Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques

Table des matières

1 Identification

Titre : Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques

Responsable : le directeur de la recherche, de l'innovation et des affaires internationales

Cette politique s'adresse à : toute la communauté de l'École Polytechnique.

Approbations

- Adoptée par l'Assemblée de direction le 3 février 2009 (ADD-494-334)

2 Préambule

La sécurité des systèmes informatiques vise à protéger les biens informatiques, qu'il s'agisse de données, de systèmes ou de services informatiques, et ce, tant au niveau de la confidentialité, que de la disponibilité et de l'intégrité. L'utilisation croissante des systèmes informatiques dans notre société fait en sorte que les enjeux concernant la sécurité de ces systèmes prennent une place de plus en plus importante. De ce fait, et étant donné que la conception et l'opération de ces systèmes, ainsi que la protection des biens informatiques qui y sont associés, font partie intégrante notamment des

disciplines du génie informatique et du génie logiciel, l'École Polytechnique ne peut qu'encourager la poursuite de travaux de recherche dans le domaine de la sécurité des systèmes d'information.

Cependant, elle reconnait aussi les risques que ce type de travaux peut comporter. C'est notamment le cas des projets de recherche portant sur l'étude de programmes informatiques malveillants (ex. virus), l'étude des vulnérabilités et l'exploitation des failles de systèmes informatiques communément utilisés, l'étude des outils et méthodes utilisés par les acteurs malveillants qui visent ces biens informatiques, ou encore l'utilisation de données recueillies afin de supporter des recherches sur l'utilisation de systèmes informatiques réels.

Les risques associés à ces activités de recherche sont multiples. En effet, étant donné l'ubiquité et les interactions toujours plus complexes entre nos environnements de travail et de recherche et les systèmes informatiques, ces activités de recherche peuvent avoir des conséquences d'ordre opérationnel ou économique, notamment :

- interrompre ou nuire au bon fonctionnement de l'infrastructure ou des systèmes informatiques de l'École Polytechnique, de l'un de ses partenaires ou de toute autre entité/individu ;
- causer des dommages aux biens informatiques (systèmes, données, services informatiques) de l'École Polytechnique, de l'un de ses partenaires ou de toute autre entité/individu;
- faire encourir des pertes économiques à l'établissement, un de ses étudiants, collaborateurs ou toute autre entité/individu;
- porter atteinte à la disponibilité, à l'intégrité, ou à la confidentialité des données de l'École Polytechnique, d'un de ses employés, étudiants, collaborateurs ou de toute autre entité/individu;
- nuire à la réputation de l'École Polytechnique ou de ses partenaires.

---

3 Cadre juridique

Sans vouloir restreindre l'énumération, les politiques, directives et normes suivantes peuvent également s'appliquer :

- la *Politique en matière de probité*;[1]
- la *Politique sur l'administration des fonds de recherche*;[2]
- la *Politique sur l'éthique de la recherche avec des sujets humains*;[3]
- la *Politique sur les données institutionnelles*;[4]
- la *Directive concernant la gestion des documents numériques*;[5]
- la *Directive concernant la protection des renseignements personnels et la destruction de documents*;[6]
- le *Règlement concernant l'utilisation et la gestion des ressources informatiques*.[7]

Les politiques et règlements des organismes de subventionnaires fédéraux (CRSNG, CRSH, IRSC, FCI, etc.) et provinciaux (FQRNT, FQRSC, FRSQ, etc.) peuvent également s'appliquer.

---

4 Objectifs

La présente procédure décrit de façon explicite les principes et les pratiques que l'École Polytechnique souhaite promouvoir auprès de ses chercheurs qui mènent des travaux de recherche comportant ou pouvant comporter des risques informatiques reliés à l'intégrité et la disponibilité des biens informatiques. La mise en oeuvre des principes et pratiques qui sont énoncés dans ce document traduit la volonté de l'École Polytechnique d'imposer à ses chercheurs les plus hauts standards d'éthique, d'intégrité et de diligence, mais également son souci de maintenir et de promouvoir sa respectabilité et sa crédibilité auprès de l'ensemble de la communauté universitaire, de ses partenaires et du public en général, tout en maintenant la compétitivité de ses équipes de recherche et le calibre des travaux menés par celles-ci.

