4.7 Security of Sensitive Statistical Information

Revised July 4, 2007

1. Policy

Statistics Canada gives "enhanced protection" to all sensitive statistical information it acquires or develops. Sensitive statistical information is categorized as “Protected B” information, as described in the Government Security Policy.

2. Definitions

(a) **Sensitive statistical information** consists of:

(i) Information provided in confidence:

- data obtained directly from respondents or from third parties in identifiable mode, under the authority of the *Statistics Act*;
- data holdings stripped of identifiers but held at a level of detail which could permit a direct relation to be established between such data holdings and identifiable units;

(ii) Paradata is information related to a statistical data collection or production process that is linked to an identifiable person, business or organization. It is distinct from the information that is the objective of the statistical data collection or production process (i.e., information provided in confidence as described in (i) above). Examples of paradata are:

- Whether a unit has been selected into a sample
- Whether a selected unit has responded
- Number of attempts to reach a selected unit
- Times of contacts (attempts and interviews)
- Interviewer characteristics, such as years of experience, that are linked to a specific sample unit
- Prior response patterns for a given unit
- Mode of collection (telephone, personal, etc.)
- Source of data (direct collection, admin file, etc.)
- Whether a particular item was reported or imputed.
- Whether a unit has consented (for data sharing, record linkage etc.)
- Any communication to or from a person that is part of the data collection process, provided that such communication can be linked to a specific sample unit

It also includes identifying information (that is used only for operational purposes, but not for analytical reasons) such as the name, address and telephone number of a survey respondent.

(iii) aggregate statistical information in the pre-release stage (including work-in-progress provided to external organizations for data validation).

(b) **Enhanced protection**: refers to a combination of security measures outlined in the Implementation Measures of this policy and in the Statistics Canada Security Practices Manual which afford the level of protection appropriate for the class of information and assets deemed to be sensitive.

Note: Information reported under the *Corporations Returns Act* must be treated in accordance with the specific provisions of that legislation.

3. Responsibilities

(a) Directors

Directors are responsible for the custody of all data holdings under their jurisdiction and, as such, they are responsible for controlling and protecting all sensitive statistical information obtained or held by their respective areas in the pursuit of their program objectives. (In situations where such information is controlled at a Branch or Field level, the appropriate senior manager (i.e., Director General or Assistant Chief Statistician) assumes these responsibilities.) In addition, the use of tax data obtained from the Canada Revenue Agency carries additional requirements.

Directors' responsibilities include:

A. For confidential data held by other divisions

- When required to meet the divisional mandate, formally requesting access to information provided in confidence and paradata held by other divisions;
- Keeping track of the location, users and use made of this information within the division;
- When applicable, reporting the location, users and use made of tax micro data provided by other divisions to the Director of Tax Data Division annually.

B. For confidential data held by the division

- Using the "need to know" principle, reviewing and approving requests from other divisions for access to information provided in confidence and paradata held in their own division;
- When applicable, informing the requesting division that the information being requested contains tax micro data;

- Keeping track of the location, users and use made of information provided in confidence and paradata held in their own division (for users both internal and external to the division);
- When applicable, reporting the location, users and use made of tax microdata held by the division to the Director of Tax Data Division annually (for users both internal and external to the division).

C. Other

- ensuring that the requirements of the Policy on the Use of Deemed Employees (and its associated guidelines) are met for individuals working in their division who are not employees of Statistics Canada, but who require access to sensitive statistical information or to areas where sensitive statistical information is used;
- reporting immediately all possible breaches of security, in particular breaches to the confidentiality provisions of the *Statistics Act* to the Director, Data Access and Control Services Division, who will undertake to inform the Chief Statistician.

(b) Director, Tax Data Division

The Director of Tax Data Division is the designated official to administer the interdepartmental agreement required by the Order in Council stipulated by Section 24 of the *Statistics Act* covering the acquisition of tax records from the Canada Revenue Agency. The Director is responsible for authorizing all requests by other divisions for access to tax micro data held by Tax Data Division.

