

POLICY FOR THE PROTECTION OF PERSONAL INFORMATION FROM ACCESS OUTSIDE CANADA

Issued by the President, January 12, 2007

Purpose

The purpose of this policy is to assist the University in meeting its obligations to all members of the University community (students, faculty, staff and alumni) and to participants in University research projects to protect their personal information from unauthorized access by authorities outside Canada. This policy is supplementary to other University regulations, policies, and guidelines concerning the administration and release of student, employee and alumni information and concerning the administration and approval of research projects.

Definitions

“Personal information” means recorded information about an identifiable individual, including, but not limited to:

- a. name, address, telephone, email (personal not business);
- b. race, ethnic origin or religious political beliefs or associations;
- c. age, sex, sexual orientation, marital status or family status;
- d. any identifying number or symbol (examples: Dalcard ID, SIN, credit card, health insurance, drivers' licence);
- e. fingerprints, blood type, or inheritable characteristics;
- f. medical or personal history;
- g. educational, employment, financial, or criminal history;
- h. personal views or opinions..

“Data repository” means any medium where data is recorded, including but not limited to, databases, spreadsheets, paper and electronic documents;

“Employees” for the purposes of this policy includes University employees, academic appointees, and individuals engaged to work on Dalhousie research projects;

“University data repository” means a data repository that is owned or controlled by the University or utilized in research projects under the direction of a faculty member.

Policy

Requirement to Store Personal Information in Canada

1. All University data repositories that store personal information shall be housed and backed-up in Canada unless:
 - a) there is no product or service available that permits the storage, housing and back-up of the personal information in Canada which meets the purchasing requirements; or
 - b) there is no product or service that permits the storage, housing or back-up of the personal information in Canada that meets the purchasing requirements in a competitive manner, having regard to the overall cost, range of services or functions, degree of sensitivity of the personal information at issue, data security arrangements, and whether it is necessary to meet the requirements of a University program, operation or activity;
2. Employees who wish to purchase a product or service under section 1(a) or (b), must obtain the prior written approval of the responsible Vice-President. In all other cases, when purchasing or renewing arrangements for software, hardware or services for the collection, hosting, storage, management, manipulation, or other use of personal information, the employee making the purchase or requesting services must ensure that the proposed arrangement includes a requirement that the personal information must be stored, housed and backed-up in Canada.

Access to Personal Information from Outside Canada

3. Access from outside Canada to personal information held in University data repositories shall not be permitted unless:
 - a) it is the individual's own personal information; or
 - b) the employee is using a web-based or other internet access tool as a necessary part of performing his or her assigned duties or as a necessary part of a research project; or
 - c) such access is approved in writing in advance by the responsible Vice-President as part of a software, maintenance or troubleshooting arrangement (including any renewals):
 - i) that is part of an overall arrangement that is necessary to meet the requirements of a University program, operation or activity; and

- ii) that contains appropriate security controls and restrictions on the use and disclosure of the personal information; or
- d) consent from the individuals to whom the information relates has been provided in a manner approved by the responsible Vice-President; or
- e) such access is otherwise approved in advance in writing by the responsible Vice-President.

Disclosure of Personal Information Outside Canada

4. Personal information held on University data repositories shall not be disclosed to any person or organization outside Canada unless:
 - a) the disclosure is to the individual to whom the information relates; or
 - b) the individual has consented to the disclosure, such consent to be in a form approved by the responsible Vice-President; or
 - c) the disclosure is necessary for the delivery of contracted payroll services under the direction of the Department of Personnel Services; or
 - d) the disclosure is necessary for completing financial transactions under the direction of the Department of Financial Services (eg. processing of cheques, drafts, credit card or other forms of payment by, and to the credit of, the University); or
 - e) such disclosure is otherwise approved in advance in writing by the responsible Vice-President.

Transporting Personal Information Outside Canada

5. Employees may transport personal information temporarily outside Canada only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. In such event, employees are required to take all reasonable precautions to protect the personal information.

Requests for Disclosure of Personal Information

6. Any requests for disclosure of personal information by authorities or organizations from outside Canada, or which have the appearance of being from such sources, shall be referred to the University Legal Counsel Office as soon as reasonably possible following receipt of such a request.

