



# Records Management Tip

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

No. 11 – January 2004

**Active Filing Series**

## Information Security – Part 2

### Access to Facilities

Departments cannot protect their information if they do not have control over who can enter their office space, warehouses, and yards. There are a number of things that departments can do protect their facilities:

- Control the distribution of keys and access codes.
- Use different keys for different areas of the building. If you are using keypad locks, use different codes for each access point.
- Escort non-employees when they are in office areas.

### Access to Equipment

It is not enough to control access to buildings. Departments should also control access to computers and storage equipment.

- Lock equipment when it is not in use. Make sure that only authorized employees have access to the key. You may want to keep equipment that contains highly confidential records locked at all times.
- Keep your equipment in secure areas.
- Consider using locks, braces, or cables to secure equipment in place.
- Make sure that all equipment is listed on up-to-date asset inventories.
- Write sign-out procedures for equipment that employees are allowed to take from the office. The procedures should cover how long employees can have the equipment.

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

---

## Access to Information and Records

Finally, to protect your information, you need to control access to the information itself.

### Paper Records

- Implement and enforce sign-out procedures for files.
- Start a “clean desk” policy for office staff.
- Limit access to records stored in secure areas.
- Put confidential transitory records into secure recycling bins. You may have to shred transitory records on site if your community does not have a recycling service. Do not send intact confidential records to the local landfill.

### Electronic Records

- Encrypt sensitive and confidential files. Make sure that the people who need access to the files can open the files.
- Use the password feature on computer screensavers to keep others from using your computer when you are away from your desk. With some operating systems, you can also press Ctrl+Alt+Del to lock your computer.
- Use the network drives to save electronic documents. The C: drive can be accessed by anyone who has access to your computer. Network drives are regularly backed up.
- Make sure that the security on network directories is appropriate for the records stored on the network. For example, only the human resources staff should be able to see the human resources records stored on the network.
- Store electronic media (e.g. tapes, diskettes, compact disks) in a dust-free area with steady temperatures and humidity.
- Mutilate tapes, diskettes, compact disks, and hard drives when they are thrown away.

### All Records

- Set up procedures to make sure that all original documents (paper and electronic) are sent for filing.
- Make sure that access lists for records are kept up-to-date. Send a copy of the access lists for semi-active records to the Records Centre.
- Records are government assets. Terminating employees should return all of the records that are in their custody, including electronic records and e-mail messages, to their supervisor. Employees should only remove copies of records with permission from their supervisor.