UNIVERSITÉ DU QUÉBEC
EN ABITIBI-TÉMISCAMINGUE

INFORMATION SECURITY POLICY

ADOPTED: 438-CA-4969 (2022-02-08)

Note: To minimize the impact of biases and prejudices which may be found in documents published by the Université, and recognize the diversity of the university community, this policy uses gender neutral language.

PREAMBLE:

As a public institution, the Université du Québec en Abitibi-Témiscamingue (hereinafter the "Université" or "UQAT") has an obligation to protect strategic and confidential information that it collects and retains, including data gathered on any individual, and to guarantee its availability, integrity, and confidentiality for the entire duration of its preservation and for which limits on distribution apply. In particular, this information includes university community members' personal information, and information subject to intellectual property rights, including trade secrets. It also includes all data, information, or documents judged to be strategic for the Université or for its partners, whether or not they were created by or received from different sources.

UQAT's responsibility to protect information includes, but is not limited to, managing access to confidential and strategic information, so that only individuals who are authorized to use this information for the purposes of their duties may access it. It applies to paper documents and digital data in the Université's custody, including data stored on technology platforms UQAT makes available to the members of its university community (for example: the Microsoft 365 environment) and in the systems it operates (for example: Gesta; SAFIRH; Moodle).

This Policy was adopted pursuant to the *Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises* and the *Directive gouvernementale sur la sécurité de l'information* issued by Quebec's Conseil du trésor. It is intended to reinforce the Université's information security governance framework by establishing rational measures and controls intended to preserve the confidentiality, integrity, and accessibility of information belonging to UQAT, or under its responsibility. These measures and controls take the information's value into account and encompass conditions for physical access to rooms or storage units containing any documents, as well as for the use of any technological tool operated by the institution.

By clarifying the roles and responsibilities of all members of the university community with respect to information security, this Policy enables the Université to comply with the laws, directives, and practices issued by the applicable government agencies. In doing so, the institution participates in reducing and mitigating risks that may affect confidential or strategic information for which UQAT is responsible and contributes to the pursuit of its teaching and research mission.

Based on the fact that the technological environment is constantly evolving and considering the human factor as a key part of the success of an information security program, this Policy also aims

to incorporate communication, awareness, and education into the formal processes of information security.

SECTION 1 — DEFINITIONS

Information asset: All documents and all data, including institutional email and research data, and any system allowing them to be viewed and used, software, operating systems, and equipment wherein the information can be found, regardless of format (paper, electronic or others).

Below are a few examples of information assets:

- A physical (paper) file regarding an individual who is an employee or a student
- Email boxes managed by UQAT
- Information systems (e.g., Gesta)
- A teaching platform (e.g., Moodle)
- Computer equipment belonging to UQAT (e.g., computers, tablets, servers)
- The contents of file servers (example: documents belonging to an entity, to a member of the faculty or student community)

UQAT is responsible for ensuring the security of the information assets under its responsibility, whether or not UQAT is the owner of said assets.

Information Management and Security Governance Framework (hereinafter "IMS Governance Framework"): Includes the content of this Policy, the information security action plan, the Université's Plan des mesures d'urgence the various procedures, directives, and guides or other documents of a similar nature which may stem from it (see Section 4), as well as incident management procedures specific to information security.

The IMS Governance Framework is intended to reinforce internal monitoring systems by offering reasonable assurance of compliance with respect to government legislation and policy, as well as other Université requirements with respect to the management of risks associated with the protection of information. In this respect, the IMS Governance Framework is a means of adjusting the level of risk through a combination of reasonable measures established to guarantee information security based on efforts corresponding to the sensitivity of that information and to potential anticipated impacts, in the event of an incident.

Confidentiality: (see Confidential information).

Board of Directors: The Université's Board of Directors.

Information Management and Security Governance Committee (hereinafter "IMS Committee"): Committee consisting of UQAT's senior managers, as described in Appendix 1.

Student community: the Université's student population (whether active or inactive).

University community: In the broader sense, this includes staff members, faculty members; sessional lecturers; groups, teams, units, centres, and Research Chairs; Module Council and undergraduate, graduate, or postgraduate Program Committee members; the student community

(whether active or inactive). Also considered members of the university community: staff and members of the Academic Council and the Board of Directors; the members of all communities created by any of the Université's administrative or academic bodies; external agencies and natural persons who use UQAT's software infrastructure: in particular, the Association générale étudiante de l'UQAT (AGEUQAT), UQAT alumni, the Université's unions, the Fondation de l'UQAT, retired UQAT employees, members of the Association des retraités de l'UQAT (ARUQAT), the Société de l'eau souterraine de l'Abitibi-Témiscamingue (SESAT) and the Société Immobilière de l'Université du Québec (SIUQ).

