



Records Management Tip

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

No. 25 – April 2005

Active Filing Series

Access Restrictions

Access restrictions were mentioned in Records Management Tip # 10, which looked at information security issues. This Records Management Tip will look at ways to implement access restrictions for records in your department.

The Active Filing series gives you tips on how to manage active records in your department.

What is an access restriction?

An access restriction is a policy or rule that makes information available to a limited number of people or for a limited use. Typically, the organization that owns the records will keep a list of the individuals or job titles that have access to a particular group of records. Only the authorized people will be given the right to retrieve and use these records.

For example, in the GNWT, only a small number of people from the Financial Management Board Secretariat (FMBS) have access rights to see employee files. Only those people who have a need to see the records are allowed to take them from the filing cabinets or retrieve them from the Records Centre.

What kinds of records have access restrictions?

There are a few common types of government records that have access restrictions. These records include:

- Executive Council (Cabinet) and Financial Management Board Records of Decision.
- Legal opinions.
- Human resources records, such as personnel files, grievance files, and the like.

Access to these records is restricted to those staff members that have a reason to see the records. These records should be kept in locked filing cabinets or in a room that can be locked. Keys should only be given to employees who are authorized to see the records.

Each department has other records that should probably be restricted for one reason or another. Typical reasons for restricting access to records include:

- They contain advice to senior management or the Minister.
- They contain sensitive information about plans, negotiations, or programs that are in the development phase.

- They contain personal information or confidential third party information.

Setting up access restrictions

The first step in setting up access restrictions is to identify the information that should be restricted. Review file lists, the Administrative Records Classification System (ARCS), and Operational Records Classification Systems (ORCS) with managers and directors. Try to identify series of records (or primaries in ARCS and ORCS) that should be restricted. Then, identify the job titles or positions in your department that should have access to this information. Avoid identifying individual employees by name.

Your department's records management manual should have a section on access restrictions. In this section, list the records series that have restricted access, and identify the job titles that have access to the records.

Educate employees in your department so that they know which records they can and cannot access.

Enforcing access restrictions

If your department is using iRIMS to manage files and folders, contact the RIMS Specialist at Public Works and Services to discuss access restrictions.

If you have identified electronic records that are stored on common network drives, such as the H:\ drive, I:\ drive, or J:\ drive, contact the Technology Service Centre or your IT Manager. The TSC will need to know which directories should be restricted and to whom access should be given.

Hard copy records that have access restrictions on them should be kept in secured locations. For example, they should be kept in locked filing cabinets or locked file rooms. Keys to filing cabinets or filing rooms should be restricted to only one or two people. Those people would be responsible for all filing and retrieval of confidential records.

The people who maintain the filing cabinets would also make sure that file charge-in and charge-out procedures are followed. All confidential records should be charged out to a user when they are removed from a filing cabinet. See Records Management Tip # 7 for information on file charge-out systems.

Notify the Records Management section, Public Works and Services, of any access restrictions on records that are in storage in the Records Centre. Files will only be retrieved for those users who are authorized to see them.