ÉCOLE POLYTECHNIQUE MONTRÉAL

Certification Procedure for Research Involving (or Potentially Involving) IT Risks

Table of Contents

1 Identification

Title: Certification Procedure for Research Involving (or Potentially Involving) IT Risks

Person in charge: Director of Research and Innovation

This policy is intended for: the entire Polytechnique Montréal community

Approval stages

- Adopted by the Assemblée de direction on February 3, 2009 (ADD-494-334)

2 Preamble

Computer security aims to protect the confidentiality, availability and integrity of IT assets (data, systems and computer services). The growing use of computer systems in our society makes security issues increasingly important. In light of this reality, and given the fact that the design and operation of

these systems, as well as the protection of related IT assets, are an integral part of the disciplines of computer and software engineering, Polytechnique Montréal strongly encourages research in the area of IT security.

However, the university also recognizes the risks that such research projects potentially involve—for instance, projects studying malware (e.g., viruses); vulnerabilities and the exploitation of flaws in commonly used computer systems and the tools and methods used by malicious users targeting IT assets; or projects using collected data to support research on the use of real computer systems.

There are multiple risks associated with these research activities. Given the ubiquitous and increasingly complex interactions between our work and research environments and IT systems, these research activities can have operational or economic consequences, such as:

- interrupting or interfering with the smooth operation of IT infrastructure or systems belonging to Polytechnique Montréal, one of its partners or any other entity/individual;
- causing damage to IT assets (systems, data, computer services) belonging to Polytechnique Montréal, one of its partners or any other entity/individual;
- causing economic losses to the institution, one of its students, collaborators or any other entity/individual;
- affecting the availability, integrity or confidentiality of data belonging to Polytechnique Montréal or one of its employees, students, collaborators or any other entity/individual;
- damaging the reputation of Polytechnique Montréal or its partners.

3 Legal framework

Without limiting the list, the following policies, guidelines and standards may also apply:

- *Probity Policy*;[1]
- *Politique sur l'administration des fonds de recherche (policy on the administration of research funds)*;[2]
- *Policy on the Ethical Conduct of Research Involving Human Subjects*;[3]
- *Politique sur les données institutionnelles (institutional data policy)*;[4]
- *Directive concernant la gestion des documents numériques (directive for the management of digital records*;[5]
- *Guidelines for the Protection of Personal Information and the Destruction of Records*;[6]
- *Regulation Concerning the Use and Management of Computer Resources*.[7]

The policies and regulations of federal granting agencies (NSERC, SSHRC, CIHR, CFI, etc.) and their provincial counterparts (FQRNT, FQRSC, FRSQ, etc.) may also apply.

4 Objectives

This Procedure explicitly describes the principles and practices to be adopted by Polytechnique Montréal researchers who are conducting research involving (or potentially involving) risks related to the integrity and availability of IT assets. The implementation of the principles and practices set out in this document reflect Polytechnique Montréal's desire to hold its researchers to the most exacting standards of ethics, integrity and rigour, as well as its concern to maintain and preserve its reputation and credibility within the entire university community, among its partners and in the public sphere,

while maintaining the competitiveness of its research teams and the calibre of their research.

This Procedure therefore aims to:

- set out Polytechnique Montréal's expectations regarding research projects conducted under its auspices that involve (or potentially involve) IT risks;
- define the general principles underlying the Procedure and its scope, and inform the Polytechnique community of the same;
- raise awareness within the Polytechnique community regarding the importance of respecting the principles and standards set forth in this Procedure;
- specific the obligations and responsibilities of all stakeholders;
- implement a mechanism to assess projects to which this Procedure applies.

5 Definitions

IT risk: any scenario or eventuality associated with the use of computer systems (those of Polytechnique Montréal, and any other directly or indirectly related computer systems that could be affected), which could damage IT assets or compromise their confidentiality, integrity or availability

Researcher: a professor, research professional, undergraduate or graduate student, postdoctoral fellow, Polytechnique Montréal staff member, or any other person who conducts research activities at Polytechnique Montréal

Partner: includes research collaborators, industrial partners, funders and granting agencies

IT Risk Review Committee (ITRRC): The committee in charge of ensuring that potential IT risks associated with a project are controlled according to the level of risk, and that research activities comply with this Procedure

IT assets[8]: resources directly associated with a computer system: hardware or software acquired or developed by an organization, with a quantifiable value and that can be included in an inventory. IT assets include computers and peripherals, databases and the data they process; software and programs; documents related to computer systems or software and any copies (hard or soft); and data at the time of transmission.