Information life cycle: The stages through which a piece of information moves, from creation to saving/recording, transfer, use, processing, and sending/transmission, through to its retention or destruction, in compliance with the Université's retention schedule under the *Archives Act*.

Information asset holders: A member of the university community who holds responsibilities or property rights (in particular, intellectual property) in documents, information, or data stored in UQAT's computer systems. In particular, the director of each entity and researchers are considered to hold information assets under their responsibility, including research data they collect, process, and analyze.

Director of an entity: Senior staff manager responsible for one of the Université's administrative bodies.

Availability: Of a piece of information, the property of being accessible when needed, and in the manner required, to an authorized individual.

Document: Is made up of information conveyed in a particular format. The information in that format is defined and structured in tangible or logical ways depending on the format it is in, and it is intelligible in the form of words, sounds or images. The information may be delivered by any means of writing, which includes a system of symbols transcribed in any one form, or as another system of symbols.

Data: Any representation of facts, figures, observations, or recordings that can take the form of image, sound, text, or physical measurements[1]. For example, a staff member's Social Insurance Number (SIN), or a student's Permanent Code are data.

Entity: Any administrative or academic body at the Université.

Security incident: Problem involving a potential breach of the availability, integrity, or confidentiality of one or more documents or any other information asset (for example, the content of an email in-box). Incidents include, but are not limited to, receipt of suspicious email, detection of viruses, and the transmission of data to an unauthorized individual. Government-wide information security incidents are incidents that may lead to consequences affecting delivery of essential services to the university community. To be considered Government-wide information security incidents, such breaches must have a presumed or real impact on the life, health, and wellbeing of individuals, and

[1] Definition adapted from the *Data, statistical information, and statistics* page (Statistics Canada, 2022).

on respect for their basic rights, the protection of their personal information, of their private life, as well as on the government's image.

Information: Pieces of information recorded in any given format (paper, electronic, or other) and intended to convey knowledge[2]. Information is a data set placed in any given context.

Accessible information: Of a piece of information, the property of being available when needed, and in the manner required, to an authorized individual.

Sensitive information: Of a piece of information, the property of being accessible only to designated or authorized individuals or entities.

Integrity: Of data or a document, the property of not having been subject to alteration or destruction.

Act: The *Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises* (RLRQ, chapter G-1.03).

Security Policy; Policy: Refers to this Policy.

Intellectual property: Intellectual property is a legal framework intended to recognize the merit of a project by granting its author(s) the exclusive rights to its distribution and its operation. Intellectual property is expressed in a variety of ways, including copyright related mainly to the literary, scientific or artistic domains, and the patent of invention, which mainly concerns industrial products. For more information, refer to the *Politique et règles en matière de propriété intellectuelle de l'UQAT.*

Université or **UQAT** : the Université du Québec en Abitibi-Témiscamingue.

Information Security Registry of Authority: Registry which indicates, in particular, the names of information holders, the systems assigned to them, as well as the roles and responsibilities of the key stakeholders in information security. This registry includes information assets categories.

Confidential information: Information about a third party (natural person or legal entity) which may not be disclosed without their consent, at the risk of causing them physical, moral, financial, or strategic harm. Confidential information is personal information, as well as any information whose disclosure to unauthorized individuals would lead to one or more impacts on: the proper conduct of business; the protection of members of the university community; the Université's strategic position; the agencies, institutions, financial, and industrial partners, and individuals maintaining relationships with it.

Acceptable risk: Risk related to one or more assets that does not require additional mitigation measures, given the low likelihood of occurrence, or potential impacts deemed to be non-critical.

Information security: The set of principles and practices related to the protection of data whatever format (paper or digital) they may take. Information security includes cybersecurity, which is more

[2] French definition excerpted from *Thésaurus de l'activité gouvernementale* (Government of Quebec, 2022).

specifically concerned with protection of digital data, devices, and networks against cyberthreats and malicious actors.

User: Any individual who uses information assets covered by this Policy.

