Institut national de la recherche scientifique

POLITIQUE DE GOUVERNANCE EN MATIÈRE DE SÉCURITÉ ET DE GESTION DES ACTIFS INFORMATIONNELS

ADOPTION		
INSTANCE	**DATE**	**DÉCISION**
Conseil d'administration	25 septembre 2024	496A-20240925-4410

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

RESPONSABLE	Direction générale et Direction de l'administration
CODE	P-08-2024.1

TABLE DES MATIÈRES

PRÉAMBULE

Dans le cadre de ses activités, l'**INRS** recueille, utilise, produit, communique et conserve une quantité importante d'Information sous plusieurs formes et plusieurs supports.

À ce titre, l'INRS reconnaît la nécessité de mettre en place une gouvernance intégrée qui favorise une gestion rigoureuse et transparente en concordance avec les dispositions de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) (**Loi**).

L'application de la Loi, de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25) et de la *Directive gouvernementale sur la sécurité de l'information* du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics impose des obligations importantes aux établissements universitaires. Pour se conformer et répondre à ses obligations réglementaires et légales, l'INRS doit adopter, garder à jour et veiller à l'application d'une politique afin d'assurer la mise en place de processus formels permettant l'encadrement de la sécurité et la gestion de ses Actifs informationnels.

1. OBJECTIFS

La *Politique de gouvernance en matière de sécurité et de gestion des actifs informationnels* (**Politique**) vise la gestion des Actifs informationnels dans le respect des droits et obligations de l'INRS afin de garantir et répondre aux objectifs de sécurité des Actifs informationnels et plus spécifiquement pour :

- maintenir des systèmes et des contrôles internes offrant une assurance raisonnable de conformité à l'égard de la législation applicable;
- favoriser la prise en compte de la sécurité des Actifs informationnels dans l'acquisition des Actifs informationnels, leur développement, leur utilisation, leur remplacement et leur destruction;
- assurer la disponibilité de l'Information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise tout en limitant la divulgation de l'Information aux seules personnes autorisées à en prendre connaissance;
- assurer l'Intégrité de l'Information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation;
- protéger la Communauté INRS contre une utilisation abusive et illégale des Actifs informationnels, et ce, dans le but d'assurer la stabilité et pérennité voulues;
- définir des principes généraux ainsi que les rôles et responsabilités des intervenants en matière de sécurité de l'Information;
- identifier et classifier les Actifs informationnels selon leur degré de criticité et veiller constamment à leur évaluation ainsi que leur protection adéquate;
- mettre en place un plan de continuité des activités et de relève informatique;
- assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels.

2. DÉFINITIONS

Aux fins de l'application de la Politique, les expressions définies revêtent le sens qui leur est donné dans le présent article.

Actif informationnel : une Information numérique ou traditionnelle sous toute forme possible, que ce soit des Documents ainsi que tout élément contribuant au traitement, à la production, à l'accès, au stockage et à la circulation de l'Information (bases de données, logiciels d'application, procédures, etc.), y compris tout Système d'information appartenant ou détenu par l'INRS.

Communauté INRS : les membres du personnel, incluant le personnel cadre supérieur, le personnel cadre et le corps professoral, la communauté étudiante, les stagiaires et les stagiaires postdoctoraux de l'INRS.

Conservation : l'ensemble des opérations techniques qui permettent de sauvegarder les Documents, d'en préserver leur Intégrité et de garantir l'accès à leur contenu.

COMSI : les personnes coordonnatrices organisationnelles des mesures de sécurité de l'Information qui participent au Réseau d'alerte gouvernemental.

CSIO : la personne désignée chef de la sécurité de l'Information organisationnelle en vertu de la Directive sur la sécurité de l'information gouvernementale.

Document : une Information, produite ou détenue par tout membre de la Communauté INRS qui est délimitée, structurée et intelligible sous forme de mots, de sons ou d'images et portée par un support traditionnel ou numérique.

Document normatif : un règlement, un code, une charte, une politique, une directive ou une procédure de l'INRS.

Gestionnaire : toute personne en situation de gestion de personnel, incluant le personnel cadre et les membres du corps professoral, qui supervise le travail et la formation de membres du personnel, de la communauté étudiante, des stagiaires et stagiaires postdoctoraux.

Incident : un événement survenu lors du traitement, de l'utilisation ou de l'entreposage de l'Information susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'Information, ou plus généralement à la sécurité des Actifs informationnels, notamment par une interruption des services ou une réduction de leur qualité, et de causer un préjudice.

