May, 2010
Updated December, 2011

Working Outside the Workplace
Home Technology Assessment

Office of the Chief Information Officer

Ministry of Technology, Innovation and
Citizens' Services
Province of British Columbia

Home Technology Assessment

Introduction:

If you have been approved to use your home computer for government work you are required to ensure that you have adequately protected your computer. **It is only in exceptional circumstances that a home PC can be used to work on government electronic records containing sensitive information.**

The following is a self-assessment guide for describing the readiness of the home technology environment for employees approved to work on government electronic records containing sensitive information (including personal information)**.**

This assessment is a requirement as described in the Government Chief Information Officer's policy entitled *Working Outside the Workplace* (WOW). The policy provides for best practices and is offered as a guide for employees when working with personal and/or confidential information outside the workplace and using: 1) a government computer (laptop/tablet); 2) DTS and Remote Desktop Connections with VPN; and 3) Outlook Web Access (Summer) and government-issued encrypted USB flash drives.

Instructions for Employees:

Please complete the following assessment. You need to provide a copy for discussion with your supervisor. You can either save and then email the completed form or print a hardcopy. Your supervisor is not approving the security measures for your home computer. Your supervisor's role is to review the completed assessment for working on confidential and/or personal information outside the workplace; the supervisor may decline to allow the information to be worked on outside of the workplace if reasonable security is not in place to protect the information.

Employees are responsible for ensuring that confidential and/or personal information is appropriately safeguarded. For the installation of the appropriate measures, see the tips available on securing a home computer available at the Office of the Chief Information Officer website, which will help in setting up home protection such as firewalls, virus scans, encryption, etc. Also, refer to the *Working Outside the Workplace* policy for more information.

Instructions for Supervisors:

Supervisors must review the completed Home Technology Assessment and approve any working outside the workplace arrangements with staff, prior to an employee working at an alternative site.

It is important for supervisors to discuss organizational expectations for the safeguarding and protection of confidential and/or personal information with employees. Refer to the *Working Outside the Workplace* policy for more information.

Only in extenuating circumstances may a home computer be used for working on GOVERNMENT'S confidential and/or personal information. The home computer must be compliant with the Home Technology Assessment, and if in extenuating circumstances (e.g., disaster recovery) there is a need to store confidential and/or personal information the storage location on the home computer MUST be encrypted. See the *Working Outside the Workplace* policy and section 15, 16 and 17 of this assessment for more information.

We recommend supervisors consult their Ministry Information Security Officer for their assessment of any potential risks identified on the completed form.

Information Links:

Tip Guide: How to Protect Your Home Computer
http://www.cio.gov.bc.ca/local/cio/working_outside_workplace/tip_sheet.pdf

Working Outside the Workplace
http://www.cio.gov.bc.ca/cio/working_outside_workplace/index.page

Office of the Chief Information Officer website
http://www.cio.gov.bc.ca

Ministry Information Security Officer Role
http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISORole.page

Ministry Information Security Officer List
http://www.cio.gov.bc.ca/cio/informationsecurity/MISO/MISO.page

Security 101 Guidebook -The Basics of Information Security in the Government of British Columbia
http://www.cio.gov.bc.ca/local/cio/informationsecurity/pdf/BasicsInfoSecurityGuidebook.pdf

Home Technology Assessment

Employee Name:	**Date Completed**:
Ministry and Division:	**Supervisor's Name:**
Phone Number(s): e.g. 000 000-0000 **Home:** **Work:**	**Supervisor's Phone Number:** e.g. 000 000-0000 **Work:**
Employee's Email:	**Supervisor's Email:**

Part 1: At-Home Assessment

	Yes	No	Don't know
Government-Approved Computer			
1. Will you be using a government issued computer to work on government's confidential and/or personal information outside the workplace?	○	○	○

If YES, go directly to Part 2. If NO or DON'T KNOW, go to Question 2.

Rationale/Comment: Government-approved computers are pre-configured to protect confidential and/or personal information whenever in use.

Comment:

Home Computer

Other Users

	Yes	No	Don't know
2a. Is there more than one user of the home computer?	○	○	○

Rationale/Comment: Separate user account profiles/ passwords that are not known to other home computer users help protect confidential information from unauthorized disclosure. For more detailed information on this

please see section 4 of the "Tip Guide: How to protect your Home Computer" document.

