SECURITY OF INFORMATION TECHNOLOGY (IT)

IT Security ensures thc safeguarding of departmental systems, assets, information, and services against deliberate and accidental threats to:

- Confidentiality of information;
- Integrity of processes and data; and,
- Availability to data, systems and services

IT security includes the hardware, softwarc, networks, telecommunications and other equipment that is interconnected, as well as the facilities in which the equipment is housed.

IT also includes all the data and information you create while carrying out your job function; your official reports, memos, e-mail messages, etc., are government records and belong to the Crown.

Why IT Security is Necessary

As DFAIT employees, there are a number of threats to IT security against which we must safeguard ourselves.

- *Deliberate* threats which include: unauthorized access to departmental data, electronic eavesdropping, non-compliance with DFAIT practices, and viruses.
- *Accidental* actions or events which include: user errors, lack of user knowledge, breakdown of computer hardwarc.

Departmcntal Networks

The systems we use to process information comprise the following departmental networks:

- SIGNET 3 (formerly known as SIGNET-D); and
- SIGNET C4.

SIGNET 3

The main departmental network used for processing unclassified and Protected A information at headquarters and missions is SIGNET 2000+/SIGNET 3. This system is accessible to all employees including locally-engaged staff abroad. It is also available to a few other government departments, organizations and some foreign governments. In the majority of missions, the SIGNET 2000+ system is administered by a locally-engaged system administrator.

Note: Personnel must have, at minimum, a Reliability Status (RS) before obtaining access to SIGNET 2000+/SIGNET 3.