



SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER

L'annexe suivante donne un aperçu de quelques lois, règlements, politiques et lignes directrices régissant la recherche sensible au Canada, en Australie, dans l'Union européenne, en France, en Allemagne, aux Pays-Bas, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis. Ces pays ont été choisis par le comité d'experts en raison de leurs liens avec le Canada, qui se traduisent par une coopération internationale étroite dans les domaines de la sécurité nationale et des sciences, par des similitudes sociopolitiques, ou parce que ces pays ont adopté des lois et des politiques transcendant les frontières et qui s'appliquent aux chercheurs canadiens.

Les documents examinés dans la présente annexe ont été sélectionnés sur la base de l'expertise du comité d'experts et de recherches documentaires effectuées à partir de plusieurs bases de données et sites Web de ministères et d'organismes gouvernementaux pertinents au Canada et dans d'autres pays. L'annexe donne un aperçu des principales politiques qui ont éclairé les délibérations du comité d'experts entre juillet 2024 et juin 2025. Elle ne vise pas à fournir un aperçu exhaustif de toutes les approches nationales et infranationales visant à garantir la sécurité de la recherche ni à énumérer toutes les méthodes permettant de reconnaître et de protéger les recherches sensibles. L'évolution rapide du contexte géopolitique pourrait entraîner la modification ou la suppression complète dans un avenir proche de certains des documents examinés aux présentes.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Canada : Lois, règlements, politiques et lignes directrices pour la reconnaissance et la protection de la recherche sensible

Politiques promulguées par le gouvernement du Canada

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement du Canada	<i>Loi sur les licences d'exportation et d'importation (LLEI) (GC, 1985a) et Liste des marchandises et technologies d'exportation contrôlée (GC, 2021).</i>	Habilite le gouvernement du Canada à restreindre les exportations de certains produits.	Résultats de recherche susceptibles de compromettre la sécurité et la souveraineté nationales, de mettre en danger la sécurité des personnes au Canada, de perturber la fourniture de services essentiels ou de nuire à un pays étranger ou à une région du monde.	<u>Reconnaissance</u> : Liste de biens et d'articles. <u>Protection</u> : Limitation des exportations vers certains pays, personnes et entités.	Tous les chercheurs et établissements de recherche.
Gouvernement du Canada	<i>Loi sur les mesures économiques spéciales (GC, 1992) et Loi sur les Nations Unies (GC, 1985b).</i>	Habilite le gouvernement du Canada à restreindre les activités auprès de personnes et d'entités sanctionnées.	Toutes les recherches susceptibles d'enfreindre les sanctions gouvernementales (p. ex., la mise à disposition de biens à une partie sanctionnée ou le transfert/l'exportation de technologies et de données techniques).	<u>Reconnaissance</u> : Personnes et entités sanctionnées. <u>Protection</u> : Interdiction de mener des activités auprès de personnes et d'entités sanctionnées.	Tous les chercheurs et établissements de recherche.
Gouvernement du Canada	<i>Loi sur la production de défense (LPD) (GC, 1985c) et Programme des marchandises contrôlées (PMC) (GC, 2016; SPAC, 2024, 2025).</i>	Contrôle les activités de recherche touchant des marchandises considérées comme ayant une importance sur le plan militaire ou de la sécurité nationale.	Recherche pouvant impliquer l'accès à des marchandises contrôlées ou la mise au point de telles marchandises.	<u>Reconnaissance</u> : Les marchandises contrôlées sont énumérées dans l'annexe de la LPD. <u>Protection</u> : L'enregistrement dans le PMC est nécessaire pour examiner, posséder ou transférer des marchandises contrôlées au Canada.	Tous les chercheurs et établissements de recherche.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement du Canada	<i>Loi sur la sûreté et la réglementation nucléaires (GC, 1997) et Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire (GC, 2010).</i>	Habilite la Commission canadienne de sûreté nucléaire à « réglementer le développement, la production et l'utilisation de l'énergie nucléaire, ainsi que la production, la possession et l'utilisation des substances nucléaires, de l'équipement réglementé et des renseignements réglementés » (GC, 1997).	Recherche impliquant des substances, équipements et renseignements nucléaires contrôlés.	<u>Reconnaissance</u> : Liste de substances, d'équipements et de renseignements nucléaires contrôlés. <u>Protection</u> : Restrictions à l'importation et à l'exportation.	Tous les chercheurs et établissements de recherche.
Gouvernement du Canada	<i>Loi de mise en œuvre de la Convention sur les armes chimiques (GC, 1995).</i>	Met en œuvre la <i>Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction</i> au Canada.	Recherche impliquant des produits chimiques toxiques ou des précurseurs répertoriés.	<u>Reconnaissance</u> : Listes de produits chimiques toxiques ou de précurseurs. <u>Protection</u> : Restrictions à l'importation et à l'exportation; restrictions à la production, à l'utilisation, à l'acquisition ou à la possession d'un produit chimique toxique ou d'un précurseur.	Tous les chercheurs et établissements de recherche.
Innovation, Sciences et Développement économique Canada (ISDE)	Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes (RTSAP) (ISDE, 2023a).	Tire parti du financement fédéral de la recherche pour interdire à ceux qui souhaitent faire progresser les domaines de recherche en technologies sensibles de maintenir des affiliations actives avec des organismes de recherche nommément désignés.	Domaines de recherche en technologies sensibles.	<u>Reconnaissance</u> : 11 domaines de recherche en technologies sensibles et organismes de recherche désignés. <u>Protection</u> : Les exigences en matière d'affiliation, de financement et de soutien en nature s'appliquent à l'ensemble de l'équipe de recherche; toutefois, seuls les chercheurs ayant un rôle désigné sont tenus de présenter une attestation confirmant qu'ils respectent les exigences de la Politique sur la RTSAP.	Chercheurs sollicitant un financement fédéral.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
ISDE	Lignes directrices sur la sécurité nationale pour les partenariats de recherche (LDSNPR) (ISDE, 2023b).	Intègre les considérations de sécurité nationale dans le développement, l'évaluation et le financement de la recherche.	Les domaines de recherche sensible, les domaines de recherche sensibles couverts par la LLEI et les domaines de recherche supplémentaires qui « peuvent être considérés comme sensibles ».	<p><u>Reconnaissance :</u></p> <ul style="list-style-type: none"> • 11 domaines de recherche sensible et d'autres domaines, y compris les minéraux critiques, les infrastructures critiques, les grands ensembles de données et les données à caractère personnel. Énumérés à l'annexe A de la LDSNPR, ils « peuvent être considérés comme sensibles ». • Recherche avec un partenaire visé. <p><u>Protection :</u> Mesures d'atténuation des risques, notamment la constitution d'une équipe de recherche solide, l'évaluation des motivations des partenaires, la cybersécurité et la gestion des données, ainsi qu'un accord sur l'utilisation prévue des résultats de la recherche.</p>	Chercheurs sollicitant du financement fédéral.
Gouvernement du Canada	<i>Loi sur les agents pathogènes humains et les toxines (LAPHT) (GC, 2009) et Règlement sur les agents pathogènes humains et les toxines (RAPHT) (GC, 2024).</i>	<p>La LAPHT établit « un régime pour promouvoir la sûreté des agents pathogènes humains et des toxines afin de protéger la santé et la sécurité publiques contre les risques qu'ils présentent. »</p> <p>Le RAPHT précise comment l'Agence de santé publique du Canada (ASPC) mettra en œuvre la LAPHT et autorise les activités réglementées impliquant des agents pathogènes humains et des toxines (ASPC, 2024).</p>	Recherche scientifique sur les agents pathogènes humains et les toxines.	<p><u>Reconnaissance :</u> Agents pathogènes humains et toxines, et agents pathogènes humains et toxines réglementés ayant un potentiel de double usage (c.-à-d. agents biologiques à cote de sécurité élevée ou ABCSE) (ASPC, 2018).</p> <p><u>Protection :</u> Licences et habilitations de sécurité.</p>	« Organismes et personnes qui exercent des activités comportant la manipulation d'agents pathogènes humains et des toxines, dont les universités, les laboratoires de santé publique, le secteur privé, les hôpitaux et les services diagnostiques de santé humaine ou animale » (ASPC, 2024).

