April 29, 2010

Working Outside the Workplace

Office of the Government Chief Information Officer

Ministry of Citizens' Services
Province of British Columbia

Table of Contents

TABLE OF CONTENTS **1**

POLICY OVERVIEW **2**

REFERENCES AND TERMS INCLUDED **2**

SCOPE **2**

SUPPORTING DOCUMENTS **3**

SECTION 1: POLICY PRINCIPLES **4**

Individual Responsibility for Management of Information 4
Confidential and/or Personal Information Must be Managed 4
Personal Information Management Requires Extra Precautions 4

SECTION 2: BEST PRACTICES **5**

BEST PRACTICE: USING A GOVERNMENT LAPTOP/TABLET **5**

BEST PRACTICE: USING DTS AND REMOTE DESKTOP CONNECTION WITH VPN **6**

BEST PRACTICE: USING OUTLOOK WEB ACCESS AND GOVERNMENT ISSUED ENCRYPTED USB MEMORY STICKS **8**

SECTION 3: WORKING OUTSIDE THE WORKPLACE POLICIES: **10**

POLICIES: 10
Information Inventory and Transport 10
Physical Security and Transport of Information, Devices and Paper Outside the Workplace 10
Working with Electronic and Paper Based Records 11
Information Incident Management Process Summary 12

SECTION 4: WORKING OUTSIDE THE WORKPLACE RESPONSIBILITIES **13**

RESPONSIBILITIES: 13
Supervisors 13
Employees 13

APPENDIX A: GLOSSARY **15**

WORKING OUTSIDE THE WORKPLACE POLICY

Policy Overview

This policy document provides direction on how to safeguard electronic and paper based confidential and/or personal information when working outside the workplace. Prior to making arrangements for working or removing confidential and/or personal information from the workplace, **employees (and others as included in the scope statement below) must ensure that they have received their supervisor's approval.**

For questions or comments regarding this policy please contact:

Knowledge and Information Services
Office of the Government Chief Information Officer
Ministry of Citizens' Services
Telephone: 250-356-0361

References and Terms Included

There are a variety of ways to refer to information in government's care. Information can be referred to generally as 'government information'. Alternatively, a specific type of information can be described as confidential and/or personal – these are the terms used throughout this policy. Confidential information includes such things as a Cabinet or Treasury Board Submission or other documents as identified within a ministry or program area. Management of personal information -- that is information recorded about an identifiable individual (such as a name, address, birth date, gender) is governed by the *Freedom of Information and Protection of Privacy Act*. The Act specifies the way government ministries (referred to in the legislation as public bodies) may use, collect, and disclose personal information in its care. Personal information is also confidential information.

The Government of British Columbia and its employees are entrusted with confidential information and/or personal information. As government employees, we are expected to apply the safeguards, prudence and due diligence needed to protect such information both inside and outside of the workplace.

A Glossary of relevant terms is included as Appendix A.

Scope

This policy applies to employees and business owners (including supervisors and service providers) or any person handling information managed (e.g., accessed, collected, used, shared, stored, disclosed, disposed of) by the Government of British Columbia.

Supporting Documents

The following documents and tools support the application of this policy:

1. Home Technology Assessment
2. Information Incident Management Process
3. *Freedom of Information and Protection of Privacy Act*

Section 1: Policy Principles

The following statements are the foundational principles guiding the development of this policy.

Individual Responsibility for Management of Information

Public Service employees are individually and collectively responsible for ensuring that confidential and/or personal information is administered as authorized by policy or legislation.

Confidential and/or Personal Information Must be Managed

Confidential and/or personal information must be managed by making reasonable security arrangements, taking into account its value and sensitivity against such risks as unauthorized access, collection, use, storage, disclosure or disposal.

Personal Information Management Requires Extra Precautions

Personal information must be accessed, collected, used, stored, disclosed and disposed of as authorized by the *Freedom of Information and Protection of Privacy Act*, *Document Disposal Act* and other relevant legislation.

Section 2: Best Practices

The following best practices are offered as guides 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 (e.g., https://Summer.gov.bc.ca)and government issued encrypted USB memory sticks. These guides are provided in such a way that each topic area can standalone, outside of the policy document.

Best Practice: Using a Government Laptop/Tablet

The safest and easiest way to work outside of the workplace is to use a government issued computer (laptop or tablet) and save information to your encrypted desktop. The following outlines the steps recommended for working outside the workplace including the use of electronic and paper based confidential and/or personal information and a government computer.

Step 1: Confirm with your supervisor that you can work with confidential and/or personal information and take it outside the workplace.

