



## Newsletter Autumn 2008

### Last month, I was asked about regulation thickness for the shredding of documents.

To make a long story short, while there used to be size requirements for the destruction of information, this is no longer the case. Has the law become more lax? No, the advent of computers has simply led to a change in regulations. Any person who operates a business must take proper security measures to protect personal information that is collected, used, communicated, preserved or destroyed, provided the measures are reasonable in view of, among other things, the information's sensitivity, intended use, quantity, distribution and format.

You are therefore required to ensure the confidentiality of documents in paper, digital, or any other information storage format.

### What's New?

Did you know that Recyshred now offers safe document storage? It's a cheaper -- and safer -- alternative to an office storeroom or rented public warehouse. We will also inform you of the proper time to destroy your documents (thus saving you money, since we can destroy them on site).

### Privacy

**Train your Employees:** Ensure your employees understand your policies on privacy, and the correct way to obtain personal information from clients. Post the following rules in the form of a checklist for all employees:

- Use alphanumeric passwords when opening a session, and change them regularly. How do I create a password that's safe and easy to remember? One way is to use the first letter of each word from a simple phrase (i.e. for "I like my 32-year-old neighbor Carol", the password would be **ilm32yoce**). This gives you an alphanumeric combination with a maximum security level.
- Never ask a client to provide personal information in the presence of a third party, and ensure the client can enter his/her PIN in full privacy and confidentiality.
- Compare signatures, and confirm that the client is the person he or she claims to be.
- If you notice that terminals or databases have been altered, report it to management.
- Store client information in a secure place.
- Shred paper waste that contains confidential data, including information on payment cards and photocopies of ID cards.
- Do not leave anything on your desk overnight.
- Enter databases only with proper authorization.
- Ensure computer systems are locked and secure when not in use.