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
ASPC	Norme canadienne sur la biosécurité (ASPC, 2022) et Ligne directrice canadienne sur la biosécurité : le double usage dans la recherche en sciences de la vie (ASPC, 2018).	Aide les parties réglementées à reconnaître les recherches susceptibles d'avoir un double usage et à en atténuer les risques.	Potentiel de recherche à double usage.	<p><u>Reconnaissance</u> : La recherche à double usage est reconnue sur la base de plusieurs questions, notamment les caractéristiques d'un organisme ou d'une toxine, la nocivité, la nouveauté, les risques de modification et le potentiel d'utilisation abusive.</p> <p><u>Protection</u> : Évaluation des risques pour déterminer si les mesures de biosécurité et de sûreté biologique existantes sont adaptées à la recherche à double usage. Des précautions supplémentaires peuvent être nécessaires, notamment des contrôles administratifs plus stricts, des niveaux de confinement plus élevés, une formation sur le potentiel de double usage de la recherche, des examens périodiques de la recherche en vue d'applications à double usage et un plan d'échange d'informations.</p>	« Installations qui détiennent un permis visant des agents pathogènes et des toxines (ci-après, un permis) en vertu de la LAPHT et du RAPHT » (ASPC, 2022).

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Canada : Lois, règlements, politiques et lignes directrices au Canada pour la reconnaissance et la protection de la recherche sensible

Rapports des organisations non gouvernementales

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
U15	Protéger la recherche au Canada : Guide des politiques et des pratiques universitaires (U15, 2023).	« Recueil de lignes directrices institutionnelles fondées sur des politiques et des pratiques avant-gardistes visant à protéger la recherche des risques d'une participation à la recherche mondiale. »	Toute la recherche universitaire.	<u>Reconnaissance</u> : Pas de mécanisme précis. <u>Protection</u> : Cinq pratiques institutionnelles : <ul style="list-style-type: none">• cadres de gouvernance et de risque;• diligence raisonnable, évaluation et gestion des risques;• communication, éducation et mise en commun des connaissances;• sécurité des réseaux et des appareils;• sécurité de la recherche et sécurité du campus.	Universités.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Allemagne : Lois, politiques et orientations en Allemagne pour la reconnaissance et la protection de la recherche sensible

Lois promulguées par le gouvernement de la République fédérale d'Allemagne

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de l'Allemagne	<i>Loi fondamentale de la République fédérale d'Allemagne (Gov. of Germany, 1949).</i>	Codification des protections constitutionnelles pour la liberté de la recherche en Allemagne.	Toutes les recherches.	Sans objet.	Tous les chercheurs en Allemagne.

Rapports et lignes directrices des organisations non gouvernementales en Allemagne

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Société Max-Planck pour le développement des sciences (MPG)	Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks (MPG, 2017).	« [L'objectif est de] prévenir l'utilisation abusive de la recherche et d'éviter les risques grâce à une autorégulation fondée sur des principes éthiques... [établit] une procédure permettant aux chercheurs de mieux résoudre les incertitudes éthiques et de prévenir les accusations de conduite contraire à l'éthique ».	Toutes les recherches.	<p><u>Reconnaissance</u> : « Les chercheurs devraient... tenir compte des conséquences et des possibilités d'application ou d'utilisation abusive de leurs travaux, et de la possibilité de les contrôler. Les projets de recherche à risque devraient... être précédés d'une évaluation des risques associés pour la dignité humaine, la vie et le bien-être des personnes, l'environnement et toute autre valeur importante protégée par la constitution ».</p> <p><u>Protection</u> : Minimisation des risques tout au long du cycle de vie de la recherche; documentation et communication des risques aux comités d'éthique et aux autres acteurs institutionnels; refus de publier certaines informations; renoncement à la recherche en dernier recours; formation.</p>	« Tous ceux qui travaillent dans les institutions de la Société Max Planck, ou avec leurs ressources dans d'autres lieux. »

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Académie nationale des sciences Léopoldine (Leopoldina); Fondation allemande pour la recherche (DFG)	Scientific Freedom and Scientific Responsibility Recommendations for Handling of Security-Relevant Research (Leopoldina et DFG, 2022).	Offrir une assistance aux chercheurs et aux établissements de recherche « pour répondre aux questions éthiques » et « contribuer à la définition de normes et de codes de conduite allant au-delà des normes statutaires pour les chercheurs travaillant dans les domaines où des considérations de sécurité entrent en jeu ».	Recherche où des considérations de sécurité entrent en jeu et recherche préoccupante sur le plan de la sécurité.	<p><u>Reconnaissance</u> : L'analyse des risques « devrait... tenir compte des conséquences et des possibilités d'application ou d'utilisation abusive de la [recherche], ainsi que de sa contrôlabilité ».</p> <p><u>Protection</u> : Réduction des risques grâce à des mesures de sécurité physique et de cybersécurité; examen des résultats de la recherche avant publication; filtrage des partenariats; documentation et communication des risques; renoncement à la recherche en dernier recours.</p>	Recherche financée par les pouvoirs publics.
German Aerospace Center (DLR)	Due Diligence in Science (DLR, 2024).	Soutien aux établissements et aux universités dans l'élaboration et la mise en œuvre d'instruments de diligence raisonnable pour évaluer les risques liés à la coopération scientifique.	Recherche scientifique impliquant des partenariats.	<p><u>Reconnaissance</u> : Évaluations systématiques des partenaires, des sujets de recherche et des établissements à l'aide de critères de filtrage – comme le pays d'origine, la sensibilité du sujet et l'accès à l'infrastructure – ainsi que vérifications des antécédents et formulaires d'auto-divulgation pour détecter les risques en matière de sécurité, d'éthique ou de droit.</p>	Gestionnaires d'universités et d'instituts de recherche. Chercheurs principaux dans les universités et les établissements.
Leibniz Association	Risk Management in International Scientific Collaboration (Leibniz Association, 2021).	Fournit des conseils sur la mise en place de « processus internes... qui peuvent être utilisés pour effectuer des évaluations standard, pragmatiques et non bureaucratiques des collaborations avec des partenaires individuels ou des pays, au cas par cas ».	Recherche scientifique impliquant des partenariats internationaux.	<p><u>Protection</u> : Respect de la législation (p. ex, contrôle des exportations), maintien de la transparence et d'accords clairs avec les partenaires, protection de la propriété intellectuelle et des données par des contrôles d'accès et le cryptage, sensibilisation des chercheurs et mise en place de stratégies de sortie et de plans d'urgence pour les collaborations à haut risque.</p>	Instituts de l'Association Leibniz.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Aotearoa Nouvelle-Zélande : Politiques, règlements et orientations de la Nouvelle-Zélande en matière de repérage et de protection de la recherche sensible

Documents promulgués par le gouvernement de la Nouvelle-Zélande

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
<p>Gouvernement de la Nouvelle-Zélande; Centre for the Protection of National Infrastructure; Science New Zealand; Universities New Zealand</p>	<p>Trusted Research: Guidance for Institutions and Researchers (Gov. of New Zealand, 2020).</p>	<p>L'accent est mis sur la collaboration internationale en matière de recherche. Le document énumère et décrit les risques liés aux acteurs étrangers hostiles dans des contextes comme les voyages internationaux, le financement, les chercheurs invités, la cybersécurité et la recherche à l'étranger.</p>	<p>Toute la recherche universitaire.</p>	<p><u>Reconnaissance</u> : La recherche conjointe et la recherche appliquée sont spécifiquement mentionnées ici. C'est au chercheur qu'il incombe de déterminer ce qu'est une recherche sensible, ce qui peut se faire par le biais des contrôles à l'exportation ou de la législation sur la protection de la vie privée. La détermination des partenariats à risque se fait par le biais d'une diligence raisonnable et de vérifications des conflits d'intérêts.</p> <p><u>Protection</u> : Il incombe au chercheur de respecter les contrôles à l'exportation et la législation sur la protection de la vie privée, de compartimenter la recherche et d'en contrôler l'accès, de faire des considérations de sécurité un élément des propositions de financement, de protéger ses partenaires, de faire preuve de transparence et de maintenir la visibilité, ainsi que de gérer la cybersécurité et la recherche à l'étranger.</p>	<p>Les établissements de recherche et les chercheurs, et en particulier les chercheurs travaillant dans les domaines des STIM, de l'innovation, des technologies à double usage, des technologies émergentes et des domaines de recherche commercialement sensibles.</p>

