



# Records Management Tip

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

No. 10 – December 2003

**Active Filing Series**

## Information Security – Part 1

Information security is an issue in most offices. Recent news headlines about identity theft, stolen computer servers, and computer viruses have shown how important it is to protect information.

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

Theft is only one of many concerns. Every office has information that should not be open to everyone who walks through the door. Personal information, confidential information about government programs, and information that is not ready to be released to the public should be protected. Poor security can have an impact in many areas, such as:

- Planning.
- Budgets and finance.
- Personal privacy.
- Program delivery.
- Public safety.

It could also damage the government's dealings with the public, other governments, and the private sector.

### Information Security Procedures

Departments need security procedures for information in all formats: paper, electronic, and other media. Often the different types of information are looked after separately. This can lead to gaps in the security infrastructure.

Records coordinators, information systems managers, and the building maintenance officers or property managers should all take part in writing security procedures. The procedures should be looked at every few years to make sure that they are up to date.

The procedures should address a number of areas:

- Responsibilities.
- Access restrictions and security classifications.
- Access to facilities.
- Access to storage areas and storage equipment.
- Access to computer networks and computer equipment

---

Public Works and Services' Systems and Communications Division (SCD) and the Technology Service Centre (TSC) look after network and computer security for the government. Departmental procedures should support the government-wide policies.

### **Responsibilities**

All employees have a role to play in protecting government information.

- **Managers and Directors** should make sure that the information that belongs to their program areas is protected and handled properly. They are also responsible for making sure that procedures for handling information are being followed.
- **Employees** are responsible for following procedures for protecting and handling information.

### **Access Restrictions**

There are a number of different types of access restrictions, which departments should address:

- As a rule, employees are only given access to the information that directly relates to their job.
- Human resources information is usually restricted to human resources officers and the individual employee. Supervisors may see parts of the personnel file.
- Access to FMBS decisions, Cabinet decisions, and legal opinions is restricted.

The government is developing information security classification levels. These should be incorporated into the department's information security plan.

The SCD and the TSC have looked after access to computer networks as part of their network security plans.