SECTION 2 — PURPOSE OF THE POLICY

The purpose of this Policy is to assert UQAT's commitment to fully performing their obligations, with respect to information security, whatever format such information takes, or method of communication used to transmit it, throughout its life cycle. The Policy also supports the implementation of the Université's Information Management and Security Governance Framework. More specifically, the Université must ensure:

- The availability of information, such that it is accessible in a timely and appropriate manner to authorized individuals.
- The integrity of the information, such that it is not destroyed, nor altered in any way, without prior authorization from the entity responsible for it, and that the format the information takes provides it with the expected stability and survivability.
- The confidentiality of the information, limiting its disclosure and its use to only authorized individuals, whatever format it takes, and especially if this information includes personal information.
- Accessibility to a technological environment fostering, in particular, the quality of learning activities, the conduct of research work, and the pursuit of administrative activities in compliance with information security best practices.
- Clear assignment of responsibilities and the implementation of a sound internal information security management process that reinforces planning activities and activities around enforcement of required measures, and the auditing of practices for the purposes of accountability.

SECTION 3 — SCOPE OF THE POLICY

This Policy applies to members of the university community, as well as any external, natural person or legal entity duly authorized to obtain access to one or more of the Université's information assets.

The Policy applies to all information assets under UQAT's responsibility, whether those assets are collected by and/or belong to it and are held and/or used by it or by a third party, on behalf of and for the benefit of, the Université.

SECTION 4 — LEGISLATIVE AND ADMINISTRATIVE FRAMEWORK

The Security Policy falls within a context governed mainly by the following legal framework:

- the Charter of Human Rights and Freedoms (RLRQ, chapter C-12)
- the Civil Code of Québec (RLRQ, chapter CCQ-1991)
- the Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises (RLRQ, chapter G-1.03)
- the Act to Establish a Legal Framework for Information Technology (RLRQ, chapter C-1.1)
- the Act Respecting Access to Documents Held By Public Bodies and the Protection of Personal Information (RLRQ, chapter A-2.1)
- the Archives Act (RLRQ, chapter A-21.1)
- the Criminal Code (RSC 1985, c. C-46)
- Copyright Act (RSC 1985, c. C-42)
- the Framework Policy for the Governance and Management of Information Resources of Public Bodies (Government of Quebec — 2010)
- the Directive gouvernementale sur la sécurité de l'information (Order-in-Council 1514–2021, December 8, 2021)
- the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (CIHR, NSERC and SSHRC, 2018)
- the Politique gouvernementale de cybersécurité (SCT, March 2020)
- the Tri-Agency Research Data Management Policy (CIHR, NSERC and SSHRC, 2021)

The Security Policy mainly encompasses the following Université policies, directives, and regulations:

- Règlement 6 — Archives et gestion documentaire
- Politique de gestion des risques
- Politique d'utilisation du courrier électronique, d'Internet, des médias sociaux et des ressources technologiques de l'UQAT
- Politique sur l'accès aux documents et sur la protection des renseignements personnels
- Politique et règles en matière de propriété intellectuelle
- Politique et procédure relative à l'acquisition et à l'utilisation des logiciels
- Procédure visant à faciliter la divulgation d'actes répréhensibles commis à l'égard de l'UQAT

- Stratégie institutionnelle de gestion des données de recherche de l'UQAT (en cours d'élaboration)
- Directive en matière d'accès

SECTION 5 — GUIDING PRINCIPLES

The guiding principles governing the Université's actions with respect to information security are the following:

a) Recognition of the importance of ensuring the security of information on the basis of its value.

b) The adequate protection of information throughout its entire life cycle, from its acquisition or creation through to its destruction (the level of security to be applied varying over the course of a document's or data set's life cycle.

c) Reliance on industry standards and on the recommendations of the Secrétariat du Conseil du trésor in order to foster deployment of best practices, use of similar bodies' or institutions' benchmarks, and to ensure compliance with legal and regulatory requirements.

d) The ongoing identification and prioritizing of risks, with a view to maintaining an acceptable level of risk, taking into account legal, organizational, technological, physical, and environmental changes, as well as the evolution of threats and risks.

e) The conduct of information security planning activities that are subject to regular monitoring by the Université's decision-making bodies in order to ensure sound governance.

f) The creation and updating of an information security incident response plan, to allow for effective reaction in case of such events, and to ensure that essential services to the university community are re-established within a specified period of time.

g) The sharing of best practices and maintaining a partnership with the education network and other public bodies.

h) The establishment of an ethical approach intended to ensure regulation of behaviours and the taking of individual responsibility: every individual who has access to information being responsible for complying with confidentiality, availability, and integrity criteria for that information.

i) Taking user needs into consideration during planning, configuration, and activation of security measures.

j) The establishment of a process based on communication, support, awareness, and education of the university community around best practices, so that each member may

understand the importance of applying the required security rules, recognize the signs of an incident, and act accordingly.