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de la Nouvelle-Zélande, Ministry of Foreign Affairs and Trade [ministère des Affaires étrangères et du Commerce]	New Zealand Strategic Goods List (Gov. of New Zealand, 2024).	La Nouvelle-Zélande contrôle l'exportation des biens figurant sur cette liste. Les biens contrôlés ne peuvent être exportés de Nouvelle-Zélande, ce qui comprend l'exportation électronique de logiciels et de technologies figurant sur la liste, à moins qu'une licence ou une autorisation d'exportation n'ait été obtenue.	Biens contrôlés inclus dans cette liste.	<p><u>Reconnaissance</u> : Les biens figurant sur cette liste.</p> <p><u>Protection</u> : Une licence d'exportation est nécessaire.</p>	Tous les chercheurs et établissements de recherche.
Gouvernement de la Nouvelle-Zélande; Centre for the Protection of National Infrastructure; Business New Zealand; Universities New Zealand; Science New Zealand; New Zealand Trade and Enterprise; NZ Growth Capital Partners; Callaghan Innovation	Due Diligence Assessments For Espionage and Foreign Interference Threats (Gov. of New Zealand, 2022).	Fournit une vue d'ensemble des risques de partenariat et de l'importance de la gestion des risques dans le cadre de la diligence raisonnable. Conseils sur les questions à poser lors de l'établissement de nouvelles relations d'affaires; recommandations sur les accords de gouvernance, les exigences en matière de financement et les risques liés aux données comme à la propriété intellectuelle.	Recherche menée en partenariat avec des acteurs étrangers.	<p><u>Reconnaissance</u> : Les technologies sensibles sont définies comme ayant un double usage, actuel ou futur. Pour déterminer si une technologie est incluse, le document se réfère aux contrôles des exportations de la Nouvelle-Zélande, à l'examen des listes de technologies sensibles d'autres pays, aux informations publiques sur les technologies et à l'avis d'experts.</p> <p><u>Protection</u> : Poser des questions sur ce que l'on sait de l'organisation partenaire, des partenaires nouveaux et existants et de leurs motivations, ainsi que d'autres facteurs à haut risque (p. ex., les atteintes à l'intégrité ou à la loi).</p>	Les personnes, les organisations et les entreprises qui s'associent à des acteurs étrangers.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Aotearoa Nouvelle-Zélande : Politiques, règlements et orientations de la Nouvelle-Zélande en matière de repérage et de protection de la recherche sensible

Rapports d'organisations non gouvernementales en Nouvelle-Zélande

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Universities New Zealand	Trusted Research Protective Security Requirements: Guide for Senior University Leaders in Aotearoa New Zealand (UNZ, 2022).	Le contenu du document vise à protéger les valeurs universitaires tout en évitant le détournement ou l'utilisation abusive de la recherche à des fins militaires ou d'ingérence étrangère. Concerne la recherche internationale et la manière de garantir l'intégrité et la sécurité des collaborations, ainsi que la protection de la propriété intellectuelle, des infrastructures de recherche, des savoirs autochtones, des données de recherche, des informations personnelles et des chercheurs.	Toute la recherche universitaire, en particulier lorsqu'elle comporte une collaboration internationale.	<p><u>Reconnaissance</u> : La recherche sensible n'est liée qu'aux contrôles des exportations et aux contrôles « attrape-tout », tandis que la recherche collaborative et la recherche appliquée sont considérées comme particulièrement vulnérables au détournement ou à l'utilisation abusive par des acteurs ou des organisations étrangers. Il incombe à l'institution de faire preuve de diligence raisonnable, d'évaluer les risques, de procéder à des audits des risques et d'utiliser le Cadre de gestion des risques fourni dans le document pour éduquer et former les chercheurs et les autres personnes impliquées dans la gestion des risques.</p> <p><u>Protection</u> : Restreindre l'accès aux installations et aux données, garantir des protocoles de cybersécurité adéquats, adhérer aux contrôles des exportations et aux contrôles « attrape-tout ».</p>	Principalement les hauts responsables d'universités, mais des conseils pertinents peuvent être utiles pour les facultés, les départements et les divisions de services au sein des universités. En outre, certaines recommandations peuvent concerner les conseils d'université et plus particulièrement les sous-comités chargés de l'audit et de la gestion du risque.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Australie : Politiques, règlements et orientations en Australie pour la reconnaissance et la protection de la recherche sensible.

Documents promulgués par le gouvernement de l'Australie

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de l'Australie	Defence and Strategic Goods List 2021 (Gov. of Australia, 2024a, 2024b).	Le gouvernement australien contrôle l'exportation des biens énumérés dans le document. Cette liste est « modifiée de temps à autre pour tenir compte des changements intervenus dans les divers régimes multilatéraux de non-prolifération et de contrôle des exportations dont l'Australie est membre » (Gov. of Australia, 2024a).	Recherche ayant trait à la défense et aux biens connexes, ou aux biens à double usage.	<u>Reconnaissance</u> : Fournit des listes de biens militaires, non militaires, létaux et à double usage. <u>Protection</u> : Licence d'exportation exigée.	Tous les chercheurs et établissements de recherche.
Gouvernement de l'Australie	Defence Trade Controls Act (Gov. of Australia, 2012).	« Contrôle de la fourniture, de la publication et du courtage de biens et technologies militaires et à double usage, de nature matérielle ou immatérielle » (Gov. of Australia, 2023a).	Données et technologies considérées comme militaires ou à double usage.	<u>Reconnaissance</u> : Utilise des listes de biens militaires, non militaires, létaux et à double usage. - <u>Protection</u> : « Cela permet au ministre de la Défense d'autoriser ou d'interdire la fourniture, la publication et/ou le courtage de biens et de technologies » (Gov. of Australia, 2023a).	Tous les chercheurs et établissements de recherche.
Gouvernement de l'Australie	Critical Technologies Statement (Gov. of Australia, 2023b); List of Critical Technologies in the National Interest (Gov. of Australia, 2023c).	Décrit certains des avantages et des risques des technologies critiques, ainsi que les mesures prises par le gouvernement pour gérer ces risques.	Recherche impliquant des technologies critiques.	<u>Reconnaissance</u> : Les technologies concernées sont indiquées dans la liste des technologies critiques. (Gov. of Australia, 2023c). <u>Protection</u> : Sans objet, car cette liste n'a pas pour but de réglementer ou de contrôler les technologies.	Gouvernement de l'Australie.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de l'Australie, Department of Health and Aged Care [ministère de la Santé et des Soins aux personnes âgées]	Security Sensitive Biological Agents (SSBA) Regulatory Scheme (Gov. of Australia, 2024c).	Désigne les ABCSE préoccupants, fournit un cadre législatif pour la réglementation des ABCSE et maintient l'accès des personnes ayant un besoin légitime de manipuler des ABCSE dans des laboratoires sécurisés, tout en limitant les actes de bioterrorisme.	Recherche impliquant les ABCSE.	<p><u>Reconnaissance</u> : Une liste des ABCSE est fournie dans la List of Security Sensitive Biological Agents (Gov. of Australia, 2016).</p> <p><u>Protection</u> : Les normes relatives aux ABCSE « définissent les exigences auxquelles l'entité doit satisfaire pour garantir la sécurité physique lors de la manipulation, du stockage, de l'élimination et du transport des ABCSE et 'des agents biologiques suspectés d'être des ABCSE, ainsi que la sécurité du personnel et de l'information » (Gov. of Australia, 2013).</p>	Entités et installations qui travaillent avec des ABCSE, connus ou suspectés.
Gouvernement de l'Australie; Department of Foreign Affairs and Trade [ministère des Affaires étrangères et du Commerce]	<i>Australia's Foreign Relations (State and Territory Arrangements) Act 2020</i> (Gov. of Australia, 2020).	« Crée un régime visant à garantir que les accords entre les gouvernements des États ou des Territoires et les entités gouvernementales étrangères n'affectent pas négativement les relations extérieures de l'Australie et n'entrent pas en conflit avec sa politique étrangère » (Gov. of Australia, 2021).	Les universités publiques qui concluent des partenariats avec des entités étrangères n'ayant ' pas d'autonomie institutionnelle.	<p><u>Reconnaissance</u> : Fournit des critères pour déterminer si une université étrangère 'est dénuée d'autonomie institutionnelle.</p> <p><u>Protection</u> : Les universités doivent informer le ministre des Affaires étrangères de leur intention de conclure un accord avec un pays étranger, ou doivent le faire lorsqu'elles en concluent un. Le ministre doit examiner la proposition de négociation ou de conclusion de l'accord et décider s'il l'approuve.</p>	Universités publiques.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Australian Research Council (ARC); Gouvernement de l'Australie	ARC Countering Foreign Interference Framework (ARC, 2023).	Décrit les rôles et les responsabilités de l'ARC, des établissements universitaires, des chercheurs et des acteurs gouvernementaux en ce qui concerne les processus d'octroi de subventions à différents stades du cycle de vie de la recherche.	Toutes les propositions de recherche soumises à l'ARC en vue d'un financement.	<p><u>Reconnaissance</u> : Si des chercheurs demandent un financement pour des recherches sur des technologies figurant sur la liste des technologies critiques, l'ARC examine une série de facteurs pour déterminer les risques éventuels.</p> <p><u>Protection</u> : Si l'ARC détermine l'existence d'un risque, les organismes de sécurité nationaux peuvent être mobilisés. L'administration de l'université d'accueil sera alors avisée et tenue de fournir une stratégie ou un plan d'atténuation des risques.</p>	Universités et chercheurs.
Australian Security Intelligence Organisation (ASIO); Gouvernement de l'Australie	Protect your Research, Collaborate with Care (ASIO, n.d.).	Se concentre sur la protection de la recherche contre les acteurs étrangers mal intentionnés qui tentent d'accéder à des informations ou à des données sensibles ou de voler la propriété intellectuelle. Décrit les méthodes par lesquelles des acteurs étrangers ou leurs mandataires peuvent approcher des chercheurs ou des universités en vue d'établir des partenariats, détaille les types de comportement dont il faut se méfier et fournit des conseils sur la protection de la recherche au sein des établissements universitaires. Présente des études de cas, des informations sur la manière de signaler les problèmes de sécurité et des liens vers des ressources supplémentaires.	Toute la recherche universitaire.	<p><u>Reconnaissance</u> : Axée sur les domaines de recherche dans lesquels l'Australie excelle et sur les types de technologies critiques ou de recherche à double usage qui intéressent les puissances étrangères et leurs mandataires. Fournit des conseils sur l'élaboration de politiques de gestion des risques qui permettent de reconnaître les domaines de recherche et les partenaires de recherche qui présentent les risques les plus élevés.</p> <p><u>Protection</u> : Former le personnel à la sensibilisation aux menaces, l'aider à détecter les menaces pour la sécurité, veiller à ce que la recherche collaborative respecte les exigences et les lois gouvernementales (p. ex., les contrôles à l'exportation), veiller à ce que le personnel déclare ses affiliations et proposer une formation sur la manière de protéger la recherche lors des voyages à l'étranger.</p>	Administrateurs et responsables de la sécurité dans les universités.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Australie : Politiques, règlements et orientations en Australie pour la reconnaissance et la protection de la recherche sensible.

