- Remove all diskettes and hard drives used to process sensitive information and store in a security approved container

- All diskettes and hard drives used for processing of sensitive information must be clearly marked at the highest level of sensitivity contained on the medium, and only used on the secure system

- SIGNET-C4 **CANNOT** process **TOP SECRET** information or material. This material must be created on a stand alone tempest computer and transmitted by using a Secure Fax to a security cleared individual

Laptop Computers

In exceptional circumstances, where the processing of sensitive information (up to **SECRET**) cannot be done at the mission, the use of a laptop may be permitted by your Director or Director General. The following precautions must be taken:

- When used, the laptop must not be connected to a power outlet (i.e. battery operated) to reduce the level of electromagnetic emanations

- The laptop and related storage media containing classified information must not be left unattended unless stored in a security approved container within the mission

- The laptop modem must not be used, even for the exchange of unclassified information

- Upon return to Canada, or even before if possible, the hard drive of the laptop must be sanitized to ensure all classified information has been erased and overwritten (see ISCA for sanitization procedures)

- The carrier of the laptop must carry a diplomatic courier certificate and must never consign the laptop and related storage media to the cargo hold

Standalone Computers

You may process sensitive information on a standalone tempest computer provided it is fitted with a removable hard drive. Printing of this material must be done using any SIGNET-C printer or a local tempest printer.