HEC MONTRÉAL

Politique de sécurité de l'information

Information Security Policy

Adoptée par le Conseil d'administration

Le 10 novembre 2011

Adopted by the Board of Directors on November 10, 2011

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.

Further, the School must meet several legal, regulatory, and contractual requirements or those resulting from its own policies related to information security. Compliance with these requirements and the bond of trust that exists between the School and the members of its staff, faculty, students and the general public are essential to maintain the reputation of HEC Montréal.

It is therefore imperative that the School adequately protect the information it owns and that entrusted to it.

1. General

Objective

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.

The main objective of this policy is to convey 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.

Scope

Information security is everyone's concern. This policy applies to all users of information resources at HEC Montréal, including members of top management, senior managers, staff members, faculty, students and research assistants, along with subcontractors, suppliers and partners of HEC Montréal.

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.

Guidelines

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. Accountability

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.

b. 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.

c. Compliance

Information security risk is managed in compliance with the applicable legal, regulatory and contractual requirements and with the policies and rules of HEC Montréal.

d. Awareness

Adequate measures have been put in place to raise awareness among all users and stakeholders, engage them in protecting the information assets of the School and favor responsible use of resources.

2. Roles and responsibilities

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

Board of Directors

- Approves the policy and its updates;
- Supervises the information security risk management process, through the Audit Committee.

Audit Committee

- Recommends adoption of the policy and policy updates to the Board of Directors;
- Supervises the information security risk management process and the application of the policy;
- Reports, as needed, to the Board of Directors.

Administration

- Validates the policy and its updates and recommends to the Audit Committee that the policy be adopted by the Board of Directors;
- Ensures the application of the policy by the management of HEC Montréal;
- Ensures that the information security program has adequate financial resources and logistics.

Information security advisor

- Formulates the policy and its updates and coordinates its implementation;

- Assists departments and administrative services in evaluating and managing information security risks, while letting them attain their business objectives;
- Identifies and maintain a list of information owners;
- Provides guidelines, proposes solutions, coordinates their implementation and facilitates compliance related to information security;
- Informs the HEC community of its responsibilities concerning information security;
- Formulates and implements the information security awareness program for staff members, in cooperation with the Information Technologies Director's Office and the Human Resources Department ;
- Maintains the log of information security incidents and manages the hierarchical and problem solving process in this area;
- Follows up information security auditors' observations and recommendations;
- Acts at all times to confirm the existence or proper functioning of a security measure, and issues recommendations if the information assets of HEC Montréal are deemed to be at risk;
- Communicates risks to information security and accounts for the application of this policy to the Executive Committee;
- Takes appropriate actions following a major incident affecting information security, in cooperation with the Information Technologies Director;

Director's Office or administrative department

- Evaluates and manages risks related to information security;
- Ensures that adequate and reasonable protection measures are put in place;
- Assigns an information owner to each business process, important activity, system or information category;
- Is responsible for protection of information delegated to a third party;
- Manages contracts and relations with suppliers for all aspects concerning information security, in collaboration with the information security advisor and the Purchasing Department;
- Maintains classification of information security;
- Informs and sensitizes everyone under its direction to the importance of information security and the existence of this policy and other applicable guidelines;
- Notifies the information security advisor of any important risk to information security.

Information owner

- Acts as the coordinator designated by the administrative unit by applying the provisions of this policy;
- Classifies information security according to the guidelines and standards of HEC Montréal, and informs the information security advisor of the results;
- Establishes and periodically reviews user access profiles and transmits them to the appropriate stakeholders;
- Identifies legal, regulatory and contractual requirements applicable to information security in collaboration with the legal affairs department and the information security advisor;

- Evaluates information security risk and informs the information security advisor of the results;
- Assumes, on behalf of the administrative unit, residual risks to information security;

Human Resources Department

- Does background checks of prospective candidates before hiring and of staff members involved with information security;
- Ensures that the responsibilities of stakeholders concerning information security and compliance with this policy are included in the job descriptions of staff members;
- Supports the information security advisor during the formulation and implementation of the information security awareness program for staff members;
- Acts with staff members concerned in case of attacks on information security, in collaboration with the information security advisor and other stakeholders;
- Takes action, follows up and imposes appropriate sanctions when policies, rules and the code of conduct concerning information security are violated, in collaboration with the immediate supervisor;
- Informs stakeholders concerned about hiring, change of positions, transfers or terminations of employment of members so that access to information assets can be updated appropriately.