Step 2: Save the confidential and/or personal information you are taking outside the workplace to the desktop of the government computer you will be using. If you need additional materials (such as paper based confidential and/or personal information) that you did not save to your laptop, record its removal from the workplace as required. Only take the minimal amount of information necessary to complete work outside of the workplace.

Step 3: When travelling, safeguard the confidential and/or personal information by ensuring you keep control of the government computer and any other work materials (e.g., paper based information) or if you must leave them unattended, ensure they are appropriately safeguarded (e.g., locked in the trunk of a car).

Step 4: Undertake your work at the alternative worksite. Be careful that you are the only one who views the confidential and/or personal information and who works on the government computer. **Do not** share your government user ID and passwords. When your work is complete, ensure the computer and other work materials are appropriately safeguarded (e.g., secured to a safe place).

Return the government computer and any work materials, safeguarding them while travelling, to the workplace. Upload the new or revised information to the network as appropriate.

Step 5: If an information incident occurs, including a privacy breach, notify your supervisor, your Ministry Chief Information Officer and report it to the Government Chief Information Officer by calling Shared Services BC at 250-387-7000 (or toll-free at 1-866-660-0811) and selecting Option 3.

For more information see the Information Incident Management Process.

Best Practice: Using DTS and Remote Desktop Connection with VPN

While government issued computers (laptops and tablets) are the first choice in securely working outside of the workplace these may not always be available. Alternatives that also offer a high level of security are DTS (Desktop Terminal Services) and Remote Desktop Connection with VPN. For access to these services, check with your supervisor. The following outlines the steps recommended for working outside the workplace including the use of electronic and paper based confidential and/or personal information as well as DTS and Remote Desktop Connection with VPN.

Step 1: Confirm with your supervisor that you can work with confidential and/or personal information and take it outside the workplace. Also with your supervisor, determine the most appropriate method of access given the cost, accessibility and sensitivity of the information being worked on. The necessary service may be ordered from iStore.

Step 2: If you need additional materials (such as paper based confidential and/or personal information) that is not accessible remotely, record its removal from the workplace as required. Only take the minimal amount of information necessary to complete work outside of the workplace.

If you are a first time user, ensure DTS or Remote Desktop Connection with VPN software is available for your use by Shared Services BC and install it as instructed.

Step 3: When travelling, safeguard any confidential and/or personal information by ensuring you keep control of work materials (e.g., paper based information) or if you must leave them unattended, ensure they are appropriately safeguarded (e.g., locked in the trunk of a car).

Step 4: When using DTS or Remote Desktop Connection with VPN, confidential and/or personal information is displayed on the computer screen but not stored. **Do not download or save to the local hard drive, or print** confidential and/or personal information accessed electronically when using a non-government computer.

If in an extenuating circumstances the need arises to download/store confidential and/or personal information when working outside the workplace it must be stored on a government issued encrypted USB memory stick using a **secured home computer** or if an encrypted USB memory stick is not available, then to an encrypted folder on a **secured home computer**. If it becomes necessary to print documents outside the workplace in an extenuating circumstance, this can only be undertaken using a **secured home computer**; in this case a Home Technology Assessment must be completed. There are tips available on securing a home computer that may be of assistance and may be found at the Office of the Chief Information Officer website.

Be careful that you are the only one who is able to view the electronic or paper based confidential and/or personal information. **Do not share** your government user ID and passwords. When your work is complete, ensure any work materials are appropriately safeguarded (e.g., secured to a safe place).

Return any work material(s), safeguarding them while travelling, to the workplace.

Step 5: If an information incident occurs, including a privacy breach, notify your supervisor, your Ministry Chief Information Officer and report it to the Government Chief Information Officer by calling Shared Services BC at 250-387-7000 (toll-free 1-866-660-0811) and selecting Option 3

For more information see the Information Incident Management Process.

Best Practice: Using Outlook Web Access and Government Issued Encrypted USB Memory Sticks

While government issued computers (laptops and tablets), DTS and Remote Desktop Connection with VPN are the preferred choices in securely working outside of the workplace these may not always be available. Outlook Web Access (e.g., available at: https://summer.gov.bc.ca) is used to access your email via a browser such as Internet Explorer. Government issued encrypted USB memory sticks are a good method of transporting electronically stored confidential and/or personal information. Prior to using any tools to work outside of the workplace check with supervisor. The following outlines the steps recommended for working outside the workplace including the use of electronic and paper based confidential and/or personal information while using Outlook Web Access , and a government issued encrypted USB memory sticks.

