BRITISH COLUMBIA | Ministry of Health

NETWORK USAGE REQUEST AND AGREEMENT FOR NON-GOVERNMENT DEVICE

OFFICE USE ONLY

MOH SECURITY CONTACT	PHONE #	AGREEMENT #
		Y Y Y Y- # # # #

DEVICE INFORMATION

NETWORK IDENTIFICATION		
Network Identification is the full computer name found by clicking on the "System" icon within Window's "Control Panel." Then click on the "Computer Name" tab to see the "Full computer name" displayed.		
DEVICE TYPE (E.G. LAPTOP, ETC.)	GOV'T EMAIL ACCESS REQUIRED? ☐ YES ☐ NO	INSTALLED ANTI-VIRUS SOFTWARE (E.G. NORTON, SYMANTEC)
LAST UPDATE OF ANTI-VIRUS DEFINITION FILE Y Y Y Y / M M / D D	LAST FULL ANTI-VIRUS SCAN ON DEVICE Y Y Y Y / M M / D D	REAL TIME VIRUS SCANNING OF ALL FILES CURRENTLY ENABLED? ☐ YES ☐ NO
METHOD FOR RECEIVING NEW VIRUS SIGNATURES AS THEY ARE AVAILABLE (E.G. MANUAL PROCESS, AUTOMATED BY SOFTWARE, ETC.)		
MAC ADDRESS *At DOS prompt type:* *ipconfig/all and note Physical Address*		

INCLUDE PHOTOCOPIES OR SCREEN IMAGES OF DEVICE SOFTWARE LICENSES

MINISTRY CONTACT

If the device owner is a contracted resource, please keep the original copy of this form in the contract file and send a copy to Information Security and Audit, Health Sector IM/IT Division, Ministry of Health.

NAME OF DEVICE OWNER	COMPANY OR ORGANIZATION NAME	
BUSINESS PHONE OF DEVICE OWNER	START DATE FOR NETWORK ACCESS Y Y Y Y / M M / D D	END DATE FOR NETWORK ACCESS Y Y Y Y / M M / D D
FLOOR NUMBER AND SITE ADDRESS OF OFFICE WHERE THE DEVICE WILL BE CONNECTED ☐		ROOM # OR LOCATION WITHIN OFFICE

In order to ensure the security of the leased Government (SPAN) data network/resources, and to avoid significant costs resulting from breaches in security, all individuals connecting non-government managed devices to the government network are required to submit this agreement via fax or mail, to:

Mail: Ministry of Health Helpdesk **Fax: 250 952-2401**
System Services | Health Sector IM/IT Division
1-1, 1515 Blanshard Street
Victoria BC V8W 3C8

GOVERNMENT NETWORK USAGE AGREEMENT

This agreement must be approved by the Information Security and Audit Branch (ISA), Health Sector IM/IT Division, Ministry of Health, before any network connections are made. **Individuals signing this agreement must read, understand, and comply with all of the following terms. Failure to do so will remove your right to use the government network.**

User agrees that they are responsible for the following:

1. Ensure that the information supplied in the Device Information section of the Network Usage Request form (above), regarding the device to be connected to the government network, is accurate at the time of completion;
2. Ensure that any changes to the Network Usage Request form (above) are reported to ISA, email ID: HLTHInfoSec@gov.bc.ca;
3. Report all security related issues to the ISA, email ID: HLTHInfoSec@gov.bc.ca and the contract manager immediately;
4. Understand that it is forbidden to test the security features of the SPAN network/resources without written permission from ISA. Without such permission, your actions will be viewed as hostile and an investigation will be initiated;
5. Use only government authorized e-mail when connected to the SPAN network. All other e-mail products are prohibited;
6. Ensure that the device has an identifiable Computer Name (e.g. including IDIR name);
7. Not connect any additional unapproved hardware devices to the network (e.g., printers, hubs, switches, wireless routers, etc.);

PRINT RESET

8. Ensure that confidential or sensitive ministry data (e.g. data that contains individuals' personally identifiable information) is **not** stored on the device. Where there is a business justification to store government information on the device, it must be formally approved by the respective government program Executive Director and the Ministry Information Security Officer; and
9. When connection to the network is no longer required, ensure the following:
   - That ***all*** acquired government data, files, and documents that have resided on the device ***are securely erased*** (multiple erasures);
   - That ***all*** acquired government software, hardware, documentation, storage media and licenses that were used in conjunction with the non-government device ***have been returned fully and completely to the ministry***; and
   - Complete and submit the Network Usage Termination of Non-Government Device form (HLTH 4619).