La présente procédure vise par conséquent à :

- décrire les attentes de l'École Polytechnique concernant la conduite de projets comportant ou pouvant comporter des risques informatiques menés au sein de l'établissement;
- définir des principes généraux qui sous-tendent la Procédure et son champ d'application et en informer la communauté polytechnicienne;

- sensibiliser et former la communauté polytechnicienne à l'importance du respect de ces principes et des normes qui en découlent;
- préciser les obligations et les responsabilités des intervenants concernés;
- mettre en place un mécanisme d'évaluation des projets visés par la présente procédure.

5 Définitions

Risque informatique : tout scénario ou éventualité associé à l'utilisation de systèmes informatiques (ceux de l'École Polytechnique mais également tout autre système informatique qui y serait relié directement ou indirectement et qui pourrait de ce fait être affecté) qui pourrait causer des dommages aux biens informatiques ou affecter leurs propriétés pertinentes de confidentialité, d'intégrité ou de disponibilité.

Chercheur : tout professeur[8], professionnel de recherche, étudiant de 1er, 2e ou 3e cycle, stagiaire postdoctoral, membre du personnel de l'École Polytechnique ou toute personne qui y mène des activités de recherche.

Partenaire : comprend notamment les collaborateurs de recherche, les partenaires industriels, les bailleurs de fonds et les organismes subventionnaires.

Comité d'évaluation des risques informatiques (CÉRI) : le comité responsable de s'assurer que les risques informatiques que peuvent comporter un projet de recherche soient encadrés en fonction du niveau de risque qu'ils représentent et que les travaux de recherche soient réalisés conformément à la présente procédure.

Biens informatiques[9] : ressource informationnelle directement associée au système informatique, qu'elle soit matérielle ou logicielle, acquise ou développée par une organisation, ayant une valeur quantifiable et qui peut faire l'objet d'un inventaire. Sont considérés comme des biens informatiques les ordinateurs et leurs périphériques, les bases de données et les données qu'elles gèrent, les logiciels et les programmes, les documents relatifs aux systèmes informatiques ou aux logiciels, leurs copies, qu'elles soient tangibles ou non, et enfin, les données au moment de leur transmission.

Infrastructure informatique[10] : ensemble des éléments de configuration utilisés dans la prestation des services des technologies de l'information, qui comprend le matériel informatique, les logiciels, les installations, les ressources humaines, la documentation et les données.

Système informatique[11] : ensemble composé d'un ou de plusieurs ordinateurs en réseau, des périphériques, du logiciel d'exploitation, des logiciels d'application et des installations de réseau, coordonné de manière à permettre le traitement et l'échange d'information.

Renseignement personnel : tout renseignement qui concerne une personne physique et qui permet de l'identifier[12]. Par renseignement personnel on entend notamment, les renseignements relatifs à la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, la situation familiale d'un individu, les renseignements relatifs à son éducation, son dossier médical, son casier judiciaire, ses antécédents professionnels, tout numéro, symbole ou toute autre indication identificatrice qui lui est propre, son adresse, ses empreintes digitales, son groupe sanguin, ses opinions ou ses idées personnelles, les idées ou opinions d'autrui sur lui.

6 Champ d'application

La présente procédure s'applique à toute recherche menée ou supervisée par un chercheur dont l'objet de la recherche peut raisonnablement comporter des risques informatiques pour les biens informatiques de l'École Polytechnique, de l'un de ses partenaires ou de toute autre entité/individu et portant notamment sur:

- l'étude de programmes informatiques malveillants;
- l'étude des vulnérabilités et l'exploitation des failles de systèmes informatiques communément utilisés;
- l'étude des outils et méthodes utilisés par les acteurs malveillants qui visent ces biens informatiques;
- l'utilisation de données recueillies afin de supporter des recherches sur l'utilisation de systèmes informatiques réels.

Note : Aucune classification des risques informatiques n'est proposée ici. Les mesures prises pour encadrer ces risques devront être fonction du niveau de risque associé à chaque projet et seront identifiées conjointement avec le chercheur responsable du projet.