IT infrastructure[9]: all the configuration elements used to provide IT services, including computer hardware, software, facilities, human resources, documentation and data

Computer system[10]: a group of one or several networked computers, peripherals, system software, application software and network facilities, that are coordinated in order to allow for the processing and sharing of information

Personal information: Any information concerning a natural person that allows that person to be identified[11]. Personal information includes information related to race, national or ethnic origin, colour, religion, age, family situation, education, medical history, criminal record, occupational background, numbers, symbols or any other particulars assigned only to that person, address, fingerprints, blood group, personal opinions or ideas, or the opinions or ideas of others regarding the person.

6 Scope

This Procedure applies to all research carried out or supervised by a researcher that may reasonably pose risks to the IT assets belonging to Polytechnique Montréal, one of its partners or any other entity/individual, notably research that:

- studies malware;
- studies vulnerabilities and the exploitation of flaws in commonly used computer systems;
- studies the tools and methods used by malicious users to target these IT assets;
- uses collected data to support research on the use of real computer systems.

Note: This document does not provide a classification of IT risks. The measures taken to manage these risks must be according to the level of risk associated with each project, and will be jointly identified with the lead investigator.

7 Principles

Polytechnique Montréal recognizes the importance of the principles stated below, which mainly serve to guide researchers in their work, as well as the ITRRC in its review of a research project or activity involving (or potentially involving) IT risks. These principles are as follows:

Proportionate approach means that research projects must be managed according to the degree of risk they pose, as well as their foreseeable benefits and harms. This means that the foreseeable harms should not be greater than the anticipated benefits. In addition, a project cannot be undertaken unless the researcher has demonstrated that they have taken all necessary precautions to ensure that the research activities they carry out, or that are carried out under their supervision, do not cause harm to Polytechnique Montréal or third parties. This also means that if a project involves major IT risks, the ITRRC can demand more frequent status reports or reject the project altogether.

Respect for privacy and the protection of personal or confidential information means that researchers must respect the privacy of individuals as well as the applicable standards related to the protection of personal or confidential information, including access to and dissemination of this information.[12]

Transparency means that a researcher whose project involves (or potentially involves) IT risks is obliged to inform the institution so that the risks can be adequately managed and the people whose data the researcher would like to use are notified, or have an opportunity to refuse access to their information.

Adherence to research purpose means that any researcher whose project involves (or potentially involves) IT risks must agree to respect the purpose of the project. This is an important principle aimed at preventing inappropriate use of information as well as certain forms of abuse and deviation. This means that researchers who, in the course of a project, identify other possible uses for the information/data to which they have access must obtain authorization from the ITRRC before being able to proceed.

8 Responsibilities

The numerous and diverse responsibilities regarding the prevention of IT risks are shared by all

stakeholders in the research process.

8.1 Researchers

Although the responsibility is shared, it is important to emphasize that researchers bear the primary scientific and ethical responsibility in their choice and conduct of research activities, as do the individuals they direct, guide or supervise. Any research activity involving (or potentially involving) IT risks that is undertaken or supervised by Polytechnique Montréal researchers, must be consistent with the university's mission, must rigorously adhere to this Procedure, and must be reviewed by the ITRRC (see sections 8 and 9) before the work is started. It is therefore researchers' responsibility to develop projects that respect the principles and rules set forth in this Procedure.

A "joint responsibility" rule applies to projects conducted by undergraduate and graduate students as part of their training program. Since the professor is always responsible for supervising and guiding such projects, the latter must ensure that students submit their project proposal to the ITRRC for review. Students are bound to respect the methodological and ethical framework of the project, and to inform their research supervisor of how the work is progressing and of any difficulties encountered. Students must actively take part in preparing the proposal submitted to the ITRRC and, if applicable, should be able to defend the project before the committee (usually accompanied by their research supervisor).