Comments:

2b. If yes, is there a separate user profile and access password set up for your work-related activities only?	○	○	○

Rationale/Comment: Separate user account profiles/ passwords that are not known to other home computer users help protect confidential information from unauthorized disclosure. For more detailed information on this please see section 4 of the "Tip Guide: How to protect your Home Computer" document.

Comments:

3. Is the screen saver set to time out after no more than 15 minutes of inactivity?	○	○	○

For more detailed information on this, please see section 4 of the "Tip Guide: How to protect your Home Computer" document.

Comments:

4. Does the screen saver require a password for re-activation?	○	○	○

Rationale/Comment: Screen saver timeouts and passwords are basic protections for confidential information. For more detailed information on this, please see section 4 of the "Tip Guide: How to protect your Home Computer" document.

Comments:

Operating System

	Yes	No	Don't know
5. Is the Operating System (OS) up-to-date with security patches and service packs?	○	○	○

Rationale/Comment: It is essential that up-to-date security patches be applied as new security vulnerabilities are continually being discovered. For information on how to check the status of the security patches and if the OS automatic update is enabled, please see section 8 of the "Tip Guide: How to Protect Your Home Computer" document.

Comments:

Virus Scanner

	Yes	No	Don't know
6. Is there active anti-virus software installed on the computer?	○	○	○

Rationale/Comment: Anti-virus software with up-to-date information on computer viruses must be installed and be actively scanning for viruses.

NOTE: If there is no anti-virus software installed and firewall in use, remote connectivity from the computer system to ANY Government resources must not be attempted. This is a mandatory requirement for passing the Home Technology Assessment evaluation.

Comments:

7. Is the anti-virus software configured to receive updates regularly?	○	○	○

Rationale/Comment: Since virus threats evolve over time, anti-virus updates are provided on a regular basis in order to provide adequate protection for the home computer. For more detailed information on this, please see sections 6 and 12 of the "Tip Guide: How to Protect Your Home Computer" document.

Comments:

8. Is a full computer virus scan set to run on a weekly basis?	○	○	○

Rationale/Comment: Regular virus scans provide better protection for the home computer. Ensure that the antivirus software is configured to scan the entire computer for viruses on a weekly basis (or more frequently).

Comments:

Personal Firewall

	Yes	No	Don't know
9. Is there a software-based and/or a hardware firewall in use?	○	○	○

Rationale/Comment: A firewall is a security measure that provides the computer additional safety and protection from intruders, hackers and malicious code from the internet. For information on how to check the status of the firewall and for additional information, please see section 7 of the "Tip Guide: How to Protect Your Home Computer" document.
NOTE: If there is no anti-virus software installed and firewall in use, remote connectivity from the computer system to ANY Government resources must not be attempted. This is a mandatory requirement for passing the Home Technology Assessment evaluation.

Comments:

Internet Browser

	Yes	No	Don't know
10. Does the Internet browser have up-to-date security patches?	○	○	○

Rationale/Comment: There are several browser products available for use. It is essential that up-to-date security patches are applied as new security vulnerabilities are continually being discovered. For information on how to check the status of browser patching and how to enable browser patch updates please see section 8 of the "Tip Guide: How to Protect Your Home Computer" document.

Comments:

Application Software

	Yes	No	Don't know
11. Are you using locally installed, stand alone office productivity applications to work on confidential and/or personal government information?	○	○	○

Rationale/Comment: Government standard Microsoft Office is available for home use for a nominal fee ($11). The use of web-based services/products (such as Google Docs) must not be used to store/record government information.

Comments:

12. Are the applications kept up-to-date with security patches?	○	○	○

Rationale/Comment: It is essential that up-to-date security patches be applied, as new security vulnerabilities are continually being discovered.

Comments:

Secure Storage

	Yes	No	Don't know
13. Is there a secure storage area (e.g., drawer, box, room) to protect devices and/or paper containing government's confidential and/or personal information?	○	○	○

Rationale/Comment: Electronic devices and confidential papers should be secured when not in use, to protect them from unauthorized disclosure.

Comments:

14. Is government's confidential and/or personal information being stored on an encrypted device (e.g., government issued USB flash drive) when using the home computer?	○	○	○

Rationale/Comment: Confidential and/or personal government information must not be stored on a home computer unless extenuating circumstances arise or exist. Even if a home computer is secured, the preferred storage method is firstly a government issued encrypted USB flash drive.

Comments:

15. If an extenuating circumstance arises or exists and it becomes necessary to store government's confidential and/or personal information on the hard drive of a home computer, is it stored in a separate encrypted folder or in a virtual encrypted disk which have been set up for work information?	○	○	○

Rationale/Comment: If for some reason it becomes necessary to store government's confidential and/or

personal information on the home computer, it must be protected from unauthorized disclosure by isolating it from other home computer users. For more detailed information please see section 9 of the "Tip Guide: How to Protect Your Home Computer" document.

Comments:

16. Are you the only person able to access the encrypted folder or the encrypted virtual disk?	○	○	○

Rationale/Comment: Access to government's confidential and/or personal information stored on the home computer must be isolated from other users in the home. For more detailed information please see section 9 of the "Tip Guide: How to Protect Your Home Computer" document.

Comments:

Secure File Deletion

	Yes	No	Don't know
17. Are you using specialized file deletion software or a built-in utility in the operating system to delete government work files in the event you had to access files containing government's personal and/or confidential information on your home computer?	○	○	○

Rationale/Comment: There are a variety of commercial general security and dedicated file deletion products available for use. There is also the built-in "Cipher" utility that is available as part of the Operating System on Windows 2000, XP, Vista and Windows 7. For more detailed information, please see section 5 of the "Tip Guide: How to Protect Your Home Computer" document. Also see the Working Outside the Workplace policy regarding the use of home computers.

Comments:

Part 2: Additional Requirements - *All respondents must complete Part 2.*

Disposal of Confidential Information and Devices

18. Are paper copies of confidential and/or personal government information disposed of securely and according to government standards?	○	○	○

Rationale/Comment: Return paper copies of confidential government information to the workplace and dispose as required by policy. Do not dispose of government's confidential and/or personal information through home recycling or garbage pickup. Records Management has file retention requirements regarding management of government records. The Disposal Handbook specifies how devices and storage media (e.g., paper, CD, DVD, tape) can be securely disposed of, available at: http://pss.gov.bc.ca/psb/pdfs/disposal_handbook.pdf.

Comments:

19. Are electronic devices containing confidential and/or personal government information disposed of securely? This includes obsolete or inoperative equipment.	○	○	○

Rationale/Comment: Government electronic storage devices are destroyed before they are disposed of. Personal storage devices that have been used to store government's confidential and/or personal information should not be discarded or donated without first securely deleting work files and information using

a specialized file deletion software or utility. The Disposal Handbook specifies how devices and storage media (e.g., paper, CD, DVD, tape) can be securely disposed of. This handbook is available at: http://pss.gov.bc.ca/psb/pdfs/disposal_handbook.pdf.

Comments:

Home (Wireless) Network			
	Yes	**No**	**Don't know**
20. If a home wireless network is in use, was the default password used to access and configure the wireless router/firewall changed?	○	○	○
Comments:			
21. Is WPA2 encryption being used for the wireless connection?	○	○	○
Rationale/Comment: Wireless routers/firewall devices have default passwords published on the Internet which would allow anyone to reconfigure the device without your knowledge."WPA2-Personal" encryption should be used and is strongly recommended. "WPA-Personal" is acceptable as well. "WEP" encryption must not be used. The option of "No encryption" must never be used. For more detailed information and specific instructions on configuring wireless network security, please see section 10 of the "Tip Guide: How to Protect Your Home Computer" document.			
Comments:			

Secure Transport of Confidential Information			
	Yes	**No**	**Don't know**
22. Will a government-issued device be used to transport confidential government information (for example, a USB flash drive, tablet or laptop)?	○	○	○
Rationale/Comment: Government-issued devices are pre-configured for the safe handling and transport of government's confidential information according to government standards. Unencrypted/unsecured personally owned computer equipment is the least preferred option for the transportation of confidential and/or personal government information.			
Comments:			

Security Control Criteria:

Remote Access:

When remotely accessing government information (e.g. using Summer (Web Outlook Mail), VPN, DTS) from a non-government computer, it is recommended that up-to-date firewall and anti-virus programs are installed and actively operating.

Remote Access - Confidential and/or Personal Information:

When remotely accessing government personal/confidential information (e.g. using Summer (Web Outlook

Mail), VPN, DTS) from a non-government computer, up-to-date firewall and anti-virus programs **must** be installed and actively operating. Access to government's personal/confidential information **must not** be attempted, unless it can be protected by verifying that the firewall and anti-virus programs are actively operating. Please refer to the WOW policy for more information.