---

7 Principes

L'École Polytechnique reconnait l'importance des principes énoncés ci-dessous qui servent principalement à guider les chercheurs dans la conduite de leurs travaux de recherche ainsi que le CÉRI dans l'évaluation d'un projet ou d'une activité de recherche comportant ou pouvant comporter des risques informatiques. Ces principes sont les suivants :

La proportionnalité signifie que les projets de recherche sont encadrés en fonction du risque qu'ils représentent ainsi que des avantages et inconvénients prévisibles de la recherche. Cela signifie notamment que les inconvénients prévisibles ne devraient pas être plus importants que les avantages escomptés. Par ailleurs, un projet ne peut être entrepris à moins que le chercheur n'ai démontré qu'il a pris toutes les précautions nécessaires pour éviter que les activités de recherche qu'il mène ou qui sont menées sous sa supervision ne causent de dommages à l'École Polytechnique ou à des tiers. Cela signifie également que si un projet comporte des risques informatiques importants, le CÉRI peut exiger des rapports d'étapes plus fréquents ou s'opposer à ce qu'il soit entrepris.

Le respect de la vie privée et la protection des renseignements personnels ou confidentiels signifient que les chercheurs doivent respecter la vie privée des personnes ainsi que les normes applicables relativement à la protection des renseignements personnels ou confidentiels dont, notamment, l'accès à ces renseignements ainsi que leur diffusion.[13]

La transparence signifie que tout chercheur dont le projet de recherche comporte ou peut comporter des risques informatiques a l'obligation d'en informer l'établissement afin que les risques qu'il comporte puissent être encadrés adéquatement et que les personnes dont il souhaite utiliser les données en soient averties ou aient l'opportunité de refuser l'accès à leur information.

Le respect des finalités signifie que tout chercheur dont le projet de recherche comporte ou peut comporter des risques informatiques doit s'engager à respecter les finalités explicitées dans celui-ci. Le respect des finalités est un principe important qui vise à prévenir tout détournement d'usage ainsi que certaines formes d'abus et de dérives. Cela signifie notamment que le chercheur qui identifie en cours de projet d'autres utilisations possibles des renseignements/données auxquels il a accès, devra au préalable obtenir l'autorisation du CÉRI à cet effet.

---

8 Responsabilités

Les nombreuses et diverses responsabilités en matière de prévention des risques informatiques sont partagées par l'ensemble des intervenants concernés par le processus de recherche.

8.1 Les chercheurs

Bien que la responsabilité soit partagée, il convient de réaffirmer la primauté de la responsabilité scientifique et éthique du chercheur dans le choix et la conduite de ses travaux de recherche, et de celle des personnes qu'il dirige, encadre ou supervise. L'École Polytechnique exige toutefois que toute activité de recherche conduite ou supervisée par ses chercheurs, et comportant ou pouvant comporter des risques informatiques, soit cohérente avec la mission de l'École Polytechnique, qu'elle respecte rigoureusement la présente procédure et qu'elle fasse l'objet d'une évaluation par son CÉRI (voir sections 8 et 9) avant d'être entreprise. Les chercheurs ont donc la responsabilité d'élaborer des projets de recherche qui respectent les principes et règles énoncés dans la présente procédure.

Une règle de « responsabilité conjointe » s'applique aux projets réalisés par les étudiants de 1er, 2e et 3e cycles dans le cadre de leur programme de formation. D'une part, la responsabilité de la direction et de l'encadrement d'un tel projet incombant toujours à un professeur, c'est donc au professeur de s'assurer que son étudiant soumette son projet pour évaluation par le CÉRI. D'autre part, l'étudiant doit s'engager à respecter le cadre méthodologique et éthique du projet, à informer son Directeur de recherche du déroulement des travaux de recherche et de toute difficulté rencontrée dans la conduite du projet. L'étudiant devrait participer activement à la préparation du dossier destiné au CÉRI et devrait, le cas échéant, être en mesure d'en débattre devant ce comité (normalement avec son Directeur de recherche).

8.2 Le Comité d'évaluation des risques informatiques (CÉRI)

Le CÉRI est l'instance mise sur pied par l'École Polytechnique pour procéder à l'évaluation des projets de recherche comportant ou pouvant comporter des risques informatiques. Son rôle et sa composition sont précisés à la section 9.

8.3 Le Comité d'éthique de la recherche (CÉR)

Le CÉR est l'instance mise sur pied par l'École Polytechnique pour procéder à l'évaluation des projets de recherche impliquant notamment l'utilisation de renseignements personnels. Par conséquent, dans le cas des projets visés par la présente procédure et qui nécessitent l'utilisation de renseignements personnels, le chercheur a l'obligation de faire évaluer son projet par le CÉR (conformément à la *Politique sur l'éthique de la recherche avec des sujets humains*)[14] suite à son approbation par le CÉRI, et ce afin de s'assurer que celui-ci réponde aux normes en vigueur.

