INFORMATION SECURITY AND MANAGEMENT GOVERNANCE POLICY

ADOPTION		
INSTANCE	**DATE**	**DÉCISION**
	September 25, 2024	496A-20240925-4410

MODIFICATION(S)		
INSTANCE	**DATE**	**DÉCISION**

RESPONSABLE	General Management and Administration Department
CODE	P-08-2024.1

TABLE OF CONTENTS

PREAMBLE

In the course of its activities, **INRS** collects, uses, produces, communicates and retains a significant amount of Information in many forms and media. As such, INRS recognizes the need to implement integrated governance that promotes rigorous and transparent management in accordance with the provisions of the *Act respecting the governance and management of the information resources of public bodies and government enterprises* (RLRQ, c. G-1.03) (the **Act**).

The application of the Act, the *Act to modernize legislative provisions respecting the protection of personal information* (RLRQ, 2021, chapter 25) and the *Government Directive on Information Security* of the Secrétariat du Conseil du trésor du Québec applicable to public bodies imposes significant obligations on academic institutions. To comply with its regulatory and legal obligations, INRS must adopt, maintain and enforce a policy to ensure the implementation of formal processes for the security and management of its information assets.

1. OBJECTIVES

The purpose of the *Information Security and Management Governance Policy* (the **Policy**) is to manage Information Assets in compliance with INRS's rights and obligations in order to guarantee and meet Information Asset security objectives, and more specifically to :

- Maintain systems and internal controls that provide reasonable assurance of compliance with applicable legislation;
- Promote consideration of the security of Information Assets in the acquisition, development, use, replacement and destruction of Information Assets;
- Ensure the availability of Information so that it is accessible in a timely manner and in the manner required while limiting the disclosure of Information to only those persons authorized to access it;
- Ensure the integrity of the Information by protecting it from unauthorized destruction, modification or alteration in any way;
- Protect the INRS Community against the misuse and illegal use of Information Assets, in order to ensure their stability and longevity;
- Define the general principles, roles and responsibilities of those involved in Information security;
- Identify and classify Information Assets according to their degree of criticality, and constantly monitor their evaluation and appropriate protection;
- Put in place a business continuity and IT succession plan;
- Safeguard the privacy of individuals, including the confidentiality of personal information.

2. DEFINITIONS

For the purposes of this Policy, defined terms have the following meanings :

COMSI : the organizational coordinators of information security measures who participate in the Government Alert Network.

CSIO : the person designated as the Head of Organizational Information Security under the Government Information Security Directive.

Document : Information, produced or held by any member of the INRS Community that is delimited, structured and intelligible in the form of words, sounds or images and delivered in a traditional or digital medium.

Incident : an event occurring during the processing, use or storage of the Information that is likely to affect the availability, integrity or confidentiality of the Information, or more generally the security of the Information Assets, in particular by interrupting services or reducing their quality, and to cause damage.

Incident Register : a register in which Information security incidents, their nature, impact, measures taken to restore normalcy and follow-up are recorded.

Information : the data, indications, set of information, including personal information, recorded by INRS on a Document or held by INRS, including Information originating from a third party. Information may be confidential, privileged, public or personal.

Information Asset : digital or traditional Information in any possible form, whether Documents or any element contributing to the processing, production, access, storage and circulation of Information (databases, application software, procedures, etc.), including any Information System owned or held by INRS.

Information Holder : Any Manager or person in a management position designated to ensure the security of an Information Asset and its underlying resources.

Information System : all the elements contributing to the processing, production, access, storage and circulation of Information.

INRS Community : staff members, including senior management, executive staff and faculty, the student community, trainees and postdoctoral fellows of INRS.

Integrity : the complete and unaltered nature of an Information Asset, proving that it has not undergone any addition, removal or modification, whether accidental or intentional.

Manager : any person in a personnel management position, including management staff and faculty members, who supervises the work and training of staff members, the student community, trainees and postdoctoral fellows.

Normative Document : an INRS regulation, code, charter, policy, directive or procedure.

Preservation : all technical operations that make it possible to safeguard Documents, preserve their Integrity and guarantee access to their content.

SAGD : the INRS Archives and Document Management Department, responsible for managing administrative Documents and historical archives produced or received by INRS. It is responsible for the Preservation of these Documents and for handling them in a way that facilitates access.