(c) Director, Informatics Technology Services Division

The Director of Informatics Technology Services Division (ITSD) is responsible for the control and protection of all sensitive statistical information in machine-readable form that is held by the Main Computer Centre. Access to this information is granted by the Director of ITSD on the basis of access decisions and authorizations made by the responsible program directors.

The Director is also responsible for the security of information transmitted electronically within all parts of the Agency over the communications networks that ITSD maintains.

(d) Directors, Regional Operations Branch

These directors are responsible for establishing and implementing appropriate systems and procedures to control and protect sensitive statistical information collected, processed and/or held by their respective jurisdictions.

(e) Director, Operations and Integration Division and Director, Operations Research and Development Division

These directors are responsible for the control and protection of sensitive statistical information processed by their respective divisions on behalf of program divisions.

(f) Director, Data Access and Control Services Division

The Director, Data Access and Control Services Division, is responsible for the development of departmental policies on information security, including all aspects of information classification, control, and access.

The Director is also responsible for providing advice, guidance, and assistance in the implementation of information security measures.

(g) Director, Resourcing and Corporate Assignments Division

The Director is responsible for ensuring that all indicated requirements of the reliability checks required for staff (i.e. Public Service Commission or *Statistics Act* employees) working with sensitive statistical information are carried out before job offers are extended.

(h) Chief, Departmental Security

The Chief, Departmental Security, is responsible for:

- arranging security checks with investigative agencies for new appointees, deemed employees and interviewers and for making appropriate recommendations based on the information received;
- developing appropriate physical security standards to protect sensitive statistical information in the Agency, including management of the guard force;
- carrying out inspections and investigations of suspected breaches or violations of security, and recommending appropriate remedial actions;
- providing advice to management on security matters and conducting security liaison external to Statistics Canada.

(i) Regional Security Officer - Regional Director

Directors of Regional Offices are designated as Regional Security Officers and are responsible for the administration of the security program in their region. See Security Practices Manual, Chapter 1, Statistics Canada’s security structure, Section 1.1 Functional responsibilities.

(j) Manager, Research Data Centre Program

The manager is responsible for controlling access and protecting all sensitive statistical information held in the Research Data Centres.

(k) Security Coordination Committee

The Committee is responsible for reviewing and providing advice on operational and technical safeguards related to the security of sensitive statistical information.

4. Inquiries

Inquiries regarding this policy may be directed to the Director, Data Access and Control Services Division.

******

Implementation Measures

While a detailed outline of personnel, physical, communications and information security standards and procedures to protect sensitive statistical information is found in the Statistics Canada Security Practices Manual, the following is a comprehensive summary.

1. Control of Sensitive Statistical Information

(a) Directors will control all sensitive statistical information under their jurisdiction by keeping an ongoing record of such information as defined in this policy. This record must include a description of the data including whether it contains tax micro data, the frequency and media of any data received, who has access within the division along with a justification and who has access outside of the division along with a justification and the approval of that person’s director.

Records (paper, electronic media, tape, etc.) containing sensitive statistical information are to be retained and disposed of using procedures specifically approved for the purpose. Retention period and format, storage location and disposal arrangements must be coordinated with the Chief, Document Management Centre, and the Chief, IT Security, Informatics Technology Services Division.

Directors must give particular attention to the control of sensitive statistical information in a portable format (e.g. microfiche, diskettes, CDs, flash drives, laptop PCs and hard drives from discarded PCs).

(b) Directors must justify and record their need to retain personal identifiers (such as, name, address, telephone number) after primary processing is completed.

(c) Directors will ensure that sensitive statistical information, as set out in paragraphs 2(a)(i) and (ii) of the "Definitions" section of the Policy, is not taken out of the work place unless authorization is provided by the Chief Statistician. Sensitive statistical information, as set out in paragraphs 2(a)(iii) of the "Definitions" section of the Policy (i.e., work in progress), may not be taken out of the work place unless authorization is provided by the Director with responsibility for the information.