Information : les données, indications, ensemble de renseignements, incluant des renseignements personnels, consignés par l'INRS sur un Document ou détenus par l'INRS, y compris une Information provenant d'une tierce personne. Une Information peut être confidentielle, privilégiée, publique ou personnelle.

Intégrité : le caractère complet et non altéré d'un Actif informationnel prouvant que celui-ci n'a subi aucun ajout, aucun retrait ni aucune modification, accidentelle ou intentionnelle.

Personne détentrice de l'Information : Tout Gestionnaire ou toute personne en situation de gestion désigné pour assurer la sécurité d'un Actif informationnel et des ressources qui la sous-tendent.

Registre des Incidents : un registre dans lequel sont consignés les Incidents de sécurité de l'information, leur nature, leur impact, les mesures prises pour le rétablissement à la normale et le suivi.

SAGD : le Service des archives et de la gestion documentaire de l'INRS, responsable de la gestion des Documents administratifs et des archives historiques produits ou reçus par l'INRS. Il en assure la Conservation et le traitement de façon à en favoriser l'accès.

SRI : le Service des ressources informationnelles sous la responsabilité d'une ou d'un membre du personnel cadre, dont la responsabilité est de développer et d'assurer la disponibilité, l'Intégrité et la confidentialité des Actifs informationnels.

Système d'information : l'ensemble des éléments contribuant au traitement, à la production, à l'accès, au stockage et à la circulation de l'Information.

3. CHAMP D'APPLICATION

La Politique s'applique à tous les membres de la Communauté INRS ainsi qu'à toute tierce personne appelés à traiter ou à utiliser un Actif informationnel.

Elle s'applique également aux fournisseurs et partenaires de l'INRS qui exploitent ou hébergent son Information ou ses Actifs informationnels, dans la mesure où ils doivent respecter les exigences qui en découlent en matière de sécurité des Actifs informationnels.

4. RESPONSABLE DE L'APPLICATION

La Direction générale doit s'assurer que les orientations, les stratégies, les politiques, les standards, les directives, les règles ou les indications d'application pris en vertu de la Loi sont respectés.

La Direction de l'administration est responsable de l'application de la Politique.

5. ÉNONCÉS DE PRINCIPES GÉNÉRAUX

La sécurité des Actifs informationnels est soutenue par une démarche proactive visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.1 PROTECTION DE L'INFORMATION

L'INRS reconnaît que les Actifs informationnels qu'il détient sont essentiels à la poursuite de sa mission et, de ce fait, qu'ils doivent faire l'objet d'une évaluation continue, d'une utilisation appropriée et d'une protection adéquate tout au long de leur cycle de vie. Le niveau de protection dont les Actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité, des bonnes pratiques et des risques d'Incident, d'erreur et de malveillance auxquels ils sont exposés.

5.2 PROTECTION DES RENSEIGNEMENTS CONFIDENTIELS

La *Politique sur la gouvernance en matière de protection des renseignements personnels de l'INRS* prévoit que toute Information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés comme confidentiels, au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

5.3 SENSIBILISATION ET FORMATION

L'INRS s'engage, sur une base régulière, à sensibiliser et à former les membres de la Communauté INRS à la sécurité des Actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

5.4 DROIT DE REGARD

L'INRS exerce, en conformité avec la législation applicable, un droit de regard sur tout usage de ses Actifs informationnels.

6. SÉCURITÉ DES ACTIFS INFORMATIONNELS

L'INRS adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité des Actifs informationnels et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent à des façons de faire reconnues et généralement utilisées.

Le comité responsable de la sécurité et de la gestion de l'Information est le comité sur l'accès à l'information et à la protection des renseignements personnels, de la sécurité et de la gestion de l'Information (**Comité AIPRP-SGI**) dont la composition est prévue à la *Politique sur la gouvernance en matière de protection des renseignements personnels de l'INRS*. L'INRS

confie au Comité AIPRP-SGI le mandat d'assurer la sécurité et la gestion de ses Actifs informationnels notamment par les moyens décrits ci-après.

6.1 GESTION DU RISQUE

Dans le but d'orienter les mesures de sécurité des Actifs informationnels et conformément à la *Politique de gestion des risques* de l'INRS, le SRI, en collaboration avec le SAGD, procède à l'identification et l'évaluation périodiques des risques qui menacent la confidentialité, l'intégrité ou la disponibilité de l'Information. Des mesures de protection sont ensuite déployées en fonction de l'évaluation des impacts et de la probabilité d'occurrence d'une menace, de façon à atténuer les risques et à les maintenir à un niveau acceptable. Le SRI procède à une évaluation des risques préalablement à toute acquisition ou tout changement important aux Actifs informationnels sous sa responsabilité.

