BRITISH COLUMBIA | Ministry of Social Development and Social Innovation

NON-GOVERNMENT DEVICE ACCESS AGREEMENT (NDAA)

This Agreement applies to the connection of a *non-government device* (3) (8) to the BC Government's network from within a ministry office for business purposes. Under no circumstance will the Province be liable to any person for any harm, loss or damage resulting from connecting a non-Government device to the Government network.

In order to safeguard the Government's information and network resources, and to avoid significant harm resulting from a breach in security, *Agreement Managers* (1) must ensure that individuals have implemented appropriate security controls and submitted this completed Agreement **prior** to connecting their non-government device to the network. In addition, all individuals must be made aware of and comply with:

- The Appropriate usage of Government IM/IT Resources and
- The Information Incident Management Process, as well as
- The Working Outside the Workplace Policy if/as applicable.

Please refer to the Glossary for a definition of terms used in this Agreement, including what is meant by a *network connection* (7) and a non-government device.

DEVICE INFORMATION

Please provide the following information about the device or, if an item does not apply, provide the rationale as to why not.

DEVICE TYPE *(e.g., Laptop, etc.)*	NAME OF ANTI-VIRSUS SOFTWARE INSTALLED *(e.g., Norton, Kaspersky)*
DEVICE NAME (5)	NAME OF FIREWALL SOFTWARE ENABLED *(e.g., ZoneAlarm)*
DEVICE MAC ADDRESS (4)	NETWORK ACCESS START DATE *(YYYY MMM DD)*
ADDRESS OF OFFICE WHERE DEVICE OWNER IS PRIMARILY LOCATED	**NETWORK ACCESS END DATE** *(YYYY MMM DD)* ***(Maximum 1 year)***

CONTACT INFORMATION

DEVICE OWNER	**AGREEMENT MANAGER**
NAME	NAME
PHONE	PHONE
EMAIL	EMAIL
COMPANY OR ORGANIZATION NAME	**MINISTRY**

NON-GOVERNMENT DEVICE ACCESS AGREEMENT (NDAA)

AGREEMENT

Individuals signing this Agreement must read and comply with the following terms to fullest extent possible for the device. Non-compliance will be investigated on a case-by-case basis; individuals found to be in non-compliance are subject to disciplinary action up to and including dismissal, cancellation of contract, and/or other legal remedies.

The Device Owner must:

1. Ensure the information supplied in this Agreement is accurate at the time of completion, inform the Agreement Manager of any changes and, where applicable, update and re-sign this Agreement.
2. Immediately report all security-related issues (including privacy breaches) per the Information Incident Management Process.
3. Understand that it is forbidden to test the security features of the SPAN/BC network/resources without written permission from the GCIO (Government Chief Information Officer). Without such permission, your actions will be viewed as hostile and an investigation will be initiated.
4. Not connect any additional unapproved hardware devices to the network (e.g. printers, hubs, switches, wireless routers, USB drives).
5. Ensure that all installed software is licensed appropriate to its use in a government environment.
6. Not store personal or sensitive government information on the device. Where there is a business justification to store such information on the device:
   - it must be formally approved in writing by the respective ministry *Information Owner* (6);
   - the information must be encrypted to government's current cryptographic standard; and
   - the primary copy of the information must be stored on the government network, not on the device.
7. When access to the government network is no longer required, or the Device Owner's relationship with the ministry changes/ends, inform the Agreement Manager and provide confirmation that:
   - all government data, files, and documents are securely erased from the device, in accordance with the IT Asset Disposal Management Process; and
   - all government-owned software, hardware, documentation, storage media and licenses have been removed from the device and returned fully and completely to the ministry.

The Device Owner must use a variety of safeguards if/as available for the device, including but not limited to the following:

- Implement device access controls (e.g. logon to device using a password, locking screen-savers) and physical safeguards (such as cable locks to secure laptops to desks);
- Utilize strong *authentication* (2) methods (including user ID and password combinations, device locking, and session time-out mechanisms) for all applications and services running on the device;
- Ensure that all installed software (including anti-virus software and associated signature files) is updated regularly with vendor security patches. Best practice is to configure the software so that it is automatically updated or, at minimum, you are notified when vendor patches are made available so they can be installed manually in a timely manner;
- Enable real-time anti-virus scanning, and conduct a full scan of all discs at least weekly; and
- Install and enable a software firewall.

In addition, the Device Owner must **not**:

- Enable Peer to Peer software (e.g. BitTorrent, Limewire) being used for personal purposes.
- Allow the device to act as a server or offer services to the network.
- Run software on the device to scan or monitor the network (e.g. NMAP, wireshark).

Ministry of Social Development and Social Innovation

NON-GOVERNMENT DEVICE ACCESS AGREEMENT (NDAA)

SIGNATURES

I, _____ (the Device Owner), have read this Agreement, understand its contents, and agree to comply with the provisions therein.

(SIGNATURE)	DATE SIGNED *(YYYY MMM DD)*

Authorizing Agreement Manager

(SIGNATURE)	(PRINT NAME)	DATE SIGNED *(YYYY MMM DD)*

Scan and email completed form to MHRSECAD@gov.bc.ca and HSDINSEC@gov.bc.ca prior to connecting device to the network. Original to be placed on Employee or Contract file; copy to Device Owner and Agreement Manager.

GLOSSARY

1. Agreement Manager - The ministry person responsible for the individual completing this Agreement. This may be an employee supervisor, a contract manager, or a business owner.

2. Authentication - The verification of the identity of a person or process. “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.

3. Device - Components that can be attached to a network, including desktops, laptops, personal digital assistants (PDA's), external storage devices, smart phones, tablets, servers, etc.

4. Device MAC Address - The Media Access Control address (MAC address) is a unique identifier associated with your device. On a computer running Windows, this can be found by typing “IPCONFIG /ALL” at the DOS prompt. On other devices, the information can usually be found in the settings.

5. Device Name - This may also be referred to as the “computer”, “host”, or “system” name. On a computer running Windows, this can be found by typing “IPCONFIG /ALL” at the DOS prompt. On other devices, the information can usually be found in the settings.

6. Information Owner - The person with responsibility and decision making authority for the information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure.

7. Network Connection - Any means of directly connecting a device to the BC Government network from within a ministry office, whether via a wired (e.g. LAN cable) or wireless (e.g. Wi-Fi, Bluetooth) connection.

8. Non-government Device - Any personally-owned or non-SSBC provisioned device. Per Core Policy 6.4.5.a.6, all IM/IT hardware must be ordered through SSBC; any device not procured per policy is considered a non-government device for the purpose of this Agreement.

ADDITIONAL RESOURCES

General Service Agreement including Schedules E (Privacy) and G (Security)	http://pss.gov.bc.ca/psb/gsa/gsa_index.html
Information Security Policy	http://www.cio.gov.bc.ca/cio/informationsecurity/policy/informationsecuritypolicy.page
IM/IT Standards Manual including wireless and cryptographic standards	http://www.cio.gov.bc.ca/cio/standards/standards_manual.page?

If you require additional information, please contact your Ministry's Information Security Officer (MISO).