8.4 Le Directeur de la recherche, de l'innovation et des affaires internationales

Le Directeur de la recherche, de l'innovation et des affaires internationales a la responsabilité de l'élaboration, de l'application et des mises à jour de la présente procédure. Toute question relevant de la présente procédure et des règles afférentes lui sont soumises. Il lui appartient également d'en assurer la diffusion et la promotion auprès de la communauté polytechnicienne et de se tenir au courant de l'évolution des idées et des pratiques en ce domaine.

Le Directeur de la recherche, de l'innovation et des affaires internationales (ou la personne qu'il désigne) reçoit tous les projets de recherche à soumettre au CÉRI et émet les certificats de conformité pour les projets de recherche comportant ou pouvant comporter des risques informatiques, qui attestent de la conformité du projet avec les règles en vigueur, sur avis du CÉRI. Il est également responsable du soutien administratif et financier nécessaire au fonctionnement du CÉRI et de la formation continue de ses membres.

Afin d'encadrer convenablement les projets comportant des risques informatiques, le Directeur de la recherche, de l'innovation et des affaires internationales s'engage également à :

a. ne rendre disponible aux chercheurs les fonds associés à tout projet comportant ou pouvant comporter des risques informatiques que suite à l'obtention d'un *Certificat d'acceptation d'un projet de recherche comportant des risques informatiques*;
b. bloquer immédiatement l'accès du chercheur aux fonds associés à tout projet comportant des risques informatiques si l'établissement découvre qu'un projet de recherche en cours :
    i. enfreint la présente procédure;
    ii. viole une loi ou un règlement fédéral/provincial applicable;
    iii. ne respecte pas les conditions d'approbation imposées par le CÉRI;
c. annuler la suspension, telle que décrite au point b) ci-dessus, une fois que l'infraction a été corrigée à la satisfaction du CÉRI.

---

9 Mandat et composition du CÉRI

Le CÉRI a pour mandat d'évaluer tous les projets comportant ou pouvant comporter des risques informatiques menés à l'École Polytechnique ou par ses chercheurs. Le CÉRI a le pouvoir d'approuver, de modifier, de mettre fin ou de refuser toute proposition ou poursuite de projet de recherche comportant ou pouvant comporter des risques informatiques. Ses décisions doivent respecter la présente procédure.

Le CÉRI fournit également au besoin, et ce avant le début des projets qu'il approuve, une formation appropriée à toutes les personnes dont les travaux de recherche comportent des risques informatiques.

Le CÉRI a également le mandat de conseiller et de soutenir les chercheurs de l'École Polytechnique quant à l'application de la présente procédure et sur toute question touchant les risques informatiques. Pour des raisons de convenance institutionnelle, l'École Polytechnique peut décider que certaines recherches ne seront pas réalisées dans son institution et ce, indépendamment de l'approbation du projet par le CÉRI.

Le CÉRI est composé d'au moins quatre (4) membres, à savoir :

- un professeur actif en recherche ou chercheur de l'École Polytechnique oeuvrant dans le domaine du génie informatique ou du génie logiciel. Celui-ci ne peut être en conflit d'intérêts avec le projet soumis pour évaluation[15];

- le Directeur du Service informatique ou son représentant;
- un gestionnaire du Bureau de la recherche et Centre de développement technologique (BRCDT) ou de la Direction de la recherche, de l'innovation et des affaires internationales (DRIAI);
- une personne provenant de la collectivité desservie par l'École Polytechnique mais qui n'y est pas affiliée; par exemple, un expert en sécurité informatique d'une entreprise ou d'un organisme.

L'une de ces personnes assure la présidence. Le quorum est de trois membres. D'autres membres ou des membres suppléants peuvent également être nommés au besoin. En cas de dissension, le vote du président est prépondérant. Les nominations, incluant celle du président et des membres suppléants, sont faites par l'Assemblée de direction, sur recommandation du Directeur de la recherche, de l'innovation et des affaires internationales. Les mandats sont d'une durée de deux ou trois ans, afin qu'ils ne viennent pas tous à échéance en même temps. Les mandats sont renouvelables. Le Directeur de la recherche, de l'innovation et des affaires internationales nomme une personne additionnelle en soutien au CÉRI qui agit à titre de secrétaire.