Rapports d'organisations non gouvernementales en Australie

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
<p>University Foreign Interference Taskforce (UFIT) avec la participation du gouvernement de l'Australie, d'Universities Australia et du Group of Eight Australia</p>	<p>Guidelines to Counter Foreign Interference In the Australian University Sector (UFIT, 2021).</p>	<p>Aide les universités à renforcer ou à créer des outils, des cadres et des ressources permettant de reconnaître et d'atténuer les risques d'ingérence étrangère. Parmi les sujets de préoccupation, citons : les données compromises, la perte de propriété intellectuelle, les atteintes à la réputation, les risques pour l'économie et la sécurité nationale, l'autocensure et les conflits avec la liberté universitaire. Les lignes directrices visent à fournir une approche équilibrée de la reconnaissance et de l'atténuation des risques sans compromettre la liberté universitaire et une culture scientifique ouverte.</p>	<p>Toute la recherche universitaire.</p>	<p><u>Reconnaissance :</u> Axée sur l'ingérence étrangère dans les activités de recherche, sans décrire les technologies ou les domaines particuliers susceptibles de présenter un risque plus élevé. Conseils sur les processus de diligence raisonnable et d'évaluation des risques pour déterminer les risques liés à l'influence étrangère.</p> <p><u>Protection :</u> Recommandations ciblées sur la meilleure façon de gérer les risques, avec des conseils sur les cadres de gouvernance et la gestion des risques; la communication, l'éducation et la mise en commun des connaissances; ainsi que la cybersécurité.</p>	<p>Universités et chercheurs.</p>

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



États-Unis : Lois, règlements, politiques et orientations des États-Unis en matière de reconnaissance et de protection de la recherche sensible

Documents promulgués par le gouvernement des États-Unis

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement des États-Unis	<i>The CHIPS and Science Act</i> (Gov. of United States, 2022).	Finance la science et la technologie des États-Unis et vise à les protéger de toute ingérence étrangère.	Recherche dans de nombreux domaines stratégiques, notamment les semi-conducteurs, l'intelligence artificielle, la biotechnologie et l'informatique.	<p><u>Reconnaissance</u> : « entités étrangères préoccupantes » et « pays étrangers préoccupants ».</p> <p><u>Protection</u> : Restreint la collaboration en matière de recherche avec les « entités étrangères préoccupantes » et les « pays étrangers préoccupants ».</p>	L'écosystème de la recherche englobe la recherche financée par le gouvernement fédéral et menée par les départements et les agences gouvernementales, ainsi que les centres de recherche régionaux.
Gouvernement des États-Unis	Presidential Memorandum on United States Government-Supported Research and Development National Security Policy (NSPM-33) (Gov. of United States, 2021) and Guidance for Implementing NSPM-33 (NSTC, 2022).	La NSPM-33 définit la politique de sécurité nationale pour la R et D soutenue par le gouvernement des États-Unis.	Recherche soutenue par les départements et les agences fédéraux.	<p><u>Reconnaissance</u> : Pas de mécanismes particuliers.</p> <p><u>Protection</u> : Approches normalisées de la divulgation d'informations (p. ex., affiliations, nominations, notices biographiques, identifiants numériques persistants pour les chercheurs bénéficiant d'un financement fédéral), identifiants numériques persistants, échange d'informations avec les organismes chargés de l'application de la loi et programmes certifiés de sécurité de la recherche pour les organismes de recherche bénéficiant d'un financement fédéral d'au moins 50 millions de dollars américains.</p>	Départements et agences fédéraux.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement des États-Unis (White House Office of Science and Technology Policy)	Guidelines for Research Security Programs at Covered Institutions (OSTP, 2024).	Les établissements de recherche recevant un financement fédéral supérieur à 50 millions de dollars par an doivent mettre en place un programme de sécurité de la recherche.	Recherche menée par des établissements recevant un financement fédéral supérieur à 50 millions de dollars par an.	<p><u>Reconnaissance</u> : Pas de mécanismes particuliers.</p> <p><u>Protection</u> : Le programme de sécurité de la recherche doit comprendre un programme de cybersécurité, un programme de déclaration des voyages, une formation sur la sécurité de la recherche et une formation sur le contrôle des exportations.</p>	Établissements de recherche recevant un financement fédéral supérieur à 50 millions de dollars.
Gouvernement des États-Unis (The U.S. Department of Commerce's Bureau of Industry and Security (BIS))	Export Administration Regulations (EAR) (US BIS, 2024).	Réglemente les exportations de biens à double usage.	Toute recherche impliquant des biens et des noms d'entreprises, d'instituts de recherche, d'organisations gouvernementales et privées ainsi que des personnes de l'étranger, qui sont assujettis à l'obligation d'obtenir une licence pour l'exportation, la réexportation et/ou le transfert (à l'intérieur d'un même pays) 'de biens spécifiés.	<p><u>Reconnaissance</u> : Une liste d'articles et de noms d'entreprises, d'établissements de recherche, d'organisations gouvernementales et privées et de particuliers étrangers.</p> <p><u>Protection</u> : Des licences d'exportation de biens à double usage sont requises dans certaines situations impliquant la sécurité nationale, la politique étrangère, la pénurie d'approvisionnement, la non-prolifération nucléaire, la technologie des missiles, les armes chimiques et biologiques, la stabilité régionale, la lutte contre la criminalité ou les préoccupations terroristes.</p>	Tous les chercheurs et organismes de recherche exportant des biens à double usage.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement des États-Unis (the Department of Energy, DOE)	Science and Technology Risk Matrix (COGR, 2023). [1] <i>[1] Certaines parties de cette matrice ne sont pas accessibles au public. L'analyse présentée ici est basée sur une présentation faite par le personnel du département de l'Énergie lors de la réunion du groupe multi-agences sur l'évaluation et l'analyse des risques en matière de sécurité de la recherche (Multi-Agency Panel on Research Security Risk Assessment & Analysis) (COGR, 2023) et sur JASON (2024).</i>	Gère les risques liés aux technologies critiques et émergentes pour lesquelles il n'existe pas d'autres mécanismes de contrôle.	Domaines technologiques émergents particuliers.	<u>Reconnaissance</u> : Domaines technologiques émergents associés à la compétitivité économique, à la sécurité nationale ou au leadership scientifique (p. ex., les technologies quantiques, les batteries, l'intelligence artificielle) et interactions avec un pays à risque particulier (Chine, Iran, Corée du Nord, Russie). Les experts en la matière évaluent les progrès réalisés dans chaque domaine et classent la recherche en trois catégories : fondamentale et non sensible, potentiellement sensible et nécessitant des mesures de protection supplémentaires. (JASON, 2024). <u>Protection</u> : Restriction des activités comme « les engagements à l'étranger, les accords de coopération en matière de R et D, les voyages officiels, l'engagement de ressortissants étrangers et l'accès aux projets et aux données qui impliquent des pays à risque (Chine, Russie, Iran et Corée du Nord) »(JASON, 2024).	S'applique aux activités des laboratoires nationaux du département de l'Énergie.
Gouvernement des États-Unis (The Department of Defense, DOD)	Policy on Risk-Based Security Reviews of Fundamental Research (US DOD, 2023).	Cerne et atténue les risques pour la sécurité nationale liés à la recherche financée par le ministère de la Défense.	Se concentre sur les affiliations et les activités des personnes qui mènent des recherches fondamentales.	<u>Reconnaissance</u> : Affiliation préoccupante. <u>Protection</u> : Suggère une panoplie de stratégies de protection, notamment le retrait ou le remplacement d'un cochercheur principal d'une proposition à plusieurs chercheurs, la formation à la sensibilisation aux risques et l'augmentation de la fréquence des rapports.	S'applique à tous les projets sélectionnés pour un financement par le département de la Défense.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
<p>Gouvernement des États-Unis (White House Office of Science and Technology Policy)</p>	<p>The United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential (The Oversight Policy) (Gov. of United States, 2024).</p> <p>The Implementation Guidance to the Oversight Policy (Gov. of United States, 2024).</p>	<p>Cadre de surveillance fédérale pour la conduite et la gestion de certains types de recherches en sciences de la vie, portant sur les agents biologiques et les toxines, et financées par le gouvernement fédéral.</p>	<p>Agents biologiques ou toxines.</p>	<p><u>Reconnaissance</u> : Agents biologiques ou toxines lorsque la recherche relève de la catégorie 1 ou 2 telle que décrite dans la politique.</p> <p><u>Protection</u> : Cadre organisationnel de la supervision de la recherche par les chercheurs principaux, les établissements de recherche et les bailleurs de fonds.</p>	<p>Départements et agences fédéraux qui financent la recherche dans les établissements de recherche aux États-Unis.</p>

