



Records Management Tip

Records management advice prepared for GNWT records professionals by the Records Management Unit, PWS

No. 33 – February 2006

**Program
Management Series**

Implementing the Management of Electronic Information Policy

Part 5

Principle # 6 is quite lengthy. The first sub-clause was discussed in Records Management Tip # 32.

The Program Management series looks at various media-specific issues and special issues relating to records management.

Principle # 6

Electronic record keeping systems must be documented.

- Record keeping requirements for electronic records, including operational business needs, legal requirements and archival requirements, should be identified and determined at the point of system design, and built into the system to minimize the unnecessary retention of records that are not required, and to ensure that records of continuing value are identified, preserved and migrated. Final disposition for electronic records is according to approved Records Disposition Authorities.
- In the case of systems that have already been designed, record keeping requirements should be determined at the point of review, upgrade, or migration.
- Responsibility for identifying record keeping requirements is shared between the Business Manager for the system, the Departmental Records Coordinator, Records Management Services and NWT Archives. Record keeping requirements determine the degree to which business activities need to be supported by reliable and authentic records and how long the record should be retained.

Record Keeping Requirements

The term “record keeping requirements” refers to the government’s need to keep records for some purpose. Record keeping requirements are found in policies, procedures, legislation, and regulations. They are also identified through an analysis of business needs. These requirements direct which records must be kept, how long they must be kept, and how they are disposed of. They also identify the records of historical importance that should be preserved as government archives.¹

¹ We are referring to archives in the traditional sense: as a collection of public, corporate, or institutional records that are kept to document the actions and decisions of the government for posterity. This is as opposed to a data archives.

Incorporating Record Keeping Requirements into System Design

Record keeping requirements should be considered when information systems are designed or re-evaluated. Because these requirements could have an impact on how records are stored, reproduced, or removed from the system, it is best to identify them at an early stage. The ideal time to identify them is during the initial assessment of user requirements.

The policy identifies several individuals who should be consulted when systems are designed. They include:

- The Business Manager.
- The Departmental Records Coordinator.
- The Records Manager at Public Works and Services.
- The Territorial Archivist at Education, Culture, and Employment.

The first three individuals will identify the appropriate length of time for keeping records in the system. The Territorial Archivist will identify the records that need to be kept as government archives. The Territorial Archivist will also give direction on how records should be preserved over the very long term.

Principle # 7

Departments should establish systems to protect electronic information....

Information Security

Electronic information must be protected from unauthorized access and use.

Departments should review their electronic record holdings, and identify the records to which access should be limited. Systems should be designed so that users cannot view confidential or personal information that does not pertain to them or which they do not require to do their jobs.

Departments should review their security procedures, and instruct employees on how to secure their records. Efforts should be made to avoid unauthorized access to workstations and network applications. Simple precautions include locking workstations with a password when an employee is away from his or her desk.

A privacy impact assessment should be done on all systems that contain personal information.