Par ailleurs, lorsque la nature ou l'ampleur d'un projet requiert une expertise ou une compétence que les membres du CÉRI n'ont pas, le CÉRI peut faire appel à toute autre personne dont il jugera l'intervention utile pour aider le CÉRI dans sa réflexion. Ces experts peuvent participer aux débats du CÉRI selon les règles que fixe le président, mais elles n'ont pas de droit de vote lorsqu'un tel vote est requis.

---

10 Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques

L'École Polytechnique exige que tous les projets de recherche comportant ou pouvant comporter des risques informatiques fassent l'objet d'une évaluation par le CÉRI avant le début des travaux. Pour ce faire, les chercheurs doivent obtenir un *Certificat d'acceptation d'un projet de recherche comportant des risques informatiques*, délivré par le CÉRI, qui atteste que le projet répond aux exigences de l'établissement en la matière.

10.1 Demande de conformité

Le chercheur a l'obligation de soumettre au Directeur de la recherche, de l'innovation et des affaires internationales (ou la personne qu'il désigne) une demande de conformité qui comprend les renseignements suivants :

1. Un document en forme libre qui :
    i. Décrit le projet de recherche, les risques (ex. codes malicieux, surcharge des équipements, nuisance au fonctionnement des systèmes, collecte de données sur le réseau etc.) qu'il comporte et les précautions que le chercheur entend prendre pour les minimiser;
    ii. Précise la source de financement du projet de recherche;
    iii. Précise la durée du projet (ou la séquence des expériences) et le nom des personnes impliquées;
    iv. Spécifie à quelles données le chercheur aura besoin d'avoir accès;
    v. Précise où et comment le chercheur recueillera ces données (par exemple, le chercheur recueillera-t-il ces données à l'entrée du réseau de l'École Polytechnique, sur tout le réseau interne ou seulement sur une portion de celui-ci ?);
    vi. Précise qui aura accès aux données, où ces données seront conservées et pour combien de temps;
    vii. Précise comment les données seront détruites;
    viii. Décrit les moyens qui seront pris pour assurer l'anonymat des données recueillies.
2. Selon le cas, une copie de la demande de subvention ou du contrat de recherche pour le projet, et le numéro de référence de l'octroi ou du contrat.
3. Si le projet implique des étudiants, des associés de recherche, chercheurs invités, employés de l'École Polytechnique ou autres[16], le formulaire de déclaration pertinent pour projets de recherche impliquant des risques informatiques dûment signé.

10.2 Traitement de la demande

Dès qu'il a reçu une demande de conformité, le Directeur de la recherche, de l'innovation et des affaires internationales émet un accusé de réception au chercheur et transmet la demande de conformité aux

membres du CÉRI.

Les membres du CÉRI évaluent dans un premier temps la pertinence du projet proposé. Par la suite, ils évaluent le niveau de risque que présente le projet ainsi que les avantages et inconvénients prévisibles de la recherche. Le CÉRI s'assure notamment que les inconvénients prévisibles de la recherche ne soient pas plus importants que les avantages escomptés et que le chercheur a pris toutes les précautions nécessaires pour éviter que les activités de recherche qu'il mène ou qui sont menées sous sa supervision ne causent des dommages à l'École Polytechnique ou à des tiers. Le CÉRI s'assure également que le chercheur respecte les normes applicables relativement à la protection des renseignements personnels ou confidentiels dont, notamment, l'accès à ces renseignements ainsi que leur diffusion. Enfin, il s'assure de sa conformité avec la présente procédure ainsi que des lois et règlements fédéraux/provinciaux applicables. Une rencontre avec le chercheur responsable du projet peut être demandée et organisée par le CÉRI.

Lorsque le CÉRI est satisfait et convaincu que le projet peut se dérouler en toute sécurité, il en avise le Directeur de la recherche, de l'innovation et des affaires internationales qui émet subséquemment un *Certificat d'acceptation d'un projet de recherche comportant des risques informatiques* qui atteste de la conformité du projet avec les règles en vigueur. Il remet le certificat au chercheur ainsi qu'une copie au Bureau de la recherche et Centre de développement technologique (BRCDT).

