



Issue Date: September 2009	Effective Date: Immediate	Responsible Agency: Department of Finance	Directive No: 606
Chapter: Government Accounting Policy			
Directive Title: PROTECTION OF PERSONAL FINANCIAL INFORMATION			

1. POLICY

The collection, use, disclosure and storage of personal financial information shall be accomplished in a manner that ensures that the data is used only for the purpose for which it is collected and is protected against unauthorized use by persons inside or outside of Government.

The handling of personal financial information shall be in accordance with the provisions of the *Access to Information and Protection of Privacy Act (ATIPP)* and the *Archives Act*.

S.5 of the *Financial Administration Act* authorizes the Financial Management Board to issue directives concerning the controlling and recording of financial data.

2. DIRECTIVE

Departments may only collect personal financial information that is required to perform the duties of the department. The collection of all other personal financial information is prohibited.

Deputy Heads are responsible for ensuring that systems are in place to safeguard personal financial information and that it is only used for its intended purpose.

The systems and procedures must comply with *ATIPP*, the *Archives Act* and the provisions of this directive.

3. PROVISIONS

3.1. Collection of Information

- 3.1.1. Personal information is defined in S. 2 of *ATIPP* as information about an identifiable individual, including (among other things):

- (a) the individual's name, home or business address or home or business phone number;
- (b) an identifying number, symbol or other particulars assigned to the individual.

Personal financial information is personal information, as defined above, which is used by the Government in conducting a financial transaction.

- 3.1.2. This directive covers personal financial information relating to employees of the Government as well as to all non-employees dealing with the Government.
- 3.1.3. Only personal financial information that is essential for the conducting of the affairs of the Government shall be collected. The information should, where possible, be collected directly from the individual and that individual must be advised of the purpose for which the information is collected and the legal authority for the collection. The reason that the information is required must be documented and retained by the Executive Finance Officer (EFO) of the Department collecting the information.
- 3.1.4. Any agreements entered into by the Government that involve the collection of personal financial data must be reviewed by the Department of Finance and the Department of Executive and Intergovernmental Affairs before they are concluded to ensure that the proper controls and safeguards are in place to comply with the terms and conditions of the proposed agreement regarding personal financial information.
- 3.1.5. The Deputy Head is responsible for reviewing all new programs or activities undertaken by their department to ensure that personal financial information collected, if any, is handled in accordance with the provisions of this Directive and *ATIPP*.
- 3.1.6. Departments may consult the Directorate of Executive and Intergovernmental Affairs and/or the Records Management section of Community and Government Services (CGS) for assistance and advice concerning the definition and handling of personal financial information.
- 3.1.7. The Deputy Head is responsible for ensuring that all public officers within their department are aware, and are familiar with, the requirements of *ATIPP*, the *Archives Act* and the provisions of this

directive, as they apply to the handling of personal financial information.

3.2. Storage and retention of information

- 3.2.1. Information is more difficult to protect if it is stored in different locations. The duplication of information in different files or electronic folders is to be avoided unless absolutely necessary for the operation of the program involved. The reason that duplicate information is required is to be documented and retained by the EFO of the department.
- 3.2.2. All personal financial information collected electronically shall be stored on a central computer server that has password, firewall, virus protection and backup features to guard against misuse of the data. The storage of personal financial information on stand alone computers, laptops, handheld or removal storage devices is prohibited.
- 3.2.3. All personal financial information collected in other than electronic format shall be stored in secure, locked storage containers (safe, file cabinets, etc.) and accessible only to public officers who require the information to carry out the activities for which the information was collected.
- 3.2.4. The retention, storage and disposal of personal financial information shall be in accordance with the Records Management policies of CGS and the provisions of the *Archives Act* as well as rules established by the Public Records Committee established under the *Archives Act*.
- 3.2.5. The EFO in each department shall ensure that a review is conducted periodically (annually recommended) of the personal financial information that is collected within their department to determine if the reason for collecting the information still exists.

3.3. Use of Information

- 3.3.1. Personal financial information must only be used or disclosed for the purpose for which it was collected, and the other uses and disclosures permitted in Divisions B and C of Part 2 of *ATIPP*, unless consent for other uses and disclosures has been granted.
- 3.3.2. Access to personal financial information stored electronically shall be limited, via password or other such method, to public officers who

require the information to carry out the activities for which the information was collected.

3.4. Rights of persons providing the information

- 3.4.1. The Government cannot refuse to provide an individual with a service because that individual has refused to provide personal financial information, unless the information is essential to the provision of that service.
- 3.4.2. The person from whom the personal financial information is collected must have reasonable access to the information retained by the Government and must have the opportunity to request that changes be made to such information.

3.5. Third party service providers

- 3.5.1. The electronic processing of personal financial information sometimes requires that the information be handled and stored by third party service providers. In these instances, the Department of Finance is responsible for obtaining assurance from these third party providers that they have the systems and safeguards in place to protect the data from being misused. The third party provider will also be required to advise the Government if the data becomes compromised and the preventative action they have taken to recover the data and prevent a reoccurrence.
- 3.5.2. Deputy Heads are responsible for ensuring that all third party services providers, who are processing or storing Government personal financial information, are complying with the requirements of any contracts or agreements that the department has entered into dealing with such information.
- 3.5.3. Any personal financial information that is electronically transmitted across open, public networks must be encrypted to current industry standards.