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



États-Unis : Lois, règlements, politiques et orientations des États-Unis en matière de reconnaissance et de protection de la recherche sensible

Rapports des organisations non gouvernementales

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
National Academies of Sciences, Engineering, and Medicine (NASEM)	Protecting U.S. Technological Advantage (NASEM, 2022).	Examine la nécessité de limiter la recherche ouverte et « prend en compte les avantages et les inconvénients des options de protection de la technologie ».	Recherche scientifique.	<p><u>Reconnaissance</u> : Suggère une approche coordonnée de la gestion des risques « qui commence par l'identification des acteurs et des moyens par lesquels ils tentent d'utiliser une technologie particulière contre les intérêts ou le leadership technologique des États-Unis ».</p> <p><u>Protection</u> : Définit les stratégies les mieux adaptées pour faire face aux risques qui en découlent.</p>	Dans l'ensemble du gouvernement fédéral.
The Center for Security and Emerging Technologies (CSET)	A New Institutional Approach to Research Security in the United States: Defending a Diverse R&D Ecosystem (Flagg et Arnold, 2021).	Examine comment aborder la question de la sécurité de la recherche menée par le secteur privé.	Recherches menées par le secteur privé.	<p><u>Reconnaissance</u> : Pas de dispositions particulières.</p> <p><u>Protection</u> : Propose la création d'un centre d'échange d'informations public-privé sur la sécurité de la recherche, dirigé par « les universités, les entreprises, les organisations philanthropiques et les pouvoirs publics », qui serait présent dans les centres de R et D les plus actifs. Cet organisme fournirait aux chercheurs, à leurs responsables et aux bailleurs de fonds « des informations de source ouverte, des formations liées à la sécurité, des ressources d'aide à la décision et... une interface avec les partenaires fédéraux ».</p>	Chercheurs, bailleurs de fonds et gestionnaires de la recherche.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
JASON	Fundamental Research Security (JASON, 2019).	Aborde la valeur et les risques associés à l'ouverture de la recherche fondamentale.	La recherche fondamentale, c'est-à-dire « la recherche pure et appliquée en science et en ingénierie, dont les résultats sont normalement publiés et largement disséminés au sein de la communauté scientifique, par opposition à la recherche exclusive et au développement industriel, à la conception, à la production et à l'utilisation des produits, dont les résultats sont normalement restreints pour des raisons d'exclusivité ou de sécurité nationale ». (Gov. of United States, 1985).	<p><u>Reconnaissance et protection :</u></p> <ul style="list-style-type: none"> • Divulgence complète des engagements et des conflits d'intérêts/engagements réels ou potentiels. • Outils spécifiques aux projets pour faciliter l'évaluation des risques dans les collaborations de recherche, les accords de recherche non fédéraux et les subventions. • Éducation et formation sur les conflits d'intérêts et l'engagement. • Coopération avec les services de renseignement et les organismes d'application de la loi afin de partager les risques d'influence étrangère fondés sur des preuves et de renforcer la valeur de la collaboration avec l'étranger. 	Recherche soutenue par la NSF.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
JASON	Safeguarding the Research Enterprise (JASON, 2024).	Définit « les mesures précises que la NSF pourrait prendre pour cerner les domaines de recherche sensibles et décrire les processus que la NSF pourrait utiliser pour assurer la sécurité dans... les domaines de recherche préoccupants ».	Recherche sensible et très sensible.	<p><u>Reconnaissance</u> : Recommande une approche dynamique pour reconnaître les recherches sensibles, sur la base de leurs applications potentielles, des niveaux de préparation technologique et de « l'impact direct et prévisible sur la sécurité nationale des applications de chaque proposition de recherche ».</p> <p><u>Protection</u> : Les stratégies d'atténuation des risques pour les projets de recherche sensibles sont notamment les suivantes « des modifications du champ d'application d'une subvention de recherche, une formation (ou une formation renforcée) du chercheur principal... sur les risques et les protections en matière de sécurité de la recherche, une formation renforcée concernant la publication de résultats potentiellement sensibles, une formation renforcée sur l'identification des personnes préoccupantes qui pourraient être considérées comme des participants ou des collaborateurs potentiels, une augmentation de la fréquence ou de la portée des rapports » et des normes de sécurité physique et de cybersécurité.</p> <p>Les projets de recherche très sensibles doivent être accompagnés de contrôles supplémentaires, notamment « des restrictions à la participation des individus préoccupants, une approbation préalable obligatoire pour les conférences ou les publications, une approbation préalable obligatoire avant la publication de données ou de logiciels en source ouverte ».</p>	Recherche soutenue par la NSF.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



France : Politiques, règlements et orientations en France pour la reconnaissance et la protection de la recherche sensible

Règlements, politiques et lignes directrices promulgués par le gouvernement de la France

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de la France	<i>Décret no 2020-1481 du 30 novembre 2020 portant mesure nationale autorisée par le paragraphe 3 de l'article 6 du règlement (CE) no 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage (Gouv. de la France, 2020).</i>	Mise en œuvre du régime de contrôle des exportations de biens à double usage de l'UE dans le droit national français (CE, 2009).	Découle de la réglementation de l'UE en matière de contrôle des exportations (CE, 2009).	<u>Reconnaissance</u> : Énumère les technologies à double usage conformes aux règlements de l'UE.	Tous les chercheurs et établissements de recherche.
Gouvernement de la France	<i>Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés (Gouv. de la France, 2024).</i>	Arrêté ministériel édictant des exigences supplémentaires en matière de contrôle des exportations pour des technologies précises, comme l'informatique quantique et les technologies adjacentes.	Technologies quantiques.	<u>Reconnaissance</u> : Énumère les technologies quantiques soumises au contrôle des exportations. <u>Protection</u> : Autorisations d'exportation.	Tous les chercheurs et établissements de recherche.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement de la France	Protection du potentiel scientifique et technique et intelligence économique (PPST) (SGDSN, 2012).	Fournit un cadre national pour la supervision de la recherche sensible; introduit des zones à régime restrictif (ZRR) soumises à des exigences en matière d'information et de sécurité physique.	Recherche en « biologie, médecine, agronomie, écologie, géologie, sciences de l'espace, informatique et technologie de l'information, et ingénierie » (Gattolin, 2021).	<p><u>Reconnaissance</u>: Fournit une liste des sujets couverts par la PPST (Gattolin, 2021). Invite les chercheurs à évaluer l'applicabilité de la PPST selon quatre critères : les intérêts économiques de la nation, les arsenaux militaires, la prolifération des armes de destruction massive et le terrorisme (SGDSN, 2012).</p> <p><u>Protection</u>: Exigences en matière de sécurité physique et de cybersécurité pour l'accès aux ZRR; filtrage des personnes demandant l'accès aux ZRR, indépendamment de leur nationalité; les partenariats de recherche impliquant des ZRR sont soumis à l'examen du gouvernement (SGDSN, 2012).</p>	Tous les chercheurs et établissements de recherche.
Gouvernement de la France	Protection numérique du potentiel scientifique et technique de la nation (SGDSN, 2018).	Guide pour la mise en conformité avec les exigences numériques et de cybersécurité fixées par la PPST.	Recherche relevant du champ d'application de la PPST.	<p><u>Reconnaissance</u>: Évaluation des risques pour reconnaître les « informations à régime restrictif » (IRR), un label pour les données sensibles qui bénéficient de protections juridiques similaires à celles qui s'appliquent aux ZRR.</p> <p><u>Protection</u>: Exigences en matière de signalement des incidents de cybersécurité ou d'autres incidents liés aux IRR; protocoles institutionnels pour la reconnaissance et l'étiquetage des IRR; processus de gestion des risques régulièrement revus; adaptation des exigences en matière de sécurité numérique et de cybersécurité au contexte opérationnel des ZRR.</p>	Chercheurs en ZRR ou travaillant avec les IRR.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