Si un projet s'échelonne sur plusieurs années ou encore s'il se déroule en plusieurs phases et que les travaux comportant ou pouvant comporter des risques informatiques ne sont pas réalisés immédiatement, celui-ci peut être évalué dans le cadre d'un processus en deux étapes. Dans ce cas, une partie des fonds peut être libérée au prorata, après une approbation de principe du protocole de recherche (via une lettre d'entente), et ce, jusqu'à la date prévue de réalisation des travaux comportant des risques informatiques. Dans tous les cas, un *Certificat d'acceptation d'un projet de recherche comportant des risques informatiques* doit être obtenu par le chercheur avant le début des travaux.

10.3 Suivi de conformité

Pour toute la durée du projet, le chercheur a la responsabilité d'aviser sans délai le CÉRI de toute modification apportée au projet de recherche comportant des risques informatiques. Le chercheur a également l'obligation de faire parvenir au directeur de la recherche, de l'innovation et des affaires internationales un *Bref rapport annuel* faisant état du déroulement du projet, des difficultés encourues ou des retards dans le déroulement de ce dernier, incluant tout changement relatif au projet initial.

L'École Polytechnique se réserve par ailleurs le droit d'effectuer des vérifications à tout moment afin de s'assurer que les mesures préconisées par le CÉRI en collaboration avec le chercheur responsable du projet, en vue d'encadrer les risques informatiques que peuvent présenter certains projets, sont appliquées adéquatement.

10.4 Fin du projet

Le chercheur doit transmettre un avis au Directeur de la recherche, de l'innovation et des affaires internationales à la fin des travaux de recherche.

---

11 Sanctions en cas de non-respect

L'École Polytechnique ne peut accepter aucune activité qui contrevienne à la présente procédure ou à sa mission, notamment qui porte atteinte à son infrastructure informatique, cause la perte, le vol ou la fuite de données, de propriété intellectuelle, mène à l'infiltration de l'infrastructure informatique de l'institution par des codes malveillants introduits intentionnellement ou par inadvertance, surcharge ses équipements etc.

Par conséquent, en cas de contravention à la présente procédure ou à une loi, règlement, norme, procédure ou directive applicable à la recherche comportant ou pouvant comporter des risques informatiques, dont notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, l'École Polytechnique peut prendre toute mesure qui s'impose selon la gravité de la contravention commise. Notamment, l'École Polytechnique peut interrompre sans délai le versement des fonds de recherche associés au projet concerné.

---

12 Modification mineure

Toute modification mineure à la présente procédure peut être apportée par le Directeur de la recherche, de l'innovation et des affaires internationales qui en informe l'Assemblée de direction.

13 Entrée en vigueur

La présente procédure entre en vigueur dès son approbation par l'Assemblée de direction.

A1 - Annexe 1

Liste de questions destinées à aider les chercheurs à déterminer si leur projet est visé par la présente procédure

Toute personne visée par la présente procédure qui répond « oui » à une question dans la liste qui suit doit soumettre son projet de recherche pour approbation par le CÉRI :

1. Votre projet de recherche est-il susceptible de causer des dommages aux biens informatiques (systèmes, données ou services informatiques) de l'École Polytechnique, de l'un de ses partenaires ou de toute autre entité/individu, et de ce fait faire encourir des pertes économiques à l'École Polytechnique, l'un de ses partenaires ou toute autre entité/individu, ou encore nuire à la réputation de l'École Polytechnique ou de l'un de ses partenaires ?
2. Votre projet de recherche implique-t-il une utilisation intense de l'infrastructure informatique (réseau, serveurs, etc.), susceptible d'affecter la performance, la disponibilité ou l'intégrité des biens informatiques (systèmes, données et services informatiques) de l'École (ex. travaux de recherche en réseautique, calcul scientifique intensif, téléchargement intensif de données, etc.) ?
3. Votre projet de recherche implique-t-il la génération de signaux électromagnétiques ou radiofréquence susceptible de nuire aux biens informatiques (systèmes, données et services informatiques) de l'École Polytechnique ?
4. Votre projet de recherche recueille-t-il des données afin de supporter des recherches sur l'utilisation de systèmes informatiques réels.
5. Votre projet de recherche porte-t-il sur l'étude de programmes informatiques malveillants (ex. virus) ?
6. Votre projet de recherche porte-t-il sur l'étude des vulnérabilités ou l'exploitation des failles de systèmes informatiques communément utilisés ?
7. Votre projet de recherche porte-t-il sur l'étude des outils et méthodes utilisés par les acteurs malveillants qui visent ces biens informatiques ?