Procedures

1. Approval under section 2 of the Policy (software, hardware or service where data is to be stored outside Canada) shall be in Form A. The employee making the purchase or request for services shall submit a completed Form A to the responsible Vice-President for signature. No purchase or service request shall be completed until Form A has been signed.

2. Approval under section 3 of the Policy (maintenance or troubleshooting services where personal information is to be accessed from outside Canada) shall be in Form B. The employee making the purchase shall submit a completed Form B to the responsible Vice-President for signature. No purchases or service request shall be completed until Form B has been signed.

POLICY FOR THE PROTECTION OF PERSONAL INFORMATION AGAINST INTERNATIONAL DISCLOSURE

FORM A – APPROVAL TO PURCHASE SOFTWARE, HARDWARE, OR SERVICES THAT STORE, HOUSE OR BACK-UP PERSONAL INFORMATION OUTSIDE CANADA

Indicate what type of personal information the product will be used to house, store or back-up (check all that apply):

- Name, address, telephone, email (personal, not business)
- Race, ethnic origin or religious political beliefs or associations
- Age, sex, sexual orientation, marital status or family status
- Any identifying number or symbol (examples: Dalcad ID, SIN, credit card, health insurance, drivers' licence)
- Fingerprints, blood type, or inheritable characteristics
- Medical or personal history
- Educational, financial, criminal or employment history
- Personal views or opinions

PLEASE NOTE: If the above information is not linked to an identifiable individual then approval is not necessary.

Name of company/firm and name of international affiliations:

(Give the full name of the company, place of operation(s), whether owned or part of an international group of companies – you should ask the company/firm for this information)

Product/service name and purpose/function:

(Give the name of the product or service and briefly describe its purpose.)

University program, operation, activity or research project:

(Describe the program, operation, activity or research project that the product or service is to support and what value it adds to that program, operation, activity or research project. In the case of research projects, please indicate whether ethics approval has been granted and provide protocol number.)

Other similar products or services available in Canada? Yes ___ No ___

If no, describe the process undertaken to support this conclusion:

If yes, why is this product superior?

(Please address comparative cost, range of service, functionality, other relevant factors)

What security measures are proposed to protect the personal information?

(Provide details concerning the security of the system as well as contractual measures taken to protected against or reduce unnecessary access to personal information)

Has the contract been reviewed by Legal Counsel Office? Yes ___ No ___

Name:

Department:

Department Approval:

Faculty approval (for academic units only):

University Approval:

Vice-President

POLICY FOR THE PROTECTION OF PERSONAL INFORMATION AGAINST INTERNATIONAL ACCESS

FORM B – APPROVAL TO PURCHASE MAINTENANCE OR TROUBLESHOOTING AGREEMENT PERMITTING REMOTE ACCESS FROM OUTSIDE CANADA

Indicate what type of personal information that the underlying software stores
(Check all that apply):

- Name, address, telephone, email (personal, not business)
- Race, ethnic origin or religious political beliefs or associations
- Age, sex, sexual orientation, marital status or family status
- Any identifying number or symbol (examples: Dalc card ID, SIN, credit card, health insurance, drivers' licence)
- Fingerprints, blood type, or inheritable characteristics
- Medical or personal history
- Educational, financial, criminal or employment history
- Personal views or opinions

PLEASE NOTE: If the above information is not linked to an identifiable individual then approval is not necessary.

Name of company/firm and name of international affiliations:

(Give the full name of the company, place of operation(s), whether owned or part of an international group of companies – you should ask the company/firm for this information)

Service-provider function:

(Give the name of the service-provider and briefly describe what product or service the service-provider is to support)

University program, operation, activity or research project:

(Identify the University program, operation, activity or research project that is being supported by the product or service that is to be serviced under the proposed arrangement. In the case of research projects, please indicate whether ethics approval has been granted and provide protocol number.)

Other services for this product available from within Canada? Yes ___ No ___

If no, describe the process undertaken to support this conclusion:

If yes, why is the underlying product superior?

(Please address comparative cost, range of service, functionality, other relevant factors)

What security measures are proposed to protect the personal information?

(Provide details concerning the security of the system as well as contractual measures taken to protected against or reduce access to personal information)

Has the contract been reviewed by Legal Counsel Office? Yes ___ No ___

Name:

Department:

Department Approval:

University Approval:

Vice-President