France : Politiques, règlements et orientations en France pour la reconnaissance et la protection de la recherche sensible

Rapports des organisations non gouvernementales en France

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Conseil national consultatif pour la biosécurité	Recherches duales à risque : Recommandations pour leur prise en compte dans les processus de conduite de recherche en biologie (Korn <i>et al.</i> , 2019).	Vue d'ensemble de la surveillance de la recherche à double usage préoccupante (RDUP) en France	Recherche universitaire en sciences de la vie.	<p><u>Reconnaissance</u> : Intégrer l'évaluation des risques de double usage dans les processus de recherche, créer des comités de surveillance locaux et former les chercheurs à reconnaître les risques d'utilisation abusive.</p> <p><u>Protection</u> : Surveillance indépendante des projets sensibles, contrôle éthique des publications et contrôle plus strict du transfert et de l'accès aux données biologiques sensibles.</p>	Chercheurs.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Pays-Bas : Politiques, règlements et orientations des Pays-Bas en matière de reconnaissance et de protection de la recherche sensible

Règlements, politiques, lignes directrices et outils promulgués par le gouvernement des Pays-Bas

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement des Pays-Bas	<i>Besluit toepassingsbereik sensitieve technologie (Décision sur le champ d'application 'de la technologie sensible) (Gov. of Netherlands, 2023).</i>	Fournit des détails sur les technologies considérées comme sensibles ou très sensibles. Cette liste s'applique aux activités commerciales (p. ex., les fusions, les investissements) dans les domaines technologiques sensibles. (Stibbe, 2023).	Biens et technologies sensibles.	<p><u>Reconnaissance</u> : Énumère les codes d'exportation pour les technologies sensibles et très sensibles, y compris celles liées aux biens militaires et à double usage.</p> <p><u>Protection</u> : L'approbation du gouvernement est requise pour l'acquisition ou la fusion de toute entreprise travaillant avec des technologies répertoriées (Stibbe, 2023).</p>	Tous les chercheurs et établissements de recherche.
Gouvernement des Pays-Bas	Knowledge security guidelines (Gov. of Netherlands, 2022).	Définit le champ d'application de la sécurité des connaissances et décrit les rôles et responsabilités des acteurs de la sécurité des connaissances; fournit des orientations pour l'analyse des risques; introduit la notion de « joyaux de la couronne » que les établissements devraient protéger en priorité; décrit des stratégies pour la mise en place d'équipes de sécurité institutionnelles; énumère des outils et des approches pour la gestion adaptative des risques.	Domaines de connaissance sensibles	<p><u>Reconnaissance</u> : Analyse des risques au niveau institutionnel pour cerner les technologies et des connaissances sensibles. Obligation de réévaluer périodiquement les technologies cernées.</p> <p><u>Protection</u> : Mise en place d'équipes de sécurité institutionnelles chargées de surveiller les partenariats de recherche, la cybersécurité et la coordination de la sécurité; adaptation des efforts de gestion des risques au cas par cas; définition d'une norme institutionnelle (p. ex., la cybersécurité).</p>	Chercheurs, établissements publics de recherche.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Ministère de l'Éducation, de la Culture et des Sciences des Pays-Bas (OCW)	National Contact Point for Knowledge Security (OCW, s.d.-a, s.d.-b).	Fournir des conseils sur la sécurité des connaissances dans les collaborations internationales en matière de recherche.	Recherche impliquant une collaboration internationale.	<p><u>Reconnaissance</u> : Fournit des conseils sur les domaines de recherche qui pourraient justifier une vigilance accrue sur le plan des partenariats et sur la manière d'évaluer les profils de risque des pays.</p> <p><u>Protection</u> : Regroupe les ressources, les outils et la législation pertinente pour une protection appropriée de la recherche.</p>	Établissements de recherche, chercheurs.
Dutch National Institute for Public Health and the Environment (RIVM)	Biosecurity Office (RIVM, s.d.a).	« Transmet des connaissances et des informations sur la biosécurité et sensibilise à la biosécurité, afin de réduire au minimum le risque d'utilisation abusive d'agents pathogènes, de connaissances et de technologies à haut risque. » (RIVM, s.d.-a).	Recherche impliquant du matériel biologique à haut risque.	<p><u>Reconnaissance</u> : Fournit un questionnaire portant sur le double usage pour repérer les recherches sensibles (RIVM, s.d.b) et regroupe diverses ressources (p. ex., listes de pathogènes, règles de contrôle des exportations).</p> <p><u>Protection</u> : Fournit des bonnes pratiques essentielles pour la gestion des recherches sensibles dans un contexte de biosécurité (RIVM, s.d.-c).</p>	Chercheurs, personnes responsables de la biosécurité institutionnelle.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Pays-Bas : Politiques, règlements et orientations des Pays-Bas en matière de reconnaissance et de protection de la recherche sensible

Rapports d'organisations non gouvernementales aux Pays-Bas

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Royal Netherlands Academy of Arts and Science (KNAW)	Knowledge Security: Academy Position Paper (KNAW, 2023)	Du point de vue de l'Académie, ce rapport examine l'utilisation du terme « sécurité des connaissances » et les principes qui devraient le sous-tendre; il passe ensuite en revue les politiques existantes et proposées sur la base de ces principes, avant de formuler d'autres recommandations sur le plan des politiques.	Recherches menées dans le cadre des <i>Knowledge Security Guidelines</i> .	<u>Reconnaissance</u> : Recommande aux évaluateurs de risques de faire la distinction entre « transfert indésirable de connaissances », « interférence » et « problèmes d'éthique et d'intégrité ». <u>Protection</u> : Critique la perspective d'un filtrage basé sur la nationalité ou les disciplines, arguant que la sensibilisation au niveau institutionnel offre une plus grande sécurité.	Tous les chercheurs et établissements de recherche.
Universities of the Netherlands	Capability Maturity Model: Knowledge Security (UNL, 2024)	Ce modèle est conçu pour « aider les universités à concevoir et à mettre en œuvre leurs politiques de sécurité des connaissances; évaluer en interne le niveau de maturité pour chaque sujet particulier et le niveau de maturité souhaité; se doter des moyens de mettre en place une stratégie interne et une planification en vue d'atteindre le niveau de maturité souhaité; améliorer l'alignement des politiques de sécurité des connaissances des universités en termes de concepts utilisés, et offrir un aperçu des sujets ».	Recherches menées dans le cadre des <i>Knowledge Security Guidelines</i> .	<u>Reconnaissance</u> : Réaffirme les processus des Knowledge Security Guidelines [lignes directrices néerlandaises sur la sécurité des connaissances] (Gov. of Netherlands, 2022), et examine les cadres juridiques, l'évaluation des risques, la formation et la sensibilisation à la reconnaissance. <u>Protection</u> : Fournit un cadre pour des approches de gestion des risques progressive qui peuvent être adaptées au profil de risque. Des pratiques de gestion des risques d'intensité variable sont décrites pour les différentes priorités de la sécurité des connaissances.	Établissements de recherche, chercheurs.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Royaume-Uni : Politiques, règlements et orientations du Royaume-Uni en matière de reconnaissance et de protection de la recherche sensible

Règlements, politiques et lignes directrices promulgués par le gouvernement du Royaume-Uni