Note: The definition of workplace is extended to include field locations of interviewers and other employees who have the Chief Statistician’s authorization to be in possession of sensitive statistical information.

(d) Inter-divisional access to information provided in confidence must be formally requested and approved in writing at the director level or higher, with supportive documentation that includes:

- a complete description of the data required
- a description of the uses for which the data are intended
- the names of the persons who will be responsible for the actual use of the data
- the names of the persons who will be the actual users of the data
- the period for which access is required and the date when the “borrowed” dataset will be destroyed

(e) On an ongoing basis, all divisions who have been given access to a data set in accordance with (d) above must ensure that access is consistent with the request, and seek updated approval if the situation changes. In particular, the division must maintain the following information:

- a complete description of the data required, including whether it contains micro tax data
- a description of how the data has been used
- an up-to-date record of the names of the persons who are responsible for the actual use of the data
- an up-to-date record of the persons who are the actual users of the data
- current and historical account of the retention and destruction of the data sets.

(f) The Director, Tax Data Division, on a regular basis will contact program directors requesting information on the micro tax data holdings within their division. Other directors must regularly verify that other divisions using their data sets are following the requirements of this policy.

2. Aggregate Statistical Information in Pre-release Stage

Control of aggregate statistical information in pre-release stage is governed by the Policy on Dissemination, Communications and Marketing Services, Appendix 1: Official Release, Annexes A, B and C (February 2004). Directors will ensure that the conditions governing work-in-progress releases are respected.

3. Protection of Sensitive Statistical Information

Directors will protect sensitive statistical information under their control:

(a) by limiting access to employees and individuals deemed to be employees under the terms of the *Statistics Act* who have a work-related need to access the information;

(b) by ensuring that the procedures set out in the Policy and Guidelines on the Use of Deemed Employees are followed when making arrangements to provide access to sensitive statistical information to deemed employees;

(c) by ensuring that the appropriate measures are in place to protect sensitive statistical information in both hard-copy and electronic formats (see Statistics Canada's EDP Security Policy, Statistics Canada's Security Practices Manual, and the Government Security Policy for detailed procedures);

(d) by ensuring that the procedures for visitor access and control are followed.

4. Disclosure of Information

(a) Directors will ensure that all publicly-released statistical information is only in a form which respects the provisions of the *Statistics Act*.

(b) Disclosure of anonymized statistical information at the individual unit level is subject to the Policy on Microdata Release.

(c) Directors must develop and implement disclosure control procedures appropriate for their divisions. These procedures will be used to screen tabulations and analytic results being prepared for external release so as to preclude the release of information that could lead to the identification of an individual person, business or organization.

(d) All requests for the disclosure of sensitive statistical information at the discretion of the Chief Statistician further to subsection 17(2) of the *Statistics Act* should be referred to Data Access and Control Services Division. If required, these requests will be reviewed by the Discretionary Release Review Committee. In the case of administrative information that comes from other departments or organizations, other conditions may apply, as set out in the MOU governing the transfer of the information.

(e) All data-sharing of information provided in confidence with other departments and organizations under sections 11 and 12 of the *Statistics Act* requires a formal agreement between Statistics Canada and the data-sharing partner. These agreements are prepared in consultation with Data Access and Control Services Division.

5. Breaches and Violations of Security

A breach of security is deemed to have occurred when any sensitive statistical information has been the subject of unauthorized disclosure or unauthorized access. A breach may include unauthorized disclosure, theft or loss or circumstances which make it probable that a breach has taken place.

Possible breaches of security, in particular breaches to the confidentiality provisions of the *Statistics Act*, must be reported immediately to the Director, Data Access and Control Services Division, who will undertake to inform the Chief Statistician.

A violation of security is any action taken in contravention of any provision of the Government Security Policy, this policy or Statistics Canada's EDP Security Policy (i.e., a policy violation, not a legal one). Violations will be reported to the Director, Data Access and Control Services Division, who will take appropriate actions.