HEC MONTRÉAL

Information Security Policy

Adopted by the Board of Directors on November 10, 2011

Updated on: December 5, 2019

Table of Contents

Foreword

The activities of HEC Montréal largely depend on information that is processed, produced and transmitted. This information is vast and may exist on paper or on an electronic medium. It includes personal information about students and staff members, intellectual property produced by faculty and researchers, and internal and administrative strategic documentation.

Like any other institution of higher education, HEC Montréal faces a multitude of threats to its confidentiality, integrity and availability of information. These threats, whose nature is constantly evolving, include identity theft and theft of confidential information, fraud, industrial espionage and theft of intellectual property, the use, disclosure and destruction of information, technical failures, natural events and human error.

In this context, the coming into force of the *Act respecting the governance and management of information resources of public bodies and government enterprises* (L.R.Q., c. G-1.03) and the *Directive sur la sécurité de l'information gouvernementale* du Conseil du Trésor du Québec (the Quebec Treasury Board's *Directive on the security of government information*) impose obligations on academic institutions in their capacity as public bodies. In order to meet its regulatory and legislative obligations, HEC Montréal must adopt, implement, maintain and enforce an information security policy that establishes the implementation of formal information security processes to ensure particularly risk management, access management and incident management.

General Provisions

Article 1.00 Objective

1.01 This policy is one of the key elements to ensure the realization of the mission and the business objectives of the School, to maintain its reputation and to comply with the applicable legal, regulatory and contractual requirements.

1.02 The main objective of this policy is to communicate the School's determination and commitment to managing information security risks effectively and efficiently. The approach adopted is aimed at identifying the stakeholders and defining their roles, and raising user awareness of the risks of designing and implementing measures to effectively safeguard the security of information assets.

Article 2.00 Scope

2.01 Information security is everyone's concern. All natural persons (teacher, researcher, student, graduate, administrative employee, retiree and consultant), or legal persons who use or access the information resources of HEC Montréal.

2.02 This policy applies to all information that HEC Montréal holds while carrying out its functions or that it safeguards, throughout its lifecycle, regardless of the form, medium and location.

Article 3.00 Guidelines

3.01 The principles that orient the School's approach, the distribution of responsibilities and the nature of actions and means put forth are as follows:

a) Availability
The School ensures the availability of the information it holds, so this information can be

accessed in a timely fashion, and in the manner required by any authorized person. To this end, the School:

(i) Ensures the reliability of the processes, systems, and information technology that support documentation;
(ii) Ensures the continuity of services and operations, in spite of constraining and damaging events;
(iii) Provides for alternative solutions to ensure the continuity of services deemed essential as well as the restoration of services in the event of an unplanned outage;
(iv) Ensures that it has proven and continually updated and documented contingency plans.

b) Integrity
The School ensures the integrity of information so that it cannot be destroyed or altered without authorization, and so that the information medium provides appropriate stability and durability. To this end, the School:

(i) Develops technological or other means to verify, through its entire life cycle, that information vital to the School's day-to-day operations has not been altered, that it is maintained in its entirety, and that the medium supporting such information provides appropriate stability and durability.

c) Confidentiality
The School ensures that the disclosure of information is limited to those authorized to access it, thus ensuring strict confidentiality. To this end, the School:

(i) Collects and retains only that information necessary to accomplish its mission, in compliance with the *Act respecting Acess to documents held by public bodies and the Protection of personal information* (L.R.Q., c. A-2.1) and the *Archives Act* (L.R.Q., c. A-21.1);
(ii) Implements access control and profiles to ensure that only those persons, objects or technological entities identified as entitled and authorized shall have access to the information, in accordance with laws and regulations
(iii) Ensures that information, documents, equipment, or materials destined for disposal, declared as surplus property, or turned over to a service provider for maintenance, recycling, destruction, or other purposes are handled in accordance with the applicable processing and destruction procedure. In addition, documents containing out-of-date or unnecessary information shall be destroyed in accordance with the retention schedule administered by the School.

d) Accountabiity
Each Office or administrative department is responsible for managing information security risks in its capacity of information owner. This accountability applies to information assets, processes and systems under the owner's responsibility or control, including that delegated to a third party.

e) Proportionality
Reasonable measures have been put in place to guarantee the confidentiality, integrity and availability of information assets, at a cost proportionate to the sensitivity of the information and to the underlying risks; different types of information may require different levels of protection. Further, measures put in place to protect information assets must not interfere with the mission of the School.

f) Awareness
The School shall ensure that the university community is informed of risks and threats that may affect information, enabling its members to recognize potential incidents and risks and to understand their roles and responsibilities with respect to information security by developing appropriate skills and competencies.

Particular Provisions

Article 4.00 Roles and responsibilities

4.01 In this policy and its application, the following mandates are assigned to different stakeholders:

4.01.01 Board of Directors

a) Adopts the policy as well as any amendment thereto.

4.01.02 Audit Committee

a) Supervises the information security risk management process and the application of the policy;
b) Ensures the adequacy of the information security measures in effect, in relation to the risks incurred;
c) Ensures that measures are in place to reduce information security risks to a level deemed acceptable for the organization;
d) Is informed of the School's actions in the area of information security, particularly with respect to the annual information security report.

4.01.03 HEC Montréal Executive Committee

a) Validates the policy and its updates and recommends to the Audit Committee that the policy be adopted by the Board of Directors;
b) Ensures the application of the policy by the management of HEC Montréal;
c) Adopts measures to promote the application of the policy and fulfill the School's legal obligations with respect to information security;
d) Determines strategic orientation, adopts action plans and receives information security reports;
e) Appoints the Information Security Officer (ISO) as required by law;
f) Appoints Sector Incident Management Coordinators (SIMC).