6.2 GESTION DES VULNÉRABILITÉS

Le SRI déploie des mesures pour maintenir à jour les logiciels afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les risques d'Incident de sécurité ou de cyberattaque. Il effectue une veille des menaces pertinentes pour l'environnement de l'INRS.

6.3 GESTION DES INCIDENTS

Le SRI met en place un processus de gestion des Incidents de sécurité. Ce processus décrit les moyens de détection, de documentation et de réponse aux Incidents. Le Comité AIPRP-SGI est responsable de la tenue du Registre des Incidents et doit être informé des Incidents de sécurité.

6.4 PLAN DE RELÈVE ET DE CONTINUITÉ INFORMATIQUE

L'INRS s'assure en tout temps de la continuité des activités nécessaires à la réalisation de sa mission, y compris lors d'un sinistre ou d'une défaillance majeure affectant les Actifs informationnels jugés essentiels. Conformément à la *Politique de continuité des activités et de gestion des mesures d'urgence* et à la *Politique de gestion des risques*, le SRI est responsable de prévoir un plan de relève et de continuité informatique.

6.5 GESTION DE L'ACCÈS AUX INFRASTRUCTURES ET À L'INFORMATION

Le SRI contrôle l'accès à ses locaux de même qu'aux Actifs informationnels sous sa responsabilité de manière à empêcher tout accès non autorisé, dommage ou intrusion. L'accès aux Actifs informationnels n'est permis qu'aux Personnes détentrices de l'Information et aux personnes autorisées à y accéder par celles-ci. Le SRI révise les accès à ses locaux et aux Actifs informationnels sous sa responsabilité sur une base périodique.

Il est notamment interdit d'accéder aux boîtes courriel ainsi qu'à toute Information appartenant à un membre de la Communauté INRS, qu'il se trouve dans un ordinateur

ou dans un quelconque répertoire, et ce, à moins d'obtenir son consentement ou d'obtenir l'autorisation de la Personne responsable de l'accès à l'information et la protection des renseignements personnels ainsi que l'autorisation de la Direction de l'administration.

6.6 PROTECTION DE L'INTÉGRITÉ DE L'INFRASTRUCTURE ET DE L'INFORMATION

Le SRI et chaque Personne détentrice de l'Information prend les mesures utiles pour protéger les Actifs informationnels sous sa responsabilité contre toute atteinte à leur Intégrité, incluant notamment les risques d'incendie, d'inondation, de survoltage, de coupures de courant et autres pannes de diverses natures.

6.7 LE CYCLE DE VIE DES SYSTÈMES D'INFORMATION

Le SRI et chaque Personne détentrice de l'Information prend les mesures utiles pour protéger la confidentialité et l'Intégrité de l'Information et assurer sa disponibilité. Le SRI est responsable d'établir des mesures d'encadrement et de suivi tout au long du cycle de vie des Actifs informationnels sous sa responsabilité.

6.8 CLASSIFICATION DES ACTIFS INFORMATIONNELS

Les Actifs informationnels sont catégorisés et inventoriés. Ils sont classifiés et protégés selon leur degré de sensibilité et selon les exigences qui y sont liées pour assurer leur sécurité.

7. RESPONSABILITÉS DES MEMBRES DE LA COMMUNAUTÉ INRS

Tout membre de la Communauté INRS est responsable d'appliquer et de respecter la Politique, directives ou toute autre indication en découlant.

Chaque personne qui accède à une Information, qui la consulte ou qui la traite est responsable de l'utilisation qu'elle en fait et doit procéder de manière à la protéger. À cette fin, elle doit notamment signer la déclaration d'engagement prévue à l'Annexe A de la Politique lors de l'embauche ou de l'inscription.

