Freedom of Information and Protection of Privacy Act	**Program**	**Privacy and Access**
	Subject	**Protecting Personal and Sensitive Information in Transit**
Effective Date: April 5, 2013 **Revised Date: May 1, 2017**		**Authorized by:** **Deputy Minister, Teresa Hennebery**

1.0 PURPOSE

1.1 To ensure security of personal and sensitive department information in transit.

2.0 DEFINITIONS

2.1 **Electronic storage medium:** USB type flash drives commonly referred to as jump drives, external hard drives, CDs and DVDs.

2.2 **Personal information:** as defined in *The Freedom of Information and Protection of Privacy Act* (section 1(i)) is recorded information about an identifiable individual, including, but not limited to:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and
- the individual's personal views or opinions, except if they are about someone else

2.3 **Portable computing device:** any computer that can be moved off-site, to include but not limited to laptops, notebooks, tablets, mobile devices, and any computer which will be used off-site.

2.4 **Sensitive information:** operational information which, if lost or disclosed, could result in harm, disruption of government affairs or other negative consequences.

3.0 POLICY STATEMENT

3.1 Department employees will take measures to protect confidential and sensitive information including, but not limited to:

- Securely maintaining paper files and documents
- Securely maintaining electronic files and documents
    - Limiting storage of personal and sensitive information on portable computing devices and electronic storage media
    - Use of password protection on devices
- Appropriate management of breaches

3.2 Department employees will follow Guide to Information Security: Information Guide for Employees regarding safe electronic and physical document handling for government employees.

4.0 PROCEDURE STATEMENT

Securely maintaining paper files and documents

4.1 A file sign out process will be established at each work site. Employees will comply with the sign out process. Client files being removed from filing rooms will be tracked using the sign out process established at each work site.

4.2 Employees will ensure that files removed from the file rooms will not be situated where others unrelated to the file may view the contents, and will be kept in a secure location when not in use.

4.3 Employees will not remove personal or sensitive files and documents from the work site unless necessary.

4.4 When an employee removes personal or sensitive files and documents from the work site, the employee will ensure information is kept in a secure (not necessarily locked) briefcase or carrying bag at all times. If the file is left unattended in a vehicle, the vehicle must be locked.

4.5 When an employee removes personal or sensitive files to another location, the files must be maintained in a secure location which would guard against unauthorized access, use, disclosure or destruction of the information.

4.6 Employees must return files to the work site as soon as possible after use.

Limiting storage of personal or sensitive information on portable computing devices and electronic storage media

4.7 Employees must limit identifiable personal information stored on portable computing devices and electronic storage media to what is minimally necessary.

4.8 Employees must only store personal information on a portable device or storage medium for the minimal amount of time necessary to complete the work.

Use of Password Protection on Devices

4.9 Where personal or sensitive information is stored on portable computing devices, the information must comply with Standard Password Configuration detailed in standards and procedures established by Government Information Security Policy (http://iis.peigov/itsecurity/index.html) .

4.10 Employees must not disable passwords and locks.

Management of Breaches

4.11 In the event that a breach occurs from the theft or loss of a device/ medium containing personal or sensitive information, the employee must report to the employee's immediate supervisor, and actions taken as per the *Managing Unauthorized Disclosure or Loss of Personal and Sensitive Information* policy.

4.0 REFERENCES

Government Information Security Policy, Standard Password Configuration

Guide to Information Security: Information Guide for Employees

Managing Unauthorized Disclosure or Loss of Personal and Sensitive Information policy

---

HISTORY:

May 1, 2017 – Recognized creation of Access and Privacy Services by removing reference to in-department FOIPP Coordinator; removed information repeated in the Managing Unauthorized Disclosure of Loss or Personal and Sensitive Information policy