Step 1: Confirm with your supervisor that you can work with confidential and/or personal information and take it outside the workplace.

Step 2: If you need additional materials (such as paper based confidential and/or personal information) that is not accessible remotely, record its removal from the workplace as required. Only take the minimal amount of information necessary to complete work outside of the workplace.

Ensure a complete understanding of the log-in procedures for Outlook Web Access.

Step 3: When travelling, safeguard any confidential and/or personal information or materials by ensuring you keep control of work materials (e.g., paper based information) or if you must leave them unattended, ensure they are appropriately safeguarded (e.g., locked in the trunk of a car).

Step 4: When using Outlook Web Access confidential and/or personal information is typically displayed on the computer screen, but not stored. **Do not download, save to the local hard drive, or print or open** confidential and/or personal information accessed via Outlook Web Access or contained on a government issued encrypted USB memory stick on a non government computer (such as a hotel computer). Opening, downloading or printing documents creates a copy of them on the computer that could be recovered by skilled professionals.

If in an extenuating circumstance the need arises to download/store confidential and/or personal information from Outlook Web Access information must be stored on a government issued encrypted USB memory stick using a **secured home computer** or if an encrypted USB memory stick is not available, then to an encrypted folder on a **secured home computer**. If it becomes necessary to print or open documents from Outlook Web Access in an extenuating circumstance, this can only be undertaken using a secured **home computer** in this case a Home Technology Assessment must be completed. There are tips available on securing a home

computer that may be of assistance and may be found at the Office of the Chief Information Officer website.

Be careful that you are the only one who is able to view the confidential and/or personal information. When your work is complete, ensure any work materials are appropriately safeguarded (e.g., secured to a safe place). **Do not share** your government user ID and passwords.

Return any work materials, safeguarding them while travelling, to the workplace.

Step 5: If an information incident occurs, including a privacy breach, notify your supervisor, your Ministry Chief Information Officer and report it to the Government Chief Information Officer by calling Shared Services BC at 250-387-7000 (toll-free 1-866-660-0811) and selecting Option 3.

For more information see the:

- Home Technology Assessment
- Information Incident Management Process.

Section 3: Working Outside the Workplace Policies:

This section provides the policy direction for working with confidential and/or personal information outside the workplace.

Policies:

Information Inventory and Transport

1. Recording Electronic or Paper Based Confidential and/or Personal Information

A. An assessment should be undertaken regarding the establishment of an information inventory system with regard to how confidential and/or personal information leaves the workplace.

B. Supervisors must approve confidential and/or personal information taken out of the workplace; in some cases this may be provided for employees who, as part of their responsibilities work with confidential and/or personal information on a regular basis outside of the workplace. For employees that only take confidential and/or personal information periodically outside of the workplace, approval must be obtained prior to each instance of removing the information from the workplace.

C. Confidential and/or personal information must be recorded prior to leaving the workplace.

D. The amount of confidential and/or personal information transported outside the workplace, whether electronic or paper records, must be limited to only that necessary for work purposes. (**NOTE:** Electronic information can only be removed from the workplace if it is encrypted (see below)).

Physical Security and Transport of Information, Devices and Paper Outside the Workplace

2. Physical Security While Working Outside the Workplace:

A. Reasonable security measures must be made to safeguard electronic storage devices and paper based confidential and/or personal information while in transport and in use outside the workplace. These measures include:

i. reducing the visibility of the device or information; and

ii. keeping control of the device or information whenever possible, or if left unattended, appropriately safeguarded (e.g., locked in the trunk of a car).

B. Secure confidential and/or personal information (e.g., storing in a lockbox, drawer or briefcase) when not in use.

3. **Encryption of Electronic Confidential and/or Personal Information When Stored or Transported Outside of the Workplace:**

   A. Prior to leaving the workplace electronic confidential and/or personal information must be encrypted onto a government approved electronic device (e.g., laptop, portable hard drive, USB memory stick).

4. **Mail or Courier Transport Electronic or Paper Based Confidential and/or Personal Information:**

   A. If it becomes necessary to mail or courier electronic or paper based confidential and/or personal information to an alternative worksite:

      i. electronic information must be encrypted;

      ii. encrypted storage devices and paper based confidential and/or personal information must be sent using BC Mail Plus, external couriers, or personal/hand delivery;

      iii. Decryption passwords, or paper based confidential and/or personal information, must not accompany the encrypted storage device that is mailed or couriered.