SRI : the Information Resources Department, under the responsibility of a managerial staff member, whose responsibility is to develop and ensure the availability, integrity and confidentiality of Information Assets.

3. SCOPE OF APPLICATION

This Policy applies to all members of the INRS Community as well as to any third party called upon to process or use an Information Asset.

It also applies to suppliers and partners of INRS who operate or host its Information or Information Assets, insofar as they must comply with the resulting requirements in terms of the security of Information Assets.

4. ENTITY IN CHARGE OF APPLICATION

General Management is responsible for ensuring compliance with the orientations, strategies, policies, standards, directives, rules or application guidelines issued under the Act.

The Administration Department is responsible for applying the Policy.

5. STATEMENTS OF GENERAL PRINCIPLES

The security of Information Assets is supported by a proactive approach aimed at regulating conduct and ensuring individual accountability.

5.1 PROTECTION OF INFORMATION

INRS recognizes that the Information Assets it holds are essential to the pursuit of its mission and, as such, must be subject to continuous assessment, appropriate use and suitable protection throughout their life cycle. The level of protection afforded to Information Assets is determined by their importance and confidentiality, by best practices and by the risks of Incidents, errors and malicious damage to which they are exposed.

5.2 PROTECTION OF CONFIDENTIAL INFORMATION

The *INRS Privacy Governance Policy* states that all confidential information must be protected from unauthorized disclosure, access or use.

Confidential information, within the meaning of the *Act respecting access to documents held by public bodies and the protection of personal information*, includes personal information as well as any information the disclosure of which would have an impact on, among other things, intergovernmental relations; negotiations between public bodies; the economy; third parties with respect to their industrial, financial, commercial, scientific or technical information; the administration of justice and public security; administrative or political decisions and auditing.

5.3 AWARENESS AND TRAINING

INRS *undertakes*, on a regular basis, to educate and train members of the INRS Community about the security of Information Assets, the consequences of a breach of their security and their role and obligations in this regard.

5.4 RIGHT OF INSPECTION

In accordance with applicable legislation, INRS exercises a right of inspection over any use of its Information Assets.

6. INFORMATION ASSET SECURITY

INRS adheres to the government's strategic orientations and objectives for Information Asset security and is committed to ensuring that the practices and solutions adopted in this regard correspond to recognized and generally used methods.

The committee responsible for information security and management is the Access to Information and Privacy and Information Security and Management Committee (**ATIP-ISM Committee**), whose composition is set out in the *INRS Privacy Governance Policy*. INRS entrusts the ATIP-ISM Committee with the mandate of ensuring the security and management of its Information Assets, in particular by the means described below.

6.1 RISK MANAGEMENT

In order to guide security measures for Information Assets, and in accordance with the INRS *Risk Management Policy*, the SRI, in collaboration with the SAGD, periodically identifies and assesses risks that threaten the confidentiality, integrity or availability of Information. Protective measures are then deployed based on the assessment of the impact and probability of occurrence of a threat, so as to mitigate the risks and maintain them at an acceptable level. The SRI carries out a risk assessment prior to any acquisition or significant change to the Information Assets under its responsibility.

6.2 VULNERABILITY MANAGEMENT

The SRI deploys measures to keep software up to date in order to keep vulnerabilities as low as possible and reduce the risk of security Incidents or cyberattacks. It monitors threats relevant to the INRS environment.

6.3 INCIDENT MANAGEMENT

The SRI implements a security Incident management process. This process sets out the means of detecting, documenting and responding to Incidents. The ATIP-ISM Committee is responsible for maintaining the Incident Register and must be kept informed of security Incidents.

6.4 IT SUCCESSION AND CONTINUITY PLAN

INRS ensures at all times the continuity of activities necessary for the fulfillment of its mission, including in the event of a disaster or major failure affecting Information Assets deemed essential. In accordance with the *Politique de continuité des activités et de gestion des mesures d'urgence (Business Continuity and Emergency Management Policy*) and the *Politique de gestion des risques (Risk Management Policy)*, INRS is responsible for providing an IT succession and continuity plan.

6.5 INFRASTRUCTURE AND INFORMATION ACCESS MANAGEMENT

The SRI controls access to its premises and to the Information Assets under its responsibility in such a way as to prevent damage, intrusion or unauthorized access. Access to Information Assets is permitted only to Information Holders and to persons authorized to access it by such Information Holders. The SRI periodically reviews access to its premises and to the Information Assets under its responsibility.