A2 - Annexe 2

Formulaire de déclaration pour étudiants impliqués dans un projet de recherche comportant ou pouvant comporter des risques informatiques

L'École Polytechnique, dans l'optique d'assurer la protection de ses biens informatiques de même que ceux de ses collaborateurs ainsi que la confidentialité et l'intégrité des données auxquelles peuvent avoir accès ses étudiants dans le cadre d'un projet de recherche, demande à ce que **tout étudiant** impliqué dans un projet de recherche comportant ou pouvant comporter des risques informatiques, se déroulant ou utilisant les ressources de l'École Polytechnique signe le présent formulaire.

Cette attestation s'inscrit dans un ensemble de mesures destinées à assurer la protection de la communauté polytechnicienne, de ses collaborateurs ainsi que du public en général, contre tout risque informatique pouvant découler d'un projet de recherche mené par les personnes visées par la *Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques*.

Je soussigné(e) _____(NOM, prénom) déclare avoir lu la *Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques* et m'engage par la présente à :

1. respecter la confidentialité de l'information à laquelle j'ai accès de façon privilégiée dans le cadre de mon projet de recherche intitulé « _____ » (TITRE), sous la supervision du professeur _____(NOM, PRÉNOM);
2. ne me servir des données, outils ou bien informatiques de l'École Polytechnique auxquels j'ai accès uniquement aux fins décrites dans mon projet de recherche;
3. ne me servir des données, outils ou biens informatiques de l'École Polytechnique auxquels j'ai accès d'aucune manière qui puisse nuire à l'École Polytechnique, ses collaborateurs, ses employés (ou autres), leurs biens, leur réputation, ou qui puisse nuire au public en général;
4. ne pas utiliser mon accès à de l'information privilégiée et aux biens informatiques de l'École Polytechnique, de mon expérience technique, et des autres autorisations dont je pourrais bénéficier pour des raisons autres que l'atteinte des objectifs de mon projet de recherche;
5. ne pas hésiter à demander l'assistance ou des conseils à mon professeur si je suis confronté à un problème dépassant mes compétences ou mes connaissances;
6. conduire mes travaux de recherche de façon honnête et faire en sorte de ne pas placer mes propres intérêts avant ceux des utilisateurs, employés et collaborateurs de l'École Polytechnique ainsi que du public en général;
7. informer mon professeur de toute situation qui pourrait me placer en conflit d'intérêt ou apparence de conflit d'intérêt;
8. ne pas m'engager dans des activités illégales (ex. vol, piratage de données, corruption, propagation de virus ou d'informations confidentielles sur des individus) et à rendre compte à mon professeur de tout fait dérangeant de cette nature dont je pourrais prendre connaissance dans le cadre de mes travaux de recherche. Dépendamment des faits observés, ce dernier en informera l'officier de sécurité informatique qui prendra les mesures qui s'imposent;
9. informer mon professeur de tout fait qui pourrait rendre vulnérables les biens informatiques de l'École Polytechnique;
10. ne jamais me servir des connaissances ou habiletés acquises dans le cadre de mon projet de recherche pour des activités illégales ou pouvant nuire ou mettre en danger le public, même au terme de ce projet.

_____

(Signature)

Une copie de la procédure relative à la certification des travaux de recherche présentant des risques informatiques m'a été fournie.

Je comprends qu'un manquement à cette procédure pourra entrainer des mesures disciplinaires pouvant aller jusqu'à l'expulsion et éventuellement des poursuites judiciaires.

(Signature)

A3 - Annexe 3

Formulaire de déclaration pour associés de recherche, chercheurs invités, employés de l'École Polytechnique ou autres[17] impliqués dans un projet de recherche comportant ou pouvant comporter des risques informatiques

L'École Polytechnique, dans l'optique d'assurer la protection de ses biens informatiques de même que ceux de ses collaborateurs ainsi que la confidentialité et l'intégrité des données auxquelles peuvent avoir accès certaines personnes (ex. associés de recherche, chercheurs invités, employés de l'École et autres) dans le cadre d'un projet de recherche, demande à ce que **toute personne** impliquée dans un projet de recherche comportant ou pouvant comporter des risques informatiques, se déroulant ou utilisant les ressources de l'École Polytechnique signe le présent formulaire.

Cette attestation s'inscrit dans un ensemble de mesures destinées à assurer la protection de la communauté polytechnicienne, de ses collaborateurs ainsi que du public en général, contre tout risque informatique pouvant découler d'un projet de recherche mené par les personnes visées par la Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques.