SECTION 6 — GENERAL INFORMATION SECURITY MEASURES

The Université commits to taking the following general measures with respect to information security:

6.1 Maintain an up-to-date Information Security Registry of Authority

The Université recognizes that its information assets, as well as all information assets under its responsibility (for example, research data), are essential to its activities and enable it to carry out its mission. Consequently, these assets must be subject to ongoing assessment, appropriate use, and adequate protection. The level of protection applied to information assets must be established based on their importance, confidentiality, and the risks of incident, error, and malicious use to which they are exposed. With this in mind, the Université agrees to draft and maintain an up-to-date Registry of Authority which includes the location of information assets, a list of key holders of those assets, and the partners involved in their creation, the management or transmittal of the information, as well as the assessment of its criticality, in order to guide the Université's actions with respect to prevention, protection, and preservation.

6.2 Formalize the institutional regulatory framework

The Université agrees to put guides, directives, procedures, or any other similar documents in place, to ensure that the IMS Governance Framework is implemented and permits traceability of actions taken with information assets.

6.3 Draft an action plan

The Université agrees to put in place and maintain an up-to-date action plan to comply with legal and regulatory requirements, and to ensure ongoing improvement in the level of organizational maturity, with respect to information security.

6.4 Awareness and education

The Université agrees to raise the awareness of and educate users, on a regular basis, regarding the security of information assets, their roles and responsibilities in this regard, as well as regarding any consequences of an incident.

6.5 Draft and maintain an up-to-date Incident Response Plan

The Université agrees to draft and maintain an up-to-date information security Incident Response Plan that aligns with its Plan des mesures d'urgence. This plan must include escalation plans and succession plans in case of incidents, to allow for effective reaction during an event, and to ensure that essential services to the university community are re-established within a specified period of time.

SECTION 7 — INFORMATION SECURITY ROLES AND RESPONSIBILITIES

This Policy defines information security roles and responsibilities, which are assigned as follows:

7.1 Board of Directors

- Adopts the Policy and any amendments thereto.
- Ensures that an IMS Governance Framework is implemented.
- Becomes familiar with the rendering of accounts with which it is presented.
- Approves organizational orientations with respect to information security.
- Ensures that budgets needed for the accomplish the objectives and orientations contained in this Policy are allocated, through an analysis of organizational priorities.

7.2 IMS Committee

- Recommends adoption of the Information Security Action Plan.
- Assesses the effectiveness and yield of the Information Security Action Plan.
- Approves information security recommendations and ensures follow-up with the Board of Directors, as required.
- Approves the information security awareness and education program intended for staff.
- Approves the Université's Plan des mesures d'urgence, as well as the specific procedures associated with information security incident management.
- Sends the necessary recommendations related to this Policy to the executive committee.
- Verifies the content of the rendering of accounts intended for applicable government bodies.
- Acts as a crisis committee when incidents occur.

7.3 Office of the Rector

- Is an active participant on the IMS Committee.
- Is notified of any major risk or incident that affects information security, and determines the organizational orientations required to manage the incident.
- Recommends organizational orientations with respect to information security.

- Recommends the allocation of budgets necessary for the accomplishment of objectives and orientations contained in the Policy.

7.4 Office of the General Secretary

- Is an active participant on the IMS Committee.
- Is notified of any major risk or incident that affects information security, and determines the organizational orientations required to manage the incident.
- Sends the necessary recommendations related to this Policy to the executive committee and ensures that the rendering of accounts for which they are responsible is carried out.
- Approves directives, procedures, processes, and guides stemming from this Policy, and ensures that the content of this Policy is communicated to all members of the university community.
- Recommends the allocation of budgets necessary for the accomplishment of objectives and orientations contained in the Policy.
- Serves as the organizational lead for information security, which includes the access management compliance component, and as head of information security for the organization.
- Ensures that the IMS Governance Framework is periodically reviewed.
- Supervises and guides the work of the Information Security Manager.
- Designates information asset holders and information asset managers, so they can be entered into the Information Security Registry of Authority.
- Ensures that an information security audit is conducted at least once every two years or following any major change likely to lead to consequences for information security and, together with the Information Technology Services, uses it to identify priority actions and related timetables.
- Is responsible for managing incidents, including the implementation and keeping up-to-date of specific procedures associated with the Université's Plan des mesures d'urgence [Emergency Response Plan].