Chaque membre de la Communauté INRS est responsable :

- des conséquences de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par elle-même ou par une tierce personne, à moins qu'elle démontre que les actions posées par une tierce personne ne découlent pas d'une négligence ou d'une malveillance de sa part;
- d'utiliser les droits d'accès qui lui sont attribués et autorisés ainsi que des Actifs informationnels qui sont mis à sa disposition uniquement dans le cadre approprié à leur utilisation et aux fins auxquelles ils sont destinés;
- de respecter les mesures de sécurité mises en place sur son poste de travail et sur tout autre équipement contenant de l'Information à protéger, et ne pas modifier ou outrepasser la configuration des mesures de sécurité ou les désactiver;

- de prendre part et de compléter les activités de formation et de sensibilisation offertes par l'INRS à ce sujet;
- de collaborer à toute intervention visant à identifier ou à mitiger une menace ou un Incident à la sécurité des Actifs informationnels;
- de se conformer aux exigences légales portant sur l'utilisation des Systèmes d'Information à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- de signaler immédiatement à sa supérieure ou son supérieur immédiat tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des Actifs informationnels de l'INRS;
- de s'abstenir de tout comportement malveillant pouvant porter préjudice ou affecter d'autres personnes ainsi que toute activité illégale, malicieuse ou contraire à la mission de l'INRS;
- au moment de son départ de l'INRS, de remettre les différentes cartes d'identité et d'accès, le matériel informatique ainsi que les Actifs informationnels qui avaient été mis à sa disposition dans le cadre de l'exercice de ses fonctions ou de ses études.

8. GOUVERNANCE

La Politique attribue la gestion de la sécurité des Actifs informationnels de l'INRS à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

8.1 COMITÉ D'AUDIT

Le comité d'audit est responsable de ce qui suit :

- examiner les enjeux, les orientations, les stratégies et les pratiques générales en matière d'Actifs informationnels;
- s'assurer de la mise en place de pratiques et normes en matière de sécurité des actifs informationnels, incluant la cybersécurité, et en assurer le suivi;
- examiner les enjeux et risques des Actifs informationnels, incluant la gestion et la sécurité de l'Information, et en assurer le suivi.

8.3 COMITÉ AIPRP-SGI

Le Comité AIPRP-SGI est responsable de ce qui suit :

- examiner le rendement et l'efficacité de la sécurité des Actifs informationnels et émettre des recommandations;
- proposer les ajustements aux documents normatifs en matière de gestion et de sécurité des Actifs informationnels;
- de s'assurer du traitement conforme des Incidents de confidentialité et la tenue du Registre des Incidents;
- examiner, prioriser et recommander aux instances les orientations stratégiques, les plans d'action, les priorités d'intervention, les documents normatifs en lien avec la sécurité de l'Information et voir à leur mise en œuvre.

8.4 PERSONNE DÉTENTRICE DE L'INFORMATION

Toute Personne détentrice de l'Information est responsable, pour les Actifs informationnels sous sa responsabilité, de ce qui suit :

- participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans en matière de sécurité des Actifs informationnels;
- participer à la catégorisation des Actifs Informationnels;
- veiller à ce que des mesures de sécurité des Actifs informationnels, y compris celles liées au respect des exigences légales de protection des renseignements personnels, soient mises en place et appliquées;
- s'assurer de l'adéquation des mesures de sécurité des Actifs informationnels en vigueur par rapport aux risques identifiés;
- déterminer les personnes autorisées à y accéder et les niveaux d'accès octroyés;
- participer à l'analyse de risques et s'assurer de la prise en charge des risques résiduels.

8.5 DIRECTION DE L'ADMINISTRATION

La Direction de l'administration est responsable de ce qui suit :

- l'application de la Politique;
- la recommandation au conseil d'administration de la nomination de la personne agissant à titre de CSIO;
- la désignation des personnes agissant à titre de COMSI.

8.6 DIRECTRICE OU DIRECTEUR DU SRI

La directrice ou le directeur du SRI est responsable de ce qui suit :

- soumettre au Comité AIPRP-GSI, pour analyse, les orientations stratégiques, les plans d'action, les priorités d'intervention, les cadres de gestion et les directives et procédures en lien avec la sécurité des Actifs informationnels et voir à leur mise en œuvre;
- définir et mettre en œuvre des mesures et des processus formels de sécurité des Actifs informationnels permettant d'assurer la gestion des risques, de l'accès à l'Information et des Incidents en matière de sécurité de l'Information;
- définir les exigences de sécurité des Actifs informationnels lors de la réalisation de projets de développement ou d'acquisition de Systèmes d'Information.

8.7 CSIO

La CSIO est responsable de la sécurité des Actifs informationnels au sein de l'INRS et s'assure du respect des exigences légales, gouvernementales et organisationnelles en cette matière.