4.01.04 Office of the Secretary General

a) Interprets laws and regulations that may affect information security;
b) Formulates and disseminates, in cooperation with the information security advisor and other stakeholders, policies concerning privacy, protection of personal information and information security;
c) Ensures that adequate contractual measures are foreseen in order to protect information and comply with this policy, in cooperation with the Purchasing Department and the information security advisor;

4.01.05 Information Security Committee

a) Acts as the primary forum for consultation on information security matters for the School;
b) Formulates recommendations on the management framework, action plans and reviews;
c) Formulates all proposals for action in matters of information security.

4.01.06 IT Governance Committee

a) Accepts residual risks with a high and critical level of importance;
b) Reports to HEC Montréal management on residual risks with a high and critical level of importance.

4.01.07 Information Security Officer (ISO)

a) Assists management in determining strategic orientations and intervention priorities;
b) Assists in implementation of the normative framework for information resources and risk mitigation measures;
c) Is the School's first respondent for information security;
d) Represents management of the institution in the reporting of government-wide incidents;
e) Is responsible for reporting, in compliance with legislative and regulatory requirements;
f) Has the overall responsibility of implementing this Policy.

4.01.08 Information Security Advisor

a) Formulates the information security policy and its updates, and coordinates its implementation;
b) Is involved in the implementation of information risk measures;
c) Develops and implements formal information security processes;
d) Formulates and implements the information security awareness program;
e) Produces an annual information security report.

4.01.09 Sectoral Incident Management Coordinator (SIMC)

a) Assists in implementation of the information security incident management process;
b) Maintains the log of information security incidents;
c) Contributes to information security risk analyses;
d) Manages the hierarchical and problem-solving process.

4.01.10 Information system owner

a) Ensures the accessibility, proper use, efficient management and security of information assets under his/her management;
b) Collaborates in the categorization of information under his/her responsibility and ensures the protection of this data.

4.01.11 Human Resources Department

a) Does background checks of prospective candidates before hiring and of staff members involved with information security;
b) Ensures that the responsibilities of stakeholders concerning information security and compliance with this policy. as well as the normative framework for information resources, are included in the job descriptions of staff members;
c) Informs and obtains from all new employees of the School their commitment to respect this policy;
d) Imposes appropriate sanctions when policies, rules and the code of conduct concerning information security;

4.01.12 Information Technologies Department

a) Ensures the security of information assets, throughout their lifecycle, by deploying appropriate security measures approved by the information owner;
b) Develops, integrates, and maintains safeguards appropriate to the level of sensitivity of the information concerned, as well as to other applicable business, legal, regulatory or contractual requirements, in the conduct of a development project or the acquisition of an information system.

4.01.13 Users

a) Complies with the security policy and any guidelines pertaining to information security and the use of information assets;
b) Complies with security measures in effect, without seeking to circumvent, disable or modify them.

Administrative Measures and Sanctions

Article 5.00 In the event of violation of this policy

5.01 The user shall be personally responsible for any violation of this policy, as shall be any person who, whether through negligence or omission, causes information to be inadequately protected.

5.02 Any member of the university community who violates the legal framework, this policy and information security measures stemming from it shall be subject to sanctions depending on the nature, seriousness and repercussions of the violation, under the law or applicable internal disciplinary rules.

5.03 Similarly, any violation by a supplier, partner, guest, consultant or external organization shall be subject to sanctions as stipulated by contract with the School or under the provisions of applicable legislation.

5.04 When an audit gives reason to believe that a law or regulation has been violated, the Director of Information Technology, in collaboration with the Secretary General, may also refer the file to any other competent authority in order to verify whether there are grounds for prosecution, among other things. The Director of Information Technology may then transmit to this authority any information collected during the verification or investigation.

In addition to the measures provided for in laws, regulations, policies or agreements, any violation of this policy may result in the following consequences, depending on the nature, seriousness and repercussions of the act or omission:

a) Cancellation of access privileges to the School's information assets. Such cancellation may be effected without notice depending on the nature and seriousness of the violation.
b) The obligation to reimburse the School for any amount that the latter is obliged to pay as a result of unauthorized, fraudulent, or illicit use of its services or information assets.

Final Dispositions

Article 6.00 Exceptional review

6.01 This policy shall be revised as needed, or in accordance with ongoing changes to legislative and regulatory obligations, taking into account new governmental orientations as well as the evolution of information security practises.

Article 7.00 Policy application and monitoring

7.01 The Information Security Officer is responsible for the application of this policy.

Article 8.00 Entry into force

8.01 This policy comes into effect on the date of its adoption by the Board of Directors. As of that date, it replaces the policy adopted on November 11, 2011.

Legislative and Regulatory Framework

Requirements concerning information security are found in several laws, regulations and contractual agreements applicable to HEC Montréal. Several normative documents (policies, statements, codes, guides, etc.) also impose requirements related to information security.

- Charter of Rights and Freedoms (art. 5)
- Civil Code of Québec (secs. 3, 35 to 37)
- An Act respecting access to documents held by public bodies and the Protection of personal information
- An Act respecting the governance and management of the information resources of public bodies and government enterprises
- Act to establish a legal framework for information technology (secs. 1 to 46)
- Act respecting labour standards
- Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information, à l'intention des ministères et organismes publics (art. 8) (in French only)
- Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS2), 2010 (ch. 5)
- CFI Policy and program guide, Canadian Foundation for Innovation, 2010 (Ch. 5.1.3)
- Code of conduct for HEC Montréal students (art. 1)
- HEC Montréal Rules and Regulations (BBA, Certificate, DES, Master's, MBA, Doctorate) (art. 18 and 19)
- Politique relative à la gestion des documents actifs, semi-actifs et inactifs, HEC Montréal (art. VI, E) (in French only)