Je soussigné(e) _____(NOM, prénom) déclare avoir lu la *Procédure de certification des travaux de recherche comportant ou pouvant comporter des risques informatiques* et m'engage par la présente à :

1. respecter la confidentialité de l'information à laquelle j'ai accès de façon privilégiée dans le cadre du projet de recherche intitulé « _____ » (TITRE), sous la supervision du professeur (RESPONSABLE DU PROJET) _____ _____(NOM, PRÉNOM) auquel je participe à titre de _____ (FONCTION OCCUPÉE);
2. ne me servir des données, outils ou bien informatiques de l'École Polytechnique auxquels j'ai accès uniquement aux fins décrites dans le projet de recherche mentionné en rubrique;
3. ne me servir des données, outils ou biens informatiques de l'École Polytechnique auxquels j'ai accès d'aucune manière qui puisse nuire à l'École Polytechnique, ses collaborateurs, ses employés (ou autres), leurs biens, leur réputation, ou qui puisse nuire au public en général;
4. ne pas utiliser mon accès à de l'information privilégiée et aux biens informatiques de l'École Polytechnique, de mon expérience technique, et des autres autorisations dont je pourrais bénéficier pour des raisons autres que l'atteinte des objectifs du projet de recherche mentionné en rubrique;
5. ne pas hésiter à demander l'assistance ou des conseils au responsable du projet si je suis confronté à un problème dépassant mes compétences ou mes connaissances;
6. conduire mes travaux de recherche de façon honnête et faire en sorte de ne pas placer mes propres intérêts avant ceux des utilisateurs, employés et collaborateurs de l'École Polytechnique ainsi que du public en général;
7. informer le responsable du projet de toute situation qui pourrait me placer en conflit d'intérêt ou apparence de conflit d'intérêt;
8. ne pas m'engager dans des activités illégales (ex. vol, piratage de données, corruption, propagation de virus ou d'informations confidentielles sur des individus) et à rendre compte au responsable du projet de tout fait dérangeant de cette nature dont je pourrais prendre connaissance dans le cadre de mes travaux de recherche. Dépendamment des faits observés, ce dernier en informera l'officier de sécurité informatique qui prendra les mesures qui s'imposent;
9. informer le responsable du projet de tout fait qui pourrait rendre vulnérables les biens informatiques de l'École Polytechnique;
10. ne jamais me servir des connaissances ou habiletés acquises dans le cadre du projet mentionné en rubrique pour des activités illégales ou pouvant nuire ou mettre en danger le public, même au terme de ce projet.

_____

(Signature)

Une copie de la procédure relative à la certification des travaux de recherche présentant des risques informatiques m'a été fournie.

Je comprends qu'un manquement à cette procédure pourra entrainer des mesures disciplinaires pouvant aller jusqu'au congédiement immédiat et éventuellement des poursuites judiciaires.

_____

(Signature)

N Notes

1 http://www.polymtl.ca/sg/docs_officiels/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/1312prot2.php
7 http://www.polymtl.ca/sg/docs_officiels/1310rei2.htm
8 Afin d'alléger la lecture, le masculin est utilisé pour désigner toute personne sans distinction de genre
9 Définition de l'Office de la Langue Française du Québec (OLFQ)
10 Définition de l'Office de la Langue Française du Québec (OLFQ)
11 Définition de l'Office de la Langue Française du Québec (OLFQ)
12 L.R.Q., c. P-39.1, 1993, c. 17, a.2.
13 On fait référence ici, entre autres, à la *Directive concernant la protection des renseignements personnels et la destruction de documents* (http://www.polymtl.ca/sg/docs_officiels/1312prot2.php)) et à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels"*
14 http://www.polymtl.ca/sg/docs_officiels/1310hum3.php
15 Lorsqu'un membre du CÉRI a un intérêt personnel dans un projet soumis pour évaluation par le CÉRI, il doit le mentionner. Dans ce cas, le Directeur de la recherche, de l'innovation et des affaires internationales nomme un autre professeur actif en recherche ou un chercheur de l'École Polytechnique oeuvrant dans un domaine pertinent.
16 N'ayant pas le statut d'étudiant de l'École Polytechnique.
17 N'ayant pas le statut d'étudiant de l'École Polytechnique.