In particular, access to email inboxes or any Information belonging to a member of the INRS Community, whether on a computer or in any directory, is forbidden without their consent or the authorization of the person responsible for access to Information and for the protection of personal Information, as well as the authorization of the Administration Department.

6.6 PROTECTION OF INFRASTRUCTURE AND INFORMATION INTEGRITY

The SRI and each Information Holder will take the necessary measures to protect the Information Assets under their responsibility against any attack on the Integrity of said assets, including in particular the risks of fire, flood, power surges, power outages and other failures of various kinds.

6.7 THE INFORMATION SYSTEMS LIFE CYCLE

The SRI and each Information Holder will take appropriate measures to protect the confidentiality and integrity of the Information and to ensure its availability. The SRI is responsible for establishing control and monitoring measures throughout the life cycle of the Information Assets under its responsibility.

6.8 CLASSIFICATION OF INFORMATION ASSETS

Information Assets are categorized and inventoried. They are classified and protected according to their degree of sensitivity and the related security requirements.

7. RESPONSABILITIES OF INRS COMMUNITY MEMBERS

All members of the INRS Community are responsible for applying and complying with the Policy, guidelines or any other indications arising therefrom.

Each person who accesses, consults or processes Information is responsible for its use and must act in such a way as to protect it. To this end, they must sign the declaration of commitment set out in Appendix A of the Policy at the time of hiring or registration.

Each member of the INRS Community is responsible for:

– The consequences of the use of their login, access code or password, whether these actions are taken by the member or by a third party, unless they can demonstrate that the actions taken by a third party are not the result of negligence or malice on the member’s part;
– Using the access rights authorized and assigned to them, and the Information Assets made available to them, only in a context appropriate for the use of such Information Assets and for the purposes for which they are intended;

- Complying with the security measures in place on their workstation and on any other equipment containing Information to be protected, and the member must not modify or override the configuration of security measures or disable them;
- Taking part in and completing the relevant training and awareness activities offered by INRS;
- Cooperating in any process aimed at identifying or mitigating a threat to the security of Information Assets or a security Incident;
- Complying with legal requirements concerning the use of Information Systems, for which intellectual property rights may exist;
- Reporting immediately to their immediate superior any act of which they are aware that may constitute an actual or suspected violation of security rules, as well as any anomaly that may adversely affect the protection of INRS's Information Assets;
- Refraining from any malicious behaviour that could harm or affect others, as well as any illegal or malicious activity or activity contrary to the mission of INRS;
- Upon leaving INRS, returning the various identity and access cards, computer equipment and Informational Assets made available to them in the course of their duties or studies.

8. GOVERNANCE

The Policy assigns the management of the security of INRS Information Assets to entities, committees and individuals by virtue of the specific functions they perform.

8.1 AUDIT COMMITTEE

The Audit Committee is responsible for :

- Reviewing issues, orientations, strategies and general practices relating to Information Assets;
- Ensuring the implementation and monitoring of Information Asset security practices and standards, including cybersecurity;
- Reviewing and monitoring issues and risks relating to Information Assets, including Information management and security.

8.2 ATIP-ISM COMMITTEE

The ATIP-ISM Committee is responsible for :

- Reviewing and making recommendations on the performance and effectiveness of Information Asset security;
- Proposing adjustments to Normative Documents concerning the management and security of Information Assets;
- Ensuring the proper handling of confidentiality Incidents and maintaining the Incident Register;
- Reviewing, prioritizing and recommending strategic orientations, action plans, intervention priorities and Normative Documents relating to Information security, and ensuring their implementation.

8.3 INFORMATION HOLDERS

For the Information Assets under their responsibility, all Information Holders are responsible for the following :

- Participating in the development of strategic orientations, policies, directives, management frameworks, guides, action plans and assessments relating to the security of Information Assets;
- Participating in the categorization of Information Assets;
- Ensuring that security measures for Information Assets, including those related to compliance with legal requirements for the protection of personal information, are implemented and enforced;
- Ensuring that existing security measures for Information Assets are appropriate for the identified risks;
- Determining who is authorized to access the Information Assets and the levels of access granted;
- Participating in risk analysis and ensuring that residual risks are addressed.

