Sensitive Information Protection Standard - DRAFT

Queen's Electronic Information Security Policy Framework
Security Standard: Sensitive Information Protection
This standard guides those responsible for managing computers, storage devices, networks, and other IT Resources which are used to store, provide access to, transmit, or otherwise are associated with the use of personal, confidential, or operationally sensitive information, as defined by the Queen's University Data Classification Standard. The requirement to protect Sensitive Information is established under the responsibilities within the Queen's University Electronic Information Security Policy, and the Queen's University Network and Systems Security Policy.

A) Encryption

1. Sensitive Information stored on workstations and servers must be encrypted in a manner that is consistent with Queen's University Electronic Information Security Policy and associated guidelines and standards.
2. When transmitted over non-secure networks, Sensitive Information must be encrypted.
3. Sensitive Information stored on portable devices such as cellular phones, PDAs, cameras, and storage devices such as portable hard drives, USB memory sticks or keys, must be encrypted in a manner that is consistent with Queen's IT standards and recommended practices.

B) Storage Location

1. Wherever possible, Sensitive Information should be stored on appropriately protected servers, and not on less secure workstations.

C) Secure Disposal and Data Removal

1. Any computing or storage device on which there may be Sensitive Information must be disposed of in a secure manner, whether being discarded, sold, or donated to some other party. This applies to all of the following types of devices:

- Computer internal hard drives, portable hard drives, USB memory drives/keys;
- Cell phones, PDAs, and cameras.
- Any other device which has the capability to store data.

D) Printers, Photocopiers and Other Multi-function document devices

1. Printers, scanners, photocopiers and facsimile devices which have internal storage capability (e.g. hard drives), must be installed, configured, and disposed of in accordance with the Multi-Function Device Security Guidelines.

E. Media Handling

1. All media, such as CD-ROM, DVD, tape, etc. that are used to store or transport personal, confidential or operationally sensitive information should be protected in accordance with the most sensitive information stored on the media, and be appropriately labelled as such.

F. Exchange of Information With External Parties

1. When exchanging sensitive information with external agencies or parties, the information needs to be appropriately protected while in transit or transfer.
2. An information sharing agreement, establishing the need for confidentiality and due diligence to protect the information, must be signed by the external party.