7.5 Office of the Vice–Rector, Resources

- Is an active participant on the IMS Committee.
- Recommends the allocation of budgets necessary for the accomplishment of objectives and orientations contained in the Policy, following strategic analysis of each of the organizational priorities.
- Supervises the cyber-insurance negotiation process and recommends coverage plans to the Université's decision-making bodies.
- Ensures that the components of the information security Incident Response Plan are incorporated into the Université's Plan des mesures d'urgence.

7.6 Information Technology Services Director

- Is an active participant in the working groups stemming from the IMS Committee, including the incident prevention and management tactical team.
- Participates in the process of drafting the Incident Response Plan and ensures that its content is communicated to the members of its team.
- Ensures that automatic surveillance and detection systems are implemented commensurate with the risks to be mitigated.
- Applies the security recommendations issued, in line with available budgets and resources.
- Ensures that intrusion and vulnerability tests are conducted at least once a year or following any major change likely to lead to consequences for information security and uses them to identify priority actions and related timetables.
- Promotes the use of shared information security systems defined by the Secrétariat du Conseil du trésor.

7.7 Information Security Manager

- Ensures the implementation of the information security management framework and of the Information Security Registry of Authority.
- Formulates the action plan, coordinates the activities specified in the plan, and reports on the progress of specified tasks for the purpose of the expected internal and external renderings of account.
- Ensures that risk analysis activities, needs assessments, and threat assessments are conducted on an ongoing basis.
- Issues recommendations dictating the principles to be adopted with respect to information security, in compliance with the legislative and regulatory framework.
- Designs the education and awareness program intended for the university community.
- Takes part in the drafting of directives, procedures, processes, and guides stemming from this Policy.
- Prepares and submits renderings of account and information security evaluations required by the applicable government bodies.
- Writes and maintains an up-to-date Incident Response Plan and registry of events and ensures that their content is communicated to the applicable individuals.
- Is a member of the working groups stemming from the IMS Committee, including the incident prevention and incident response tactical team.
- Sends the necessary recommendations related to this Policy to the IMS Committee.
- Advises the university community, in particular when acquiring new technological tools or when managing technological changes.

- Reports any government-wide information security incidents to the MES [Ministry of Higher Education], and the Offices of the Rector and the General Secretary, according to terms set by the latter.
- Reports information security risks, including government-wide risks, to the Offices of the Rector and the General Secretary.
- Submits an Information Security Action Plan to the Office of the General Secretary on a yearly basis, which includes priority actions and related timetables stemming from audit and intrusion test exercises.

7.8 Service des archives et gestion documentaire

- Creates and maintains an up-to-date classification of the Université's information assets, together with the holders of these assets.
- Works together with the Service des technologies de l'information, the Information Security Manager and the holders of information assets to identify and locate those assets, and determine the best practices for the use, protection, and sharing of those information assets, depending on their level of criticality.

7.9 Holders of information assets

- Ensure the application of sound information management and handling practices within their teams.
- Together with the Service des archives et gestion documentaire assess the availability, integrity, and confidentiality of assets under their responsibility when updating the Information Security Registry of Authority.
- Inform the Service des archives et gestion documentaire of any change to their business process, or any addition of information assets requiring an update to the Information Security Registry of Authority.
- Determine the specific access rights associated with these assets in accordance with the assessment of the criticality of the information contained on them, and the official duties of the individuals designated to access them, as well as on the basis of guidelines provided by the Office of the Secretary General.
- Work together with the Service des technologies de l'information to determine the most appropriate times to carry out critical enhancements and upgrades.
- Immediately report any act of which they are aware which they deem likely to be a real or presumed violation of security rules, as well as any anomaly or incident which may prejudice the protection of information assets under their responsibility:
    - By contacting 819-762-0971 ext. 2525 directly.
    - By following the instructions provided by the Service des technologies de l'information staff and/or Office of the Secretary General.
- Follow the instructions provided at the time any new software is acquired or used.