5. **Travel Outside Canada**

   A. Electronic or paper based confidential and/or personal information must not be transported or accessed outside of Canada unless specific legislative requirements are met (refer to the *Freedom of Information and Protection of Privacy Act* for more information).

6. **Undertaking Work in Public Areas**

   A. Working on confidential and/or personal information in public areas is not recommended including public computers (e.g., computers located in hotel lobbies).

Working with Electronic and Paper Based Records

1. **Using Electronic Information Outside the Workplace**

   A. The most appropriate electronic method for accessing confidential and/or personal information must be established prior to working outside the workplace. Consideration must be given to the cost, utility, and level of protection needed relative to the type of information. Options in descending order of preference include:

      - government approved computers with encryption (e.g., laptops and tablets);
      - Desktop Terminal Service (DTS);
      - Remote Desktop Connection with VPN;

- Outlook Web Access (e.g., Summer.gov.bc.ca) (for email use only).

B. Confidential and/or personal information **must not be downloaded/ stored** to a non government computer**.**

C. **If in an extenuating circumstance** it becomes necessary to **download/store** confidential and/or personal information using a non government device it must be stored on a government issued encrypted USB memory stick or an encrypted folder on a **home computer**, after a Home Technology Assessment has been completed and appropriate safety measures installed.

D. Confidential and/or personal information **must not be printed** using a non government computer.

E. **Do not open** email attachments or documents that contain confidential and/or personal information from Outlook Web Access (e.g., Summer.gov.bc.ca) or a government issued USB memory stick when using a non-government computer.

F. **If in extenuating circumstance**s, when government devices (e.g., computer, encrypted USB memory stick) are not available and it becomes necessary **to open or print** confidential and/or personal information using a non government computer then only a **home computer** may be used once a Home Technology Assessment has been completed and appropriate safety measures installed.

See Best Practice Guides for more information.

2. Using Paper-Based Information Outside the Workplace

A. Only authorized individuals may access and/or view paper based confidential and/or personal information outside the workplace.

B. Paper-based information used outside the workplace and no longer required for work purposes, must be returned to the workplace and scheduled using the applicable records management procedures.

Information Incident Management Process Summary

3. Reporting the Loss or Unauthorized Disclosure of Government Information

A. Any employee, service provider or other person who discovers a suspected or actual information incident including a privacy breach, must notify their supervisor, their Ministry Chief Information Officer and report it to the Government Chief Information Officer by calling Shared Services BC at 250-387-7000 (toll-free 1-866-660-0811) and select Option 3, stating that they require a “Security Investigation”.

For more information see the Information Incident Management Process.

Section 4: Working Outside the Workplace Responsibilities

This section outlines responsibilities associated with working outside the workplace for supervisors and employees.

Responsibilities:

Supervisors

When preparing or allowing employees to work outside of the workplace supervisors are responsible for:

- Approving any working outside the workplace arrangement(s) with staff;
- Providing direction on when and how to record confidential and/or personal information before it leaves the workplace.
- Ensuring employees are aware of:
  - where to find information and assistance to ensure the safeguarding of electronic and/or paper based confidential and/or personal information when working outside of the workplace; and
  - how to report an information incident.
- Communicating appropriate safeguarding, physical security and transportation measures of electronic and/or paper based confidential and/or personal information as included in this policy or established within the work area as a result of this policy.
- Ensuring government approved devices and tools are available for employees to securely transport and work with electronic and/or paper based confidential and/or personal information at alternative worksites.
- Undertaking periodic reviews to ensure that employees are using appropriate handling and transportation methods.
- Ensuring a Home Technology Assessment is completed and that any recommended updates are confirmed with the employee prior to using a home computer. **NOTE:** Only in extenuating circumstances can a home computer be used (see specific instructions as included in this policy document).

Employees

When preparing or working outside of the workplace employees are responsible for:
Ensuring that prior to making arrangements for working or removing confidential and/or personal information from the workplace, they have received their supervisor's approval.

- Understanding the policy requirements as outlined in this document and/or established within the workplace, including safeguarding and security measures prior to transporting or working with electronic and/ or paper based confidential and/or personal information.
- Knowing where to seek assistance if questions arise regarding safeguarding electronic and/or paper based confidential and/or personal information.
- Knowing how to report an information incident.