8.4 ADMINISTRATION DEPARTMENT

The Administration Department is responsible for :
- Enforcing the Policy;
- Recommending to the Board of Directors the appointment of the CSIO;
- Appointing individuals to act as COMSI.

8.5 SRI DIRECTOR

The SRI Director is responsible for the following :
- Submitting to the ATIP-ISM Committee for analysis the strategic orientations, action plans, intervention priorities, management frameworks, directives and procedures related to the security of Information Assets, and seeing to their implementation;
- Defining and implementing formal Information Asset security measures and processes to ensure the management of risks, access to Information and Information security Incidents;
- Defining Information Asset security requirements for projects to develop or acquire Information Systems.

8.6 CSIO

The CSIO is responsible for the security of Information Assets within INRS and ensures compliance with relevant legal, governmental and organizational requirements.

8.7 COMSI

COMSI act on an operational level and have the following responsibilities :
- Participating in the implementation of measures and providing the necessary support to the CSIO, in particular with regard to the management of Incidents and Information Asset security risks;
- Representing INRS on the Governmental Alert Network;
- Implementing the Threat, Vulnerability and Incident Management (TVIM) process at INRS.

8.8 DIRECTOR OF HUMAN RESOURCES

With regard to the security of Information Assets, the Director of Human Resources must :

– Verify, where necessary, the criminal records of applicants for employment and of staff members involved in the security of Information Assets;
– Impose appropriate sanctions in the event of a breach of Normative Documents relating to the security of Information Assets.

8.9 SAGD

The SAGD is responsible for document management under the *Act respecting the governance and management of information assets* and for implementing measures for the security of Information regardless of its medium, as well as measures for the secure destruction of Information in its custody.

9. SANCTIONS

In addition to the remedies and penalties provided for in legislation, any contravention of the Policy may result in the withdrawal of access rights to Information Assets or the imposition of administrative and disciplinary measures up to and including dismissal or expulsion, depending on the nature and seriousness of the misconduct.

In the event of non-compliance with the Policy, INRS may also exercise any appropriate recourse against any member of the INRS Community, even after the member's employment or studies at INRS have ended.

Likewise, any contravention of the Policy by a third party is subject to the sanctions provided for in the contract binding them to INRS or under the provisions of applicable legislation.

10. UPDATES

The Policy will be updated as required, or at least every five years.

11. FINAL PROVISIONS

The Policy comes into force upon adoption by the Board of Directors.

APPENDIX A

DECLARATION OF COMMITMENT FORM

Within 30 days of the coming into force of the *Politique de gouvernance en matière de sécurité et de gestion de l'information* (Information Security and Management Governance Policy) or of joining or enrolling, all members of the INRS Community must declare that they have read this policy, that they understand its meaning and scope, and that they agree to follow it.

All members of the INRS Community are obliged to protect the Information Assets made available to them by INRS. To that end, they are responsible for:

1. Complying with this Policy and all other INRS normative documents relating to information security and the use of Information Assets
2. Accepting the consequences of their own or others' use of their username, access code, or password, unless they can demonstrate that a third party's actions are not the result of negligence or malice on their part
3. Using the authorized credentials assigned to them and the Information Assets made available to them only where appropriate and for their intended purposes
4. Following the security measures in place at their workstation and on any other equipment containing Information to be protected, and not modifying, overriding, or deactivating any security measures
5. Taking part in and completing the informational and training activities offered by INRS on the subject
6. Collaborating in efforts to identify or mitigate security threats or Incidents related to Information Assets
7. Complying with legal requirements concerning the use of products for which intellectual property rights may exist
8. Immediately reporting to their immediate superior any actual or suspected violations of security rules, as well as any anomalies that may adversely affect the protection of INRS's Information Assets
9. Refraining from malicious behaviour that could harm or affect others, as well as any activity that is illegal, malicious, or against INRS's mission
10. On leaving INRS, handing over the identity and access cards, computer equipment, and Information Assets made available to them in the course of their duties or studies

I declare that I have read the *Politique de gouvernance en matière de sécurité et de gestion de l'information* (Information Security and Management Governance Policy). I acknowledge my responsibilities with regard to confidentiality and computer security.

Name

Signature

Date