8.2 IT Risk Review Committee (ITRRC)

The ITRRC is a body established by Polytechnique Montréal to review research projects that involve (or potentially involve) IT risks. Its role and composition are described in Section 9 below.

8.3 Research Ethics Board (REB)

The REB is the body established by Polytechnique Montréal to review research projects involving the use of personal information. Thus, in the case of projects to which this Procedure applies, and that require the use of personal information, the researcher must submit the project for REB review (in accordance with the *Policy on the Ethical Conduct of Research Involving Human Subjects*)[13] after obtaining approval from the ITRRC, in order to ensure that the project complies with existing standards.

8.4 Dean of Research and Innovation

The Dean of Research and Innovation is in charge of developing, applying and updating this Procedure. Any questions concerning this Procedure and its rules are submitted to the Dean, who is also responsible for disseminating and promoting the Procedure within the Polytechnique community, and keeping up to date on the latest ideas and practices in the field.

The Dean of Research and Innovation (or the Dean's designated proxy) receives all research projects submitted to the ITRRC and, on the advice of the ITRRC, issues compliance certificates for projects involving (or potentially involving) IT risks, attesting that they are compliant with existing rules. The Dean must also ensure that the ITRRC has sufficient administrative and financial support to remain operational and provide ongoing training to its members.

To appropriately manage projects involving IT risks, the Dean of Research and Innovation also undertakes to:

a. only release funds associated with any project involving (or potentially involving) IT risks once the researcher has obtained a Certificate of Approval for a Research Project Involving IT

Risks;

b. immediately suspend the researcher's access to funds associated with any research project involving (or potentially involving) IT risks if the institution learns that an ongoing project:
    i. contravenes this procedure;
    ii. violates an applicable federal or provincial law;
    iii. fails to respect any condition of approval imposed by the ITRRC;

c. rescind the suspension described in point b) above, once the contravention is rectified, to the satisfaction of the ITRRC.

9 Mandate and composition of the ITRRC

The ITRRC's mandate is to assess all research projects involving (or potentially involving) IT risks that are carried out at Polytechnique Montréal or by its researchers. The ITRRC has the authority to approve, propose changes to, terminate or reject any proposed or ongoing research that involves (or potentially involves) IT risks. Its decisions must respect this Procedure.

The ITRRC will provide as needed, before the start of the projects it approves, appropriate training for all the individuals whose research involves IT risks.

The ITRRC also has the mandate to advise and support Polytechnique Montréal researchers in the application of this Procedure and in all matters related to IT risks. For institutional reasons, Polytechnique Montréal may refuse to allow certain research within its jurisdiction, even if the ITRRC has approved the project.

The ITRRC consists of at least four members, namely:

- a professor active in research or a Polytechnique Montréal researcher working in the field of computer or software engineering. The latter cannot have a conflict of interest with the project submitted for review[14];
- the Director of the IT Department or his or her representative;
- a manager from the Office of Research / Centre for Technological Development (BRCDT) or the Research and Innovation Directorate (DRI);
- a person from the community served by Polytechnique Montréal who has no affiliation with the institution (e.g., an IT security expert from a private company or organization).

One of these individuals will act as Chair. Quorum shall consist of three members. Other members or substitute members may also be nominated if necessary. In cases of dissent, the Chair has a deciding vote. Nominations, including those of the Chair and substitute members, are made by the Assemblée de Direction, on the recommendation of Polytechnique Montréal's Dean of Research and Innovation. Terms last two or three years, so that they do not all end at the same time, and are renewable. The Dean of Research and Innovation will nominate an additional support person for the ITRRC who will act as secretary.

When the nature or scope of a project requires a level of expertise or competency that the regular ITRRC members do not have, the committee can call on experts to guide it in its deliberations. These experts can take part in the ITRRC's discussions according to rules set by the Chair, but they do not have voting rights if a vote is required.

10 Certification Procedure for Research Involving (or Potentially Involving) IT Risks

Polytechnique Montréal requires all research projects involving (or potentially involving) IT risks to be reviewed by the ITRRC before the work begins. Researchers must obtain a Certificate of Approval for a Research Project Involving IT Risks, issued by the ITRRC, confirming that the project meets the relevant institutional requirements.