8.8 COMSI

Les COMSI agissent sur le plan opérationnel et ont les responsabilités suivantes :

- intervenir dans la mise en œuvre de mesures et apporter le soutien nécessaire au CSIO, notamment en matière de la gestion des Incidents et des risques en sécurité des Actifs informationnels;
- représenter l'INRS auprès du Réseau d'alerte gouvernemental;
- appliquer le processus de gestion des menaces, vulnérabilités et Incidents (GMVI) à l'INRS.

8.9 DIRECTRICE OU DIRECTEUR DU SERVICE DES RESSOURCES HUMAINES

En matière de sécurité des Actifs informationnels, la directrice ou le directeur du Service des ressources humaines doit :

- vérifier, au besoin, les antécédents judiciaires des candidats à l'embauche et des membres du personnel impliqués dans la sécurité des Actifs informationnels;
- imposer les sanctions appropriées lors de violation des Documents normatifs touchant à la sécurité des Actifs informationnels.

8.10 SAGD

Le SAGD est responsable de la gestion documentaire aux termes de la *Loi sur la gouvernance et la gestion des Actifs informationnels* et ainsi, de mettre en œuvre des mesures de sécurité de l'Information indépendamment de son support ainsi que des mesures de destruction sécuritaire de l'Information sous sa garde.

9. SANCTIONS

Toute contravention à la Politique, en plus des recours et pénalités prévus à la législation, peut entraîner le retrait des droits d'accès aux Actifs informationnels ou l'imposition de mesures administratives et disciplinaires pouvant aller jusqu'au congédiement ou à l'expulsion, selon la nature et la gravité de la faute commise.

En cas de non-respect de la Politique, l'INRS peut également exercer tout recours approprié contre tout membre de la Communauté INRS, et ce, même après la fin de son lien d'emploi ou de ses études à l'INRS.

De même, toute contravention à la Politique par une tierce personne, est passible des sanctions prévues au contrat le liant à l'INRS ou en vertu des dispositions de la législation applicable en la matière.

10. MISE À JOUR

La Politique est mise à jour au besoin ou, au minimum, tous les cinq ans.

11. DISPOSITIONS FINALES

La Politique entre en vigueur dès son adoption par le conseil d'administration.

ANNEXE A

FORMULAIRE DE DÉCLARATION D'ENGAGEMENT

Dans les 30 jours de l'entrée en vigueur de la *Politique de gouvernance en matière de sécurité et de gestion de l'information* ou de l'entrée en fonction ou de l'inscription, tout membre de la Communauté INRS doit déclarer avoir pris connaissance de cette politique, en comprendre le sens, la portée et s'engager à la respecter.

Tout membre de la Communauté INRS a l'obligation de protéger les Actifs informationnels mis à sa disposition par l'INRS. À cette fin, il est responsable :

1. de se conformer à la présente Politique et à tout autre document normatif de l'INRS en matière de sécurité de l'Information et d'utilisation des Actifs informationnels;
2. des conséquences de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par elle-même ou par une tierce personne, à moins qu'elle démontre que les actions posées par une tierce personne ne découlent pas d'une négligence ou d'une malveillance de sa part;
3. d'utiliser les droits d'accès qui lui sont attribués et autorisés ainsi que des Actifs informationnels qui sont mis à sa disposition uniquement dans le cadre approprié à leur utilisation et aux fins auxquelles ils sont destinés;
4. de respecter les mesures de sécurité mises en place sur son poste de travail et sur tout autre équipement contenant de l'Information à protéger, et ne pas modifier ou outrepasser la configuration des mesures de sécurité ou les désactiver;
5. de prendre part et de compléter les activités de formation et de sensibilisation offertes par l'INRS à ce sujet;
6. de collaborer à toute intervention visant à identifier ou à mitiger une menace ou un Incident à la sécurité des Actifs informationnels;
7. de se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
8. de signaler immédiatement à sa supérieure ou son supérieur immédiat tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des Actifs informationnels de l'INRS;
9. de s'abstenir de tout comportement malveillant pouvant porter préjudice ou affecter d'autres personnes ainsi que toute activité illégale, malicieuse ou contraire à la mission de l'INRS;
10. au moment de son départ de l'INRS, de remettre les différentes cartes d'identité et d'accès, le matériel informatique ainsi que les Actifs informationnels qui avaient été mis à sa disposition dans le cadre de l'exercice de ses fonctions ou de ses études.

Je déclare avoir pris connaissance de la *Politique de gouvernance en matière de sécurité et de gestion de l'information*. Je reconnais mes responsabilités en matière de sécurité informatique et de confidentialité de l'information.

_____
Nom

_____ _____
Signature Date