7.10 Users

- Become familiar with this Policy, directives, procedures, and other courses of action stemming from it and, at all times, take care to observe their obligations with respect to these documents.
- Use the information assets placed at their disposal in accordance with the access rights they have been granted, and solely when necessary for carrying out their duties, while limiting themselves to use for the intended purposes, and complying with distribution restrictions associated with the information asset's level of confidentiality.
- Respect the security measures implemented at their workstation, as well as during any handling of equipment or document containing data to be protected.
- Comply with legal requirements and organizational procedures concerning the handling and use of any information asset which contains personal information, or information subject to the application of intellectual property rights.
- By their use of UQAT's technology tools and infrastructure, consent to automatic monitoring conducted for the mitigation of related information security risks.
- Participate in all exercises and training identified as being mandatory by the Université.
- When travelling internationally, in particular for the purpose of research activities, observe the practices recommended by the Government of Canada and contact the Office of the Secretary General's information security team for any helpful reference.
- Immediately report any act of which they are aware which they deem likely to be a real or presumed violation of security rules, as well as any anomaly or incident which may prejudice the protection of information assets under their responsibility:
    - By contacting 819-762-0971 ext. 2525 directly.
    - By following the instructions provided by the Service des technologies de l'information [Information Technology Services] staff and/or Office of the Secretary General.
- When they leave the Université, hand over all information assets (including computer or telephone equipment, information in electronic, paper, or other formats) belonging to UQAT and placed at their disposal for the purposes of fulfilling their duties.

7.11 Signatories to contracts

Over and above their responsibilities as users and, where applicable, being individuals who are information asset holders, signatories to contracts:

- Together with the Office of the Secretary General, make sure that service agreements and contracts entered into with service providers, partners, and agents stipulate clauses that guarantee compliance with information security requirements.
- Prior to acquisition of a new technology platform, ensure that a security and compliance certification was carried out beforehand for said platform, by the Office of the Secretary General.

SECTION 8 — PENALTIES

When a user contravenes this Policy or a directive stemming from it, this individual expose themselves to administrative, legal, or disciplinary action based on the severity of their act. This action may include suspension of privileges, reprimand, suspension, firing or other action, in accordance with provisions contained in the collective agreements, memorandums of understanding/agreements, or contracts. In cases where the user in default is a student, such action includes any other penalties that may apply pursuant to regulations and policies governing students.

The Université may send information collected that suggests a violation of any Act or regulation in effect has been committed to any judicial authority.

SECTION 9 — FINAL PROVISIONS

a) This Policy comes into force on the date of its adoption by the Board of Directors.

b) The individual appointed to the position of Secretary General ensures that the provisions of this Policy and its directives are implemented.

c) In the event changes occur that might impact this Policy, it will be reviewed accordingly.

d) This Policy falls within the scope of the Information Management and Security Framework. Obligations stemming from it may be outlined in directives, procedures, guides, or similar documents.

APPENDIX 1 – Composition of the IMS Committee and Working Groups

NOTE: Individuals identified below are the core participants in working groups. Depending on the types of files being handled, other individuals may be called upon to join any of these groups.

Information Management and Security Governance Committee (IMS Committee)

- Participating individuals: Senior managers of UQAT

Coordination ensured by the individual responsible for information security

IMS Working Group

- Action plan, risks list, and Information Security Registry of Authority follow-up
- Coordinates implementation of deliverables
- Identifies and analyzes new risks

Participating individuals:

- Information Technology Services Director
- Employee responsible for operational security at the Information Technology Services
- Information Security Manager
- General Secretary, as required
- Archivist, as needed

Process and Policy Management Team

- Identification of legal, regulatory and job requirements
- Policy and control mechanism creation

Participating individuals, co-opted as required:

- Human Resources spokesperson
- Spokesperson from the Office of the Registrar
- Spokesperson from the Office of the Vice-Rector, Academics, Research and Creation
- Spokesperson from the Table de Développements numériques
- Spokesperson from Finance Services

Compliance Management Team

- Maintains the legal and regulatory framework inventory
- Confirmation of priorities and impact levels with respect to protection of personal information
- Audit management

Participating individuals:

- General Secretary
- Legal Counsel
- Coordinator of Risk Management

Incident Prevention and Management Tactical Team

- Creation of escalation scenarios, and succession plans in case of incidents
- Coordination of actions to be taken in case of incidents/events

Participating individuals:

- Director, Information Technology Services
- Information Security Manager
- Employee responsible for operational security at the Information Technology Services