10.1 Application for Certificate of Approval

The researcher must submit to the Dean of Research and Innovation (or the Dean's designated proxy) an application for a Certificate of Approval, including the following information:

1. A free-form document that:
    i. describes the research project, the risks involved (e.g., malicious code, system overload, interference with normal operation of systems, gathering of data on the network, etc.), and the measures the researcher intends to take to minimize these risks;
    ii. indicates the project funding source;
    iii. indicates the duration of the project (or sequence of experiments) and the names of the individuals involved;
    iv. indicates what data the researcher will need to have access to;
    v. indicates where and how the researcher will gather this data (e.g., will they gather the data at the entry point of the Polytechnique Montréal network, throughout the internal network or in only a portion of it?);
    vi. indicates who will have access to the data, where the data will be stored and for how long;
    vii. indicates how the data will be destroyed;
    viii. describes measures to be taken to ensure the anonymity of collected data.
2. Depending on the case, a copy of the project grant application or research contract and the reference number for the award or contract.
3. If the project involves students, research partners, visiting researchers or employees of Polytechnique Montréal or other institutions[15], a signed copy of the Declaration Form for a Research Project Involving IT Risks.

10.2 Processing of the application

Once he or she has received the application for a Certificate of Approval, the Dean of Research and Innovation sends an acknowledgement of receipt to the researcher and forwards the application to the ITRRC.

The ITRRC members first assess the relevance of the proposed project. They then assess the degree of risk posed by the project as well as foreseeable benefits and harms. The ITRRC ensures that foreseeable harms of the research do not outweigh anticipated benefits, and that the researcher has taken all the necessary precautions to prevent the research activities they will be conducting (or that will be carried out under their supervision) from causing harm to Polytechnique Montréal or to third parties. The ITRRC also ensures that the researcher has respected the applicable standards regarding the protection of personal or confidential information, including access to and dissemination of such information. Finally, the ITRRC ensures that the proposed project is compliant with this Procedure and applicable federal and provincial laws. A meeting with the lead investigator can be requested and organized by the ITRRC.

Once the ITRRC members are satisfied that the project can be carried out in complete safety, they notify the Dean of Research and Innovation, who then issues a Certificate of Approval for a Research Project Involving IT Risks that attests to the project's compliance with existing rules. The Dean issues this certificate to the researcher and sends a copy to the Office of Research / Centre for Technological Development (BRCDT).

If a project is to be carried out over several years or in several stages, and the work involving IT risks is not to be undertaken immediately, there can be a two-stage approval process. In this case, part of the funds may be released on a pro-rated basis, following an "in principle" approval of the research protocol (through a letter of agreement), up to the projected date of the work involving IT risks. In all cases, a Certificate of Approval for a Research Project Involving IT Risks must be obtained by the researcher before the research begins.

10.3 Compliance monitoring

For the duration of the project, the researcher must promptly notify the ITRRC of any changes in the research project involving IT risks. The researcher is also required to send to the Dean of Research and Innovation a brief annual status report indicating the progress of the project and any difficulties or delays, including any changes to the original project.

Polytechnique Montréal reserves the right to carry out checks at any time to ensure that the measures recommended by the ITRRC together with the lead investigator, aimed at controlling potential IT risks associated with certain projects, are being adequately applied.

10.4 End of project

The researcher must notify the Dean of Research and Innovation of the conclusion of the research project.

11 Sanctions in case of non-compliance

Polytechnique Montréal cannot accept any activity that contravenes this Procedure or its mission, notably any activity that damages its IT infrastructure; causes the loss, theft or leakage of data or intellectual property; leads to an infiltration of the institution's IT infrastructure through malicious code that is intentionally or inadvertently introduced; leads to a system overload, etc.

Consequently, in cases of non-compliance with this Procedure or any law, regulation, standard, policy or guideline applicable to research involving (or potentially involving) IT risks, notably the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, Polytechnique Montréal can immediately suspend payments of research funds associated with the project or can take any other required measure, depending on the seriousness of the breach.

12 Minor amendment

Minor amendments to this Procedure can be made by the Dean of Research and Innovation, who will inform the Assemblée de direction of the same.

13 Effective date

This Procedure is effective from the time it is approved by the Assemblée de direction.