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
National Protective Security Authority (NPSA); the National Cyber Security Centre (NCSC), en partenariat avec Universities UK	Trusted Research: Guidance for Academics (NPSA & NCSC, 2024a); Trusted Research: Guidance for Senior Leaders (NPSA & NCSC, 2024b); Trusted Research: Guidance for Industry (NPSA & NCSC, 2022).	Les documents sont destinés à « sensibiliser aux risques que peuvent présenter les collaborations en matière de recherche lorsque l'on travaille avec des organisations ou des partenaires de recherche ayant des liens avec des nations dont les valeurs démocratiques et éthiques sont différentes des nôtres » (NPSA et NCSC, 2024a). Les documents « [décrivent] les risques pour la recherche et l'innovation au Royaume-Uni; [aident] les chercheurs, les universités britanniques et les partenaires industriels à avoir confiance dans la collaboration internationale et à prendre des décisions éclairées concernant les risques; [et expliquent] comment protéger la recherche et le personnel contre le vol, l'utilisation abusive ou l'exploitation potentiels. Ils sont produits en consultation avec les universités et l'industrie, et conçus pour aider le secteur britannique de la recherche et de l'innovation, un leader mondial, à tirer le meilleur parti de la collaboration internationale tout en protégeant la propriété intellectuelle (PI), la recherche sensible et les informations personnelles » (NPSA et NCSC, 2024a).	Toute la recherche universitaire; toute la recherche industrielle, en particulier les chercheurs dans les domaines des STIM, les technologies à double usage, les technologies émergentes et les domaines de recherche commercialement sensibles.	<p>Reconnaissance : Il incombe au chercheur de déterminer si sa recherche est commercialement sensible, si elle est potentiellement brevetable, si elle est liée à la défense/sécurité nationale ou si elle peut avoir des applications futures à double usage. Ces orientations renvoient aux contrôles à l'exportation pour des conseils supplémentaires et à la National Security and Investment Act pour 17 secteurs de l'économie qui sont plus risqués pour la sécurité nationale (NPSA et NCSC, 2024a). Les partenaires industriels sont encouragés à utiliser les niveaux de maturité technologique pour déterminer si leur recherche est sensible. (NPSA et NCSC, 2022).</p> <p>Protection : Il incombe au chercheur de s'assurer que les collaborations sont sûres et de le démontrer dans les propositions de financement (conflits d'intérêts transparents, cybersécurité adéquate, diligence raisonnable en ce qui concerne les questions de sécurité nationale (NPSA et NCSC, 2024a). Les hauts dirigeants ont des responsabilités dans la gestion de l'accès aux installations sensibles et aux plateformes informatiques (NPSA et NCSC, 2024b).</p>	Chercheurs universitaires, universités, hauts dirigeants et partenaires industriels.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Gouvernement du Royaume-Uni	Academic Technology Approval Scheme (ATAS) (Gov. of United Kingdom, 2025a).	Les chercheurs et les étudiants de certains pays qui viennent au Royaume-Uni pour étudier des sujets sensibles doivent obtenir un certificat.	Domaines de recherche sensibles.	<u>Reconnaissance</u> : Les domaines de recherche sensibles sont classés selon les codes de la hiérarchie des agrégateurs communs; les candidats de certains pays doivent vérifier si leur domaine d'étude ou de recherche est inclus.	Chercheurs et universités.
Gouvernement du Royaume-Uni	UK Strategic Export Control List (Gov. of United Kingdom, 2025b).	Les contrôles à l'exportation limitent l'exportation et la communication de technologies sensibles ou de biens stratégiques (Gov. of United Kingdom, 2023).	Technologies sensibles figurant sur la liste.	<u>Reconnaissance</u> : La liste est fournie (liste consolidée des biens stratégiques militaires et à double usage dont l'exportation nécessite une autorisation). <u>Protection</u> : Le fait de ne pas obtenir les licences appropriées peut entraîner des poursuites pénales. (Gov. of United Kingdom, 2023).	Tous les chercheurs et établissements de recherche.
Gouvernement du Royaume-Uni	<i>National Security and Investment Act</i> (Gov. of United Kingdom, 2024a, 2024b).	Permet au gouvernement d'intervenir dans l'acquisition ou la vente de recherches ou de technologies sensibles si elles sont jugées préjudiciables à la sécurité nationale.	Technologies sensibles figurant sur la liste.	<u>Reconnaissance</u> : Si la technologie en question figure sur la liste des 17 secteurs sensibles de l'économie, le vendeur est légalement tenu d'en informer le gouvernement. <u>Protection</u> : Contrôle des acquisitions par le gouvernement et intervention en cas de menace probable pour la sécurité nationale.	Tous les citoyens et toutes les entreprises.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
UK Research and Innovation (UKRI)	Trusted Research and Innovation: Principles and Expectations (UKRI, 2025).	La recherche et l'innovation de confiance (R&IC) impliquent « la protection de la propriété intellectuelle, de la recherche sensible, du personnel et de l'infrastructure du Royaume-Uni contre le vol, l'utilisation abusive et l'exploitation potentiels »; les principes de gestion de la R&IC s'appliquent à l'UKRI et les attentes s'appliquent aux bénéficiaires de subventions.	Toutes les recherches financées par l'UKRI.	<u>Reconnaissance</u> : Les bénéficiaires sont tenus de faire preuve de diligence raisonnable à l'égard des partenaires du projet. <u>Protection</u> : Gestion de l'information et de l'échange des connaissances par la cybersécurité, la séparation des données, la gestion de l'accès aux données, l'application des droits de propriété intellectuelle et le respect des contrôles à l'exportation.	Chercheurs, universités et UKRI.

Rapports d'organisations non gouvernementales au Royaume-Uni

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Universities UK (UUK)	Managing Risks in Internationalisation : Security Related Issues (Universities UK, 2020).	Fournit aux instances dirigeantes et aux cadres supérieurs des universités des conseils sur la manière de gérer l'internationalisation dans le cadre universitaire. Il s'agit notamment d'établir des structures de gouvernance claires et d'identifier les membres du personnel responsables de la gestion des risques. Les stratégies de protection de la réputation, des valeurs, des personnes, des campus et des partenariats sont abordées. Décrit les types de changements qui peuvent être nécessaires pour faire face à l'internationalisation, tels que : des changements dans la prise de conscience et la compréhension des individus; des changements dans les systèmes, les processus et les comportements institutionnels; et des changements dans les systèmes et les processus intersectoriels.	Toute la recherche universitaire.	<u>Reconnaissance</u> : Processus de diligence raisonnable pour repérer les risques relatifs au partenariat, formation et éducation à la sensibilisation et à la gestion des risques. <u>Protection</u> : Mesures en matière de cybersécurité, respect de la législation sur le contrôle des exportations.	Chefs d'établissement et organes exécutifs des universités.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
<p>UK Research Integrity Office (UKRIO)</p>	<p>Code of Practice for Research (UKRIO, 2023).</p>	<p>Encourage « la bonne conduite dans la recherche et aide à prévenir les erreurs et les fautes professionnelles, afin d'aider les organisations et les chercheurs à mener des recherches de la plus haute qualité et à maintenir une culture de recherche saine ». Couvre « les domaines de bonnes pratiques en matière de recherche généralement inclus dans les politiques organisationnelles pour la conduite de la recherche, en s'appuyant sur les bonnes pratiques existantes et les expériences de l'UKRIO en matière de bonne conduite de la recherche et d'inconduite ».</p>	<p>Toutes les recherches.</p>	<p><u>Reconnaissance</u>: Suggère que les organismes et les chercheurs procèdent à des évaluations des risques afin de déterminer les risques pour « l'organisme ou la recherche, ou encore la santé, la sécurité, le bien-être et la santé mentale des chercheurs et des participants à la recherche, ainsi que le public, l'environnement et la sécurité nationale ».</p>	<p>« Les chercheurs individuels et les organismes qui effectuent, financent, accueillent ou participent d'une autre manière à la recherche. »</p>

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Union européenne : Politiques, règlements et orientations de l'Union européenne en matière de reconnaissance et de protection de la recherche sensible

Règlements, politiques, lignes directrices et outils promulgués par l'UE

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Commission européenne (CE)	<i>Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) (Règlement UE 2021/821) (CE, 2021a)</i>	Définit les « biens à double usage »; énumère les technologies et les sujets relevant du champ d'application de la réglementation; établit les paramètres du régime de contrôle des exportations dans l'UE, y compris l'harmonisation avec les accords et traités internationaux.	Logiciels et technologies pouvant être utilisés à des fins civiles et militaires, y compris la recherche sur les biens énumérés ou impliquant ces derniers.	<p><u>Reconnaissance</u> : Fournit une liste des biens contrôlés.</p> <p><u>Protection</u> : Autorisation d'exportation par les autorités compétentes.</p> <p>Les contrôles sur les transferts de technologie ne s'appliquent pas aux informations relevant du « domaine public » et à la « recherche scientifique fondamentale ».</p>	Tous les chercheurs et établissements de recherche des États membres de l'UE.
CE	Recommandation (UE) 2021/1700 du 15 septembre 2021 relative aux programmes internes de conformité pour les contrôles de la recherche portant sur les biens à double usage en vertu du règlement 2021/821 (CE, 2021b)	Guide l'application du Règlement 2021/821 aux chercheurs et aux établissements.	Voir ci-dessus.	<p><u>Reconnaissance</u> : Lignes directrices pour l'évaluation des risques; filtrage des partenariats de recherche; évaluation du niveau de préparation technologique; listes des domaines de recherche sensibles; liste des scénarios; liste des signaux d'alerte potentiels au cours de la procédure de diligence raisonnable.</p> <p><u>Protection</u> : « Contrôles « attrape-tout » (c'est-à-dire contrôles des biens à double usage ne figurant pas sur la liste); instructions sur l'établissement de rapports et d'audit; orientations en matière de sécurité physique et de sécurité de l'information.</p>	Organismes de recherche, chercheurs, directeurs de recherche et personnel des organismes de recherche chargés de la conformité.

