Disposal and/or Reuse of Diskettes and Equipment

If diskettes, hard drives and dedicated laptops contain Protected B to Secret information, send them to SPAS marked "for destruction". If diskettes, hard drives or laptops are to be reused in the same environment (for processing Protected B to Secret), contact SXTC for sanitization.

If diskettes or hard drives contain unclassified or Protected A information, contact SIGNET Support to have the media securely deleted before reuse or disposal.

Safeguard Your System from Viruses

DFAIT's anti-virus software products automatically strip executable attachments on e-mails to and from correspondents external to the Department. Thus, if you receive or send a message containing a stripped e-mail attachment, you will receive a message from the Antigen anti-virus software saying the attachment was removed.

If you certify that the file is essential to the business of the Department and respects acceptable use policies, you may arrange for its delivery by forwarding the automated e-mail to -EXTOTT - SXIM – OPS, providing the required certifications.

Guidelines

- Make sure you scan for viruses.
- Always use the anti-virus software installed on the network to scan each diskette coming from another workstation before you use it.
- If you get a message reporting a virus on your machine, contact SIGNET support or your System Administrator. Do not shut down your system or try to remove the virus yourself.

If you suspect or detect a virus, immediately contact your System Administrator.

Use of DFAIT Networks

The policy governing the use of DFAIT electronic networks applies to employees (federal, contractors, etc.) who have authorized access to the Department's electronic networks or to the INTERNET through use of the Department's computers, network connectivity or stand-alone workstations via modems. For more information please use the following link:
http://intranet.lbp/department/sxd/policy/policy-e.asp