A1 - Appendix 1

List of questions to help researchers determine whether this Procedure applies to their project

Any person to whom this Procedure is addressed, who answers “Yes” to a question in the following list, must submit their research project to the ITRRC for approval:

1. Is your research project likely to cause damage to the IT assets (systems, data and computer services) belonging to Polytechnique Montréal, one of its partners or to any other entity/individual, and thus result in economic losses to Polytechnique Montréal, one of its partners or any other entity/individual, or damage the reputation of Polytechnique Montréal or one of its partners?
2. Does your research project involve an intense use of Polytechnique Montréal’s IT infrastructure (network, servers, etc.) that might affect the performance, availability or integrity of Polytechnique’s IT assets (systems, data and computer services)—for example, research activities involving network computing, computationally intensive calculations, intensive downloading of data, etc.)?
3. Does your research project involve the generation of electromagnetic signals or radio frequencies likely to damage Polytechnique Montréal’s IT assets (systems, data and computer services)?
4. Does your research project involve gathering data to support research on the use of real computer systems?
5. Is your research project focused on the study of malware (e.g., viruses)?
6. Does your research project involve the study of vulnerabilities or the exploitation of flaws in commonly used computer systems?
7. Does your research project involve the study of tools and methods used by malicious users targeting these IT assets?

A2 - Appendix 2

Declaration form for students involved in a research project involving (or potentially involving) IT risks

To ensure the protection of its IT assets and those of its collaborators, as well as the confidentiality and integrity of data to which its students may have access as part of a research project, Polytechnique Montréal requires **all students** involved in a research project involving (or potentially involving) IT risks, that will be carried out at or use the resources of Polytechnique Montréal, to sign this form.

This statement is one of a series of measures designed to safeguard the Polytechnique community, its collaborators and the general public against any IT risks that might result from a research project carried out by the individuals to whom the Certification Procedure for Research Involving (or Potentially Involving) IT Risks applies.

I, the undersigned, _____(LAST NAME, FIRST NAME) declare that I have read the Certification Procedure for Research Involving (or Potentially Involving) IT Risks, and I hereby agree:

1. to respect the confidentiality of the information to which I have special access as part of my research project titled "_____" (TITLE), under the supervision of Dr. _____(LAST NAME, FIRST NAME of professor);
2. to use the data, tools or IT assets belonging to Polytechnique Montréal to which I have special access solely for the purposes described in my research project;
3. to refrain from using the data, tools or IT assets belonging to Polytechnique Montréal to which I have special access in any way that could harm Polytechnique Montréal, its collaborators, its employees (or others), or their property or reputation, or the general public;
4. to refrain from using my access to confidential information and to Polytechnique Montréal's IT assets, or my technical experience, or other authorizations I might be granted for any purposes other than meeting the objectives of my research project;
5. to not hesitate to ask my professor for assistance or advice if I encounter a problem that exceeds my knowledge or capabilities;
6. to carry out my research activities in an honest manner and to ensure that I do not put my personal interests before those of Polytechnique Montréal users, employees and collaborators, and of the general public;
7. to inform my professor of any situation that could place me in a conflict of interest or the appearance of a conflict of interest;
8. to not engage in illegal activities (e.g., theft, data tampering, data corruption, spreading of viruses or confidential information on individuals) and to report to my professor any disruptive event of this nature that might come to my attention during my research activities. Depending on the events observed, the professor will inform the IT security officer, who will take whatever measures are required;
9. to inform my professor of any event that could make Polytechnique Montréal's IT assets vulnerable;
10. to never use the knowledge or skills acquired during my research project for illegal activities or activities that could put the public in danger, even once the project has been completed.

_____

(Signature)

I have been provided with a copy of the Certification Procedure for Research Involving (or Potentially Involving) IT Risks.

I understand that failure to comply with this Procedure could result in disciplinary measures, including expulsion and eventual legal proceedings.

_____

(Signature)

A3 - Appendix 3

Declaration form for research partners, visiting researchers, Polytechnique Montréal employees or others[16] involved in a research project involving (or potentially involving) IT risks

With a view to protecting its IT assets and those of its collaborators, and ensuring the confidentiality and integrity of data to which certain individuals (e.g., research partners, visiting researchers, university employees or others) may have access during the course of their research Polytechnique Montréal requires that this form be signed by anyone participating in a research project involving (or

potentially involving) IT risks, that is to be carried out at the university or make use of its resources.

