Act*, the *Financial Administration Act*, and all other GNWT legislation and policies.

2. Purpose

This policy provides direction on how the Government of the NWT will implement information security standards, guidelines, and procedures. This policy sets baseline requirements and responsibilities for the secure use of electronic information, information systems, and technologies, in order to fulfill our mandates, support program and service delivery, achieve strategic priorities, and meet accountability obligations prescribed by law.

3. Principles

The Government of the Northwest Territories has a responsibility to protect the rights and entitlements of the residents of the NWT and our business partners. The following principles will help fulfil that responsibility:

- Responsibility and accountability for electronic information security must be explicit.
- Awareness of risks and security initiatives must be disseminated.
- Security must be addressed taking into consideration both technical and non-technical issues.
- Security must be cost-effective**.**
- Security must be coordinated and integrated.
- Security must be reassessed periodically.

- Security procedures must provide for monitoring and a timely response.
- Ethics must be promoted by respecting the rights and interests of others.

4. Scope

This policy applies to all Electronic Information Assets and the underlying technologies used in the creation, maintenance, processing, storing, transmission or disposition of information within or by the Government of the Northwest Territories. Boards, Authorities, and other arms length organizations are required to comply with this policy when using GNWT electronic information assets to deliver their services.

Other aspects of Security, including non-electronic, information fall outside this scope.

5. Definitions

"Electronic Information Assets" refer to the information and information technology assets used to support the delivery of government programs and services, and are comprised of the following:

- "Electronic information" refers to the data and information held by the Government of the NWT and its boards and agencies, used in the management planning and delivery of its programs and services on behave of the residents of the Northwest Territories.

- "Information technology assets" are the, computer hardware, software and networks that are used to store, process or transmit electronic information.

"*Availability*" refers to the assurance that information will be ready for use as expected and when required until such time that the Public Records Committee has authorized its destruction.

"*Confidentiality*" refers to the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to GNWT or other interests, with reference to specific provisions of the Access to Information and Protection of Privacy Act.

"Integrity" refers to information being complete and accurate with no unauthorized alterations. Information can be altered and retain its integrity provided the alterations are allowed by policy, are authorized, and are documented

"*Baseline security requirements*" are mandatory provisions of the Government Electronic Information Security Policy and its associated operational standards, procedures and technical documentation.

"*Office of the CIO*" is the Government of the NWT Office of the Chief Information Officer.

6. Responsibilities

I. Employees of the Government of the NWT and its Boards Authorities and other arms length organizations are responsible for understanding the privacy and security implications of their position within the government and to comply with the security requirements identified by the "*Use of Government Email and Internet Guidelines and the GNWT Code of Conduct."*

- Employees of the Government of the NWT and its Boards Agencies and other arms length organizations agencies shall not engage in activities that may compromise the security electronic information assets of the GNWT.

II. Departments Boards, Authorities and other arms length organizations are accountable for all elements of information security in their custody or control including provisions for contracted services and acceptance of residual risks. This includes:

- conducting threat and risk assessment and data classification for all information assets
- the implementation of appropriate security measures to protect the integrity, availability and confidentiality of the information contained within the asset consistent with those published in the "Government of the Northwest Territories, Standard of Best Practice for Information Security Management"
- formalizing their security measures in a written document

III. The Electronic Information Security Committee (EISC) is responsible for ensuring that GNWT continues to meet its legal and fiduciary obligations by:

- maintaining this policy by bringing forward any revisions to Informatics Policy Committee (IPC)
- recommend new or updated security standards and guidelines in compliance with this policy to IPC, and
- annually report to IPC on the status of compliance and implementation of this policy.

IV. Based on the recommendations of the EISC, the Office of the CIO, will:

- communicate baseline security requirements to all stakeholders,
- define corporate technology security standards,
- review all threat and risk assessments for consistency, compatibility and completeness.
- review information security classifications for consistency and compatibility and
- authorize the implementation of corporate security measures.

V. Public Works and Services Systems and Communications (S&C) and The Technology Service Centre (TSC) are responsible for ensuring that:

- operational controls are adequate and compliant with corporate standards and consistent with the best practices established in “Government of the Northwest Territories, Standard of Best Practice for Information Security Management”
- Ongoing monitoring of unauthorized or inappropriate network or system access to enable detection of security incidents.

7. Authority and Accountability

I. General

This Policy is issued under the authority of the IPC. The authority to make exceptions and approve revisions to this Policy rests with IPC. Authority and accountability is further defined as follows:

- Electronic Information Security Committee

  Members of the Electronic Information Security Committee (EISC) are accountable to IPC for the provision of advice and recommendations on this maintenance and implementation of this policy and all supporting documentation.

II. Specific

The EISC Chairman is:

1. Responsible for documenting any policy revisions and presiding over EISC committee meetings reviewing this policy; and
2. Authorised to forward to IPC any policy revisions and recommendations from EISC members for further comments or suggestions.

8. Prerogative of the Information Policy Committee

Nothing in this Policy shall in any way be construed to limit the prerogative of the IPC to make decisions or take action respecting information or information technology security, outside the provisions of this Policy.

9. Supporting Documentation and Information

This policy is supplemented by Operational security standards approved by the IPC Chairman including the "*Government of the Northwest Territories Standard of Best Practice for Information Security Management*". They contain mandatory and recommended measures to direct and guide the implementation of the policy.

Chairman
Informatics Policy Committee

Appendix A - Committees

1. Electronic Information Security Committee

The Informatics Policy Committee established the Electronic Information Security Committee. Its members are:

- Two (2) representatives from the Recorded Information Management Committee
- Two (2) representative from Information Technology Advisory Committee
- Two (2) Access and Privacy departmental representatives
- 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 the Systems & Communications
- A Representative from FMBS, Labour Relations and Compensation Services
- Others as designated by IPC

2. Informatics Policy Committee

Financial Management Board established the Informatics Policy Committee as a sub-committee of the Senior Management Committee. Its members are:

- The Secretary of the Financial Management Board (Chair)
- The Deputy Minister of Public Works and Services
- The Deputy Minister of Education, Culture and Employment
- Two other Deputy Ministers or equivalents on a rotational basis

3. Recorded Information Management Committee

The Informatics Policy Committee established the Recorded Information Management Committee. Its members are:

- A representative from each GNWT department.
- A representative from the Records Management Unit of Public Works and Services (Chair)
- A representative from the Northwest Territories Archives
- A representative from the Office of the Chief Information Officer

Appendix A - Committees

4. Information Technology Advisory Committee

The Informatics Policy Committee established the Information Technology Advisory Committee. Its members are:

- Representatives from Informatics Policy Committee member departments.
- Deputy Ministers from non Informatics Policy Committee departments may recommend an employee from their department for participation on the committee
- The Chief Information Officer, Financial Management Board Secretariat, or designate (Chair)

5. Public Records Committee

The Archives Act establishes the Public Records Committee. Its members are:

- The Territorial Archivist (Chair)
- The Records Manager of Public Works and Services
- Such other persons as may be appointed by the Minister responsible for the Archives *Act*