



## TELEWORK

### Introduction

The Government of Canada (GC) defines Telework as a flexible work arrangement whereby GC employees have approval to carry out some or all of their work duties from alternative locations.

Telework generally takes place at one designated alternative location, usually the employee's home. Telework often includes computer network access to GC networks to access GC information and applications.

In addition to telework, the GC recognizes that traveling employees sometimes need remote access to GC networks from locations such as hotels, airports, and external workplaces to discharge their work responsibilities.

### Policy on Telework

The Treasury Board of Canada Secretariat (TBS) publishes the GC's *Telework Policy* which includes the following:

- GC departments should ensure that teleworkers understand the security risks common to teleworking and how to minimize those risks,
- GC departments should permit the employee to use their own personal computing equipment, and
- The *Telework Policy* recommends use of GC devices to ensure a consistent deployment of security measures.

### Telework connectivity types

PCs, laptops or Palmtops are the most common tools for telework. These devices connect to the GC Networks by various means including:

- Cellular Connectivity,
- High Speed Internet Connectivity,
- Dial-Up Internet Connectivity, and
- Wireless Network Connectivity.

### Telework locations

Telework is usually identified as "working from home" however other qualifying locations are:

- Hotel rooms,
- Internet cafés,
- Airports, and
- Other GC locations.

### Threats

Typical security threats jeopardizing the confidentiality, integrity and availability of the data on the device at telework locations are:

- Physical access to remote device -
  - Malicious Code,
  - Social Engineering,
- Theft, and
- Loss.

### Basics Safeguards

Various techniques used to provide security protection include:

- Physical security such as locks and cable restraints,
- BIOS protection,
- Operating System (OS) Safeguards -
  - Strong Passwords,
  - Use of non-Administrator Accounts,
  - Locking current session,
- Encryption of stored data,
- Host Intrusion Detection System (HIDS),
- Content Filtering Software,
- Security Maintenance and Monitoring,
- Communications Security -
  - Strong Identification and Authentication,
  - Virtual Private Network Encryption,
  - Firewalls,
  - Network Intrusion Prevention System, and
  - Network Access control.