This statement is part of a set of measures designed to safeguard the Polytechnique community, its collaborators and the general public against any IT risks potentially resulting from a research project carried out by individuals to whom the Certification Procedure for Research Involving (or Potentially Involving) IT Risks is addressed.

I, the undersigned, _____(LAST NAME, FIRST NAME) declare that I have read the Certification Procedure for Research Involving (or Potentially Involving) IT Risks, and I hereby undertake:

1. to respect the confidentiality of information to which I have special access as part of the research project titled " _____" (TITLE), under the supervision of professor (LEAD INVESTIGATOR) _____(LAST NAME, FIRST NAME) in which I will be participating as _____ (POSITION HELD);
2. to use Polytechnique Montréal data, tools or IT assets to which I have access solely for the purposes described in the research project indicated above;
3. to refrain from using the data, tools or IT assets belonging to Polytechnique Montréal to which I have special access in any way that could harm Polytechnique Montréal, its collaborators, its employees (or others), or their property or reputation, or the general public;
4. to refrain from using my access to confidential information and to Polytechnique Montréal's IT assets, or my technical experience, or other authorizations I might be granted for any purposes other than meeting the objectives of the research project mentioned above;
5. to not hesitate to ask the lead investigator for assistance or advice if I encounter a problem that exceeds my knowledge or capabilities;
6. to carry out my research activities in an honest manner and to ensure that I do not put my personal interests before of those of Polytechnique Montréal users, employees and collaborators, and of the general public;
7. to inform the lead investigator of any situation that could put me in a conflict of interest or the appearance of a conflict of interest;
8. to not engage in any illegal activities (e.g., theft, data hampering, data corruption, spreading of viruses or confidential information on individuals), and to report to the lead investigator any disruptive event of this nature that might come to my attention during my research activities. Depending on the events observed, the lead investigator will inform the IT security officer, who will take whatever measures are required;
9. inform the lead investigator of any event that could make Polytechnique Montréal's IT assets vulnerable;
10. to never use the knowledge or skills acquired during the abovementioned research project for illegal activities or activities that could harm or put the general public in danger, even once the project has been completed.

_____

(Signature)

I have been provided with a copy for the Certification Procedure for Research Activities Involving (or Potentially Involving) IT Risks.

I understand that failure to comply with this Procedure could result in disciplinary measures, including

expulsion and eventual legal proceedings.

_____

(Signature)

N Endnotes

[1] http://www.polymtl.ca/sg/docs_officiels/en/1310prob.htm
[2] http://www.polymtl.ca/sg/docs_officiels/1310fore.htm#2
[3] http://www.polymtl.ca/sg/docs_officiels/1310hum3.php
[4] http://www.polymtl.ca/sg/docs_officiels/1310donn.htm
[5] http://www.polymtl.ca/sg/docs_officiels/1312gdn1.htm
[6] http://www.polymtl.ca/sg/docs_officiels/en/1312prot2.php
[7] http://www.polymtl.ca/sg/docs_officiels/1310rei2.htm
[8] Definition of the Office de la Langue Française du Québec (OLFQ)
[9] Definition of the Office de la Langue Française du Québec (OLFQ)
[10] Definition of the Office de la Langue Française du Québec (OLFQ)
[11] R.S.Q., c. P-39.1, 1993, c. 17, s.2.
[12] Here we are referring to, among others, the *Guidelines for the Protection of Personal Information and the Destruction of Records* (http://www.polymtl.ca/sg/docs_officiels/en/1312prot2.php) and the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information.*
[13] http://www.polymtl.ca/sg/docs_officiels/1310hum3.php
[14] When an ITRRC member has a personal interest in a project submitted to the ITRRC for review, he or she must notify the other members. In such cases, the Dean of Research and Innovation will appoint another professor active in research or a Polytechnique Montréal researcher who is working in an applicable field.
[15] When such individuals are not Polytechnique Montréal students.
[16] When such individuals are not Polytechnique Montréal students.