- Limiting the amount of personal and/or confidential information taken outside the workplace to only that necessary to complete the work.
- Following directions provided by their supervisor relative to recording confidential and/or personal information before it leaves the workplace.
- Ensuring that electronic and/or paper based confidential and/or personal information is protected from loss or unauthorized disclosure when it is transported or used outside of the workplace.
- Using the remote access method (e.g., DTS) as approved by their supervisor to securely access confidential and/or personal information when working outside of the workplace and understanding any limitations associated with the approved method.
- Completing a Home Technology Assessment and any recommended updates prior to using a home computer. **NOTE:** Only in extenuating circumstances can a home computer be used (see specific instructions as included in this policy document). The Home Technology Assessment, once completed must be discussed/submitted with your supervisor.
- Protecting user passwords and any other information that could allow unauthorized access to government information.

Appendix A: Glossary

Alternative Worksite – also referred to as "Worksite" refers to the sites that an employee may work outside of the regular workplace.

Confidential Information - Types of confidential information including, but not limited to:

- Cabinet confidences, for example, a briefing note to Cabinet;
- government economic or financial information, for example, information about a proposed administrative plan that has not yet been implemented or made public;
- information harmful to intergovernmental relations, for example, information received in confidence from another government;
- third party business information, where its disclosure would harm the third party;
- personal information, where its disclosure would constitute an unreasonable invasion of a third party's privacy, for example, a reference to correspondence from an identifiable individual;
- legal advice or law enforcement information.

Examples of confidential information are defined in Sections 12 to 22 of the *Freedom of Information and Protection of Privacy Act* manual.

Employee: Includes employees who have sworn the Public Service Oath.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher or code) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Government Approved Electronic Devices: Devices approved for use within the government infrastructure and are available for use by employees. Devices include laptops, portable hard drives, USB memory sticks, memory cards or other electronic devices used to store or process electronic information.

Government Information: Means all recorded information, regardless of physical format, that is received, created, deposited or held by or in any ministry, agency, board, commission, Crown corporation, institution, committee or council reporting or responsible to the Government of British Columbia. Government records include machine-readable records, data stored in information systems, film, audio and audiovisual tapes, etc. Government records include cabinet ministers' records that are created and/or accumulated and used by a Minister (or a Minister's office) in developing, implementing and/or administering programs of government. Government records do not include legislative records (records created and/or accumulated and used by an individual or an office in the administration of the Legislative Assembly of British Columbia or by a Member of the Legislative Assembly). The retention and final disposition of most government records is governed by the *Document Disposal Act*.

Home Computer: A computer that typically is owned and used by a single responsible user or a small group of known users. Users typically have the authority to install software, change settings and customize the machine's behaviour to their preferences.

Information Incident: A single or a series of unwanted or unexpected events that threaten information security or privacy. Government employees are expected to take reasonable safeguards to protect information regardless whether working at the workplace or an alternative worksite. Since an information incident can happen to anyone, government has established a single, consistent process that must be used if an information incident occurs or is suspected.

Non-government Computer: Any computer not managed or owned by government such as home computers (see definition) or public access computer. Many non-government computers in public locations can be used by a variety of individuals throughout the course of a day and therefore security cannot be verified. Users typically don't have the authority to install software or change settings. A home computer, in contrast, is typically used by a single responsible user, who can customize the machine's behaviour to their preferences.

Personal Information: Recorded information about an identifiable individual other than business contact information. Personal information can be about government employees, government clients or others and may be held by government or administered by service providers on behalf of government. Personal information includes, but is not limited to:

- name, address, telephone number, email;
- race, national/ethnic origin, colour, religious or political beliefs or associations;
- age, sex, sexual orientation, marital status;
- identifying number or symbol such as social insurance number or driver's licence number;
- fingerprints, blood type, DNA prints;
- health care history;
- educational, financial, criminal, employment history; and
- anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.

Primary Record: the "official copy of record" or "master copy" of government records (e.g., as opposed to convenience copies created for reference or temporary use. Includes the administrative and operational records that are created by government offices, and are to be filed and retained in accordance with the standard government records classifications and scheduling systems (i.e., ARCS/ORCS).

Record: Includes records created and received in all media and formats. Examples include: records created using electronic communications devices/technologies such as email and instant messaging; information stored on magnetic tapes, thumb drives, LANs, and in databases; records held in electronic document and records management systems; paper files, maps and GIS; and documents created and posted to websites, SharePoint and Groove.

Storage Media: Any object upon which data can be stored. Some media, such as tapes, tape cartridges, and magnetic or optical disks can only be read by a machine. Other storage media, such as paper, microfilm and microfiche can be read directly by humans without using a machine. Permanent government records are stored on human readable media (e.g., paper).

Workplace: Refers to the government office or place of work including those defined in a teleworking agreement.

Worksite: Also referred to as "alternative worksite" refers to the sites that an employee may work outside of the regular workplace.