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
CE	Recommandation (UE) 2023/2113 de la Commission du 3 octobre 2023 relative aux domaines technologiques critiques pour la sécurité économique de l'Union en vue d'une évaluation approfondie des risques avec les États membres (CE, 2023).	Propose un processus d'évaluation des risques à mener conjointement par les États membres de l'UE dans quatre domaines technologiques clés.	Recherche dans les domaines technologiques critiques.	<p><u>Reconnaissance</u> : Énumère les domaines technologiques à haut risque : semi-conducteurs avancés, intelligence artificielle, technologies quantiques et biotechnologies.</p> <p><u>Protection</u> : Établit les principes directeurs pour l'évaluation des risques liés aux technologies à haut risque dans les États membres de l'UE.</p>	Organismes de recherche, chercheurs, directeurs de recherche et personnel des organismes de recherche chargés de la conformité.
CE	Recommandation du Conseil sur le renforcement de la sécurité de la recherche (CE, 2024).	Fournit des orientations sur le renforcement de la sécurité de la recherche dans l'UE.	« La recherche sur les "connaissances et technologies critiques" renvoie aux connaissances et technologies, incluant le savoir-faire, dans des domaines émergents et de rupture et dans des domaines essentiels à la compétitivité économique, au bien-être social et à la sécurité de l'Union et de ses États membres et dans lesquels, par conséquent, une dépendance excessive à l'égard de pays tiers n'est pas souhaitable. »	<p><u>Reconnaissance</u> : Analyse de risque basée sur le profil institutionnel de l'organisation de l'UE, le sujet de recherche et le profil de risque des pays et organisations partenaires.</p> <p><u>Protection</u> : L'utilisation d'accords de partenariat pour définir les protections de la propriété intellectuelle, les stratégies de sortie pour les partenaires non conformes et les mesures de sécurité physique et de cybersécurité, y compris la compartimentation.</p>	UE, États membres de l'UE, organismes de recherche et organismes de financement de la recherche.
CE	EU Grants: How to Complete Your Ethics Self-Assessment (CE, 2021c).	Conseils sur le respect de l'éthique de la recherche, y compris l'utilisation abusive potentielle des résultats de la recherche.	Propositions de recherche et recherches soutenues par un certain nombre de programmes de financement de l'UE.	<p><u>Reconnaissance</u> : Demande aux candidats de soumettre une évaluation des risques avec leur proposition.</p> <p><u>Protection</u> : Suggère des mesures comme la formation à la sécurité de la recherche, des restrictions à la publication et des ajustements à la conception de la recherche.</p>	Candidats et bénéficiaires des programmes de subventions de l'UE.

SÉCURITÉ DE LA RECHERCHE AU CANADA ET À L'ÉTRANGER



Union européenne : Politiques, règlements et orientations de l'Union européenne en matière de reconnaissance et de protection de la recherche sensible

Outils des organisations non gouvernementales dans l'UE

Auteur	Titre	Résumé	Champ d'application	Mécanismes de reconnaissance et de protection	Application
Fédération européenne des académies des sciences et des humanités (ALLEA)	Code de conduite européen pour l'intégrité en recherche (ALLEA, 2023).	Présente des principes de haut niveau et des responsabilités éthiques qui soutiennent une recherche sûre et responsable.	Toutes les recherches.	<u>Protection :</u> Promouvoir une recherche responsable en encourageant la prise de conscience des risques, le respect des normes juridiques et éthiques, la protection des données et la conclusion d'accords de collaboration formels.	Chercheurs de l'UE.

- ALLEA (All European Academies). (2023). The European Code of Conduct for Research Integrity. Berlin, Germany: ALLEA.
- ARC (Australian Research Council). (2023). ARC Countering Foreign Interference Framework. Canberra, Australia: ARC.
- ASIO (Australian Security Intelligence Organisation). (s.d.). Protect your Research, Collaborate with Care. Canberra, Australia: ASIO.
- ASPC (Agence de la santé publique du Canada). (2018). Ligne directrice canadienne sur labiosécurité : le double usage dans la recherche en sciences de la vie. Ottawa, ON : Gouvernement du Canada.
- ASPC (Agence de la santé publique du Canada). (2022). Norme canadienne sur la biosécurité, troisième édition. Ottawa, ON : Gouvernement du Canada.
- ASPC (Agence de la santé publique du Canada). (2024). Foire aux questions (FAQ) : Règlements. Extrait en août 2024, de <https://www.canada.ca/fr/sante-publique/organisation/mandat/a-propos-agence/lois-reglements/politique-prestation-lignes-directrices-exigences-reglementaires/foire-questions-faq-reglements.html>.
- CE (Commission européenne). (2009). Règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage (refonte).
- CE (Commission européenne). (2021a). Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte).
- CE (Commission européenne). (2021b). Recommandation (UE) 2021/1700 de la Commission du 15 septembre 2021 relative aux programmes internes de conformité pour les contrôles de la recherche portant sur les biens à double usage en vertu du règlement (UE) 2021/821 du Parlement européen et du Conseil instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage. Bruxelles, Belgique : CE.
- CE (Commission européenne). (2021c). EU Grants : How to Complete Your Ethics Self-Assessment. Bruxelles, Belgique : CE.
- CE (Commission européenne). (2023). Recommandation (UE) 2023/2113 de la Commission du 3 octobre 2023 relative aux domaines technologiques critiques pour la sécurité économique de l'Union en vue d'une évaluation approfondie des risques avec les États membres. Strasbourg, France : CE.
- CE (Commission européenne). (2024). Council Recommendation on Enhancing Research Security. Bruxelles, Belgique : CE.
- COGR (Council on Governmental Relations). (2023). Multi-Agency Panel on Research Security Risk Assessment & Analysis. Washington, D.C.: COGR.
- DLR (German Aerospace Center). (2024). Due Diligence in Science. Cologne, Germany: DLR.
- Flagg, M. et Arnold, Z. (2021). A New Institutional Approach to Research Security in the United States. Washington, D.C.: Center for Security and Emerging Technology.

- Gattolin, A. (2021). Mission d'information « Influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences. » Paris, France : Sénat de la France.
- GC (Gouvernement du Canada). (1985a). Loi sur les licences d'exportation et d'importation (L.R.C. (1985), ch. E-19).
- GC (Gouvernement du Canada). (1985b). Loi sur les Nations Unies (L.R.C. (1985), ch. U-2).
- GC (Gouvernement du Canada). (1985c). Loi sur la production de défense (L.R.C. (1985), ch. D-1).
- GC (Gouvernement du Canada). (1992). Loi sur les mesures économiques spéciales (L.C. 1992, ch. 17).
- GC (Gouvernement du Canada). (1995). Loi de mise en œuvre de la Convention sur les armes chimiques (L.C. 1995, ch. 25).
- GC (Gouvernement du Canada). (1997). Loi sur la sûreté et la réglementation nucléaires (L.C. 1997, ch. 9).
- GC (Gouvernement du Canada). (2009). Loi sur les agents pathogènes humains et les toxines (L.C. 2009, ch. 24)
- GC (Gouvernement du Canada). (2010). Règlement sur le contrôle de l'importation et de l'exportation aux fins de la non-prolifération nucléaire (DORS/2000-210).
- GC (Gouvernement du Canada). (2016). Règlement sur les marchandises contrôlées (DORS/2001-32).
- GC (Gouvernement du Canada). (2021). Liste des marchandises et technologies d'exportation contrôlée (DORS/89-202).
- GC (Gouvernement du Canada). (2024). Règlement sur les agents pathogènes humains et les toxines (DORS/2015-44).
- Gouv. de la France. (2024). Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies associés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés.
- Gouv. de la France. (2020). Décret n° 2020-1481 du 30 novembre 2020 portant mesure nationale autorisée par le paragraphe 3 de l'article 6 du règlement (CE) no 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.
- Gov. of Australia (Gouvernement de l'Australie). (2013). Security Sensitive Biological Agent (SSBA) Standards. Canberra, Australia: Gov. of Australia.
- Gov. of Australia (Gouvernement de l'Australie). (2016). SSBA – Fact sheet 5