Legal Affairs

Under this policy, the legal affairs coordinator shall:

- Interpret laws and regulations that may affect information security;
- Inform the information security advisor, the information owner and other stakeholders, if necessary, of the applicable legal, regulatory and contractual requirements;
- Validate the contractual clauses concerning information security, in collaboration with the information security advisor;
- Ensure that adequate contractual measures are foreseen to protect information and comply with this policy, in cooperation with the Purchasing Department and the information security advisor;
- Formulate and disseminate, in cooperation with the information security advisor and other stakeholders, policies concerning privacy, protection of personal information and information security.

Document and Archives Management Department

- Assists administrative units in identifying and implementing secure information management modes;
- Puts in place adequate and reasonable security measures for management of semi-active documents, HEC Montréal archives and some private archives, in compliance with this policy;
- Ensures the secure destruction of information entrusted to it, when required by the purpose of the information or upon request by departments and administrative departments.

Security Department

- Controls physical access to School premises;

- Manages means of physical access (keys, smart cards, access codes, biometrics, etc.) and to premises with restricted access (computer rooms, archives institutional, storerooms, etc.);
- Controls circulation of equipment leaving the School premises;
- Collaborates with the information security advisor and other stakeholders in awareness activities related to information security.

Information Technologies Department

- Develops and implements guidelines, processes, standards and procedures concerning the security of information assets, notably access management, incident management and integrity of information;
- Evaluating initial risks, does periodic evaluations as needed and communicates the results to the information security advisor and to information owners;
- Ensures the security of information assets throughout their lifecycle by deploying appropriate security measures approved by the information owner;
- Develops, integrates and maintains security measures corresponding to the level of sensitivity of the information and other applicable business, legal, regulatory and contractual requirements;
- Supports the information security advisor in formulating and implementing an awareness program on information security for staff members;
- Informs the information security advisor of any important risk to information security;
- Formulates and ensures compliance with the code of ethics for all employees specializing in information technology, notably developers and network administrators.

Users

- Read and comply with policies, rules, code of conduct and other pertinent guidelines on information security at HEC Montréal that concern them;
- Get informed and actively participate in implementing the policy;
- Use information assets strictly for the purposes for which they are intended and within the access rights granted to them.

3. Definitions

For the application of this policy:

Information asset

Information in the strict sense, regardless of the medium where it is situated, and the systems used for its processing, usage, storage, retention and communication. The loss, theft or destruction of such assets may cause harm to HEC Montréal. Examples of information assets are the *student* file and staff members' files.

Lifecycle

The lifespan of information, from its creation or acquisition, and including its treatment, storage transmission and use, until its transmission destruction or archiving.

Management of information security risks

Systematic approach that allows managers to make informed decisions in a context of uncertainty, by considering important issues related to information security risk.

Information

Information recorded on any medium (paper or electronic) or communicated in order to transmit knowledge. For example, information includes structured (databases) and unstructured (Word, Excel, PowerPoint, PDF, files, etc.) records, emails, text messages, oral communications and messages, photographs, drawings, faxes, originals and copies of paper documents, automated rapports and backup copies and archives.

Stakeholder

Any individual, department or organization whose role is defined in this policy, or a third-party with specific responsibilities related to information security.

Information owner

The information owner is the person designated by the director of an administrative unit. The owner notably ensures:

- That an adequate hierarchical classification by degree of risk is established for the information processed.
- That all information stored is classified based on established categories and that an inventory is kept of each information category.
- That adequate protection measures are put in place for each type of information.
- That a periodic check is done to ensure that information continues to be classified adequately and that protection measures remain valid and effective.

Risk to information security

Any event involving a degree of uncertainty that may threaten the confidentiality, integrity or availability of information and cause harm to HEC Montréal.

Residual risk

Residual risk is the risk that persists after a given risk has been addressed through different measures. Residual risk is also the portion of the risk that the School plans to retain deliberately or that it must assume.

4. 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.

- *Québec 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)*
- *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)
- *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)
- *Personal Information Protection Policy for Students of HEC Montréal (Politique sur la protection des renseignements personnels des étudiants de HEC Montréal)*
- *Regulation relating to the use of Information Resources (Règlement relatif à l'utilisation des ressources informationnelles)*
- *Politique relative à la gestion des documents actifs, semi-actifs et inactifs, HEC Montréal* (art. VI, E)