

SHARP® Security

Sharp answers to your “Personal Information Protection and Electronic Documents Act (PIPED Act)” questions.

In today’s high tech society, steps must be taken to ensure that information we once assumed would be kept private – stays private. Federal and Provincial Government’s have rolled out legislation to try to keep pace with societies’ need for protection. The PIPED Act is one of the first acts to apply to both public and private institutions. Several other pieces of legislation protect Canadians including specific acts concerning government, education, health care and finance.

Sharp has the experience and technology to help both private and public enterprises protect the confidential information they have been entrusted with. The key security issues highlighted by several acts are: Physical Safeguards, Technical Safeguards, Administrative Safeguards, Restricted Access and Disposal of Records. Legislation also covers the unnecessary collection and retention of private information and electronic documents. Sharp has developed a number of security features for its commercial office equipment that will help organizations resolve their security concerns and meet the required government privacy standards.

Technology Issue: All modern Photocopiers (Multi-function Products) contain memory chips that store images of every document that passes through the device. A copy of every copied/printed/faxed/scanned document is stored inside the machine. These page images are retained in the devices’ memory until the memory is full. The oldest images are then simply overwritten. This storage/collection issue is compounded when the Multi-function Product (MFP) contains a Hard Drive. Hard drives are capable of storing tens of thousands of pages. It is said that data is recoverable from computer hard drives unless the information is overwritten up to seven times. MFP Ram and Hard Drive memory have the same recoverability. Depending on the size of memory and number of processed documents, private information could be sitting unprotected in the print device for days, weeks or even years. This standard technological feature causes the unnecessary collection and retention of private information and a potentially huge data security risk.

To illustrate: A copier with a 40 GB hard drive can store approximately sixty thousand pages of information that is recoverable after it is overwritten up to seven times. The total number of un-intentionally stored/collected images would be approximately 420,000 pages. The RAM memory would add another few thousand pages.

A serious security risk exists to the information stored and collected inside of these MFP devices. This private information is subject to both accidental and intentional removal/retrieval. The potential risk becomes even more frightening when the product is retired from service. The information stored inside the machine will travel with it to its next destination. Products are often traded-in, re-sold, re-cycled.

The Sharp security option will ensure all copy, print, scan and fax information is safeguarded by first encrypting it then erasing it. Using new encryption technology, the new generation of Sharp machines can support key sizes of as much as 256 bits, double the standard used for e-commerce. After encrypting the information stored in RAM and on the Hard Drive the Sharp Security Kit “sanitizes” the data by overwriting it up to seven times. This security option is recognized by the printing security authorizing body ICCC. (International Common Criteria Consortium, or Common Criteria – www.commoncriteria.org). The kit is the first software solution of its kind to carry the Common Criteria Validation certificate, also known as ISO standard 15408, an emerging global standard for information technology security evaluations.

Built-in capabilities like "Confidential Printing" and our standard "Audit/Account controls" take your document security policies to the next level. Network scanning security is supported through network “User Authentication.” Network access to the device can also be restricted with our “IP/Mac Address Filtering” control. Confidential Faxing is now easier with a new industry standard "F-Code" ability.

Protect the personal, private or confidential information you have been entrusted with and meet regulatory requirements like the HIA and PIPED Act in Canada and the HIPAA and GLB Act in the USA. Do you know where your documents are? Be Sharp.