Devices attached to the government network must have the following configuration:

- All applications and services running on the device being connected to the government network must utilize strong authentication methods (including userid and password combinations; device locking and session time-out mechanisms; see Glossary below for definitions of authentication and other terms);
- All products installed on your device must (a) be authorized, (b) be licensed software and (c) have all vendor security patches installed;
- Anti-virus software must be installed and anti-virus real-time scanning of **all files** must be enabled when connected to the government network;
- Up-to-date anti-virus signature files must be installed and maintained and all device-resident files must be virus-scanned at least weekly or more frequently as required;
- Have wireless networking disabled; and
- The primary source of any government document must be stored on the ministry LAN, not on the device or any removable media.

Additionally, I agree that the ministry:

- Has the authority to audit devices without prior notice to ensure compliance with the terms of this agreement;
- Has the authority to seize devices if required for security investigations; and
- Will not be liable for accidental damage to these devices that may occur during its operation or during a security investigation.

I, _____ have read the Government Network Usage Agreement. I understand its
Device Owner (print name)
contents and agree to comply with its provisions.

_____ _____
Device Owner (signature) *Date*

_____ _____ _____
Authorizing Program Executive Director (signature) *Authorizing Program Executive Director (print name)* *Date*

_____ _____ _____
Authorizing Ministry Information Security Officer (signature) *Authorizing Ministry Information Security Officer (print name)* *Date*

GLOSSARY

Authentication	The verification of the identity of a person or process.
Device	Components that can be attached to networks, including laptops, personal digital assistants (PDAs), servers, etc.
Strong authentication	Describes the level of security safeguards that are used in authentication processes. For example, "strong passwords" refer to using passwords that are composed of letters, numbers and special symbols in such a manner as to preclude guessing. "Strong authentication methods" involves the use of two or more authentication techniques to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: Secret - something the person knows. Something that the individual knows, has, is, and can do.

Requirements for Non-Government Devices used on the Government Network

To ensure that the performance and integrity of the government network is not jeopardized, all non-government devices that are connected to the network must use a variety of safeguards, such as personal firewalls and antivirus software.

What Software Can Be Used?

Permissible software on non-government devices that are connected to the government network includes:

- Government-approved sofware (e.g. Microsoft Office, Adobe products or other licensed software such as Word Perfect);
- Operating system software;
- Anti-virus software;
- Access controls (e.g., logon to device using a password);
- Encryption (that provides minimum 256 bit or stronger encryption);
- Secure network connections (including Virtual Private Networks);
- Vendor patches and upgrades (including anti-virus signature files); and
- Vendor supplied security safeguards (including personal firewalls, intrusion detection software, and locking screen-savers).

If you have questions regarding the suitability of the software you intend to use, please discuss your requirements with the Ministry Information Security Officer.

Using physical locking safeguards, such as cable locks to secure laptops to desks, also provide further safeguards to the device when it is connected to the network. For further information on the required procedures, please review the Connecting Non-Government Devices to Government Networks Procedures.

What Software Can't Be Used?

By definition, non-government devices may contain software that is not part of the government's standard software configuration. As a result, when the non-government device is attached to the network, this non-standard software may unintentionally jeopardize the integrity and subsequent performance of the government network.

Thus, to be sure that the non-standard software does not expose the network to increased risks, non-government devices should remove the non-standard software prior to the device being used on the network, rather than leaving it on the device (as the software may have automatic logon features when it is connected to a network environment).

The following software categories illustrate the types of software that pose significant risk to the government network:

- Peer-to-peer software (e.g., BitTorrent, eDonkey, Limewire, Morpheus, Shareaza);
- File transfer software (e.g., that uses the File Transfer Protocol or FTP, such as Filezilla, SmartFTP);
- Messaging software including Instant Messaging software (e.g., Google Talk, ICQ, I2Planet, Lan Messenger, MSN Messenger, Skype);
- News group readers (e.g., Usenet readers, including Really Simple Syndication or RSS Readers, such as Rocket RSS Reader); and
- Network testing or traffic software (e.g., network traffic sniffers or eavesdropping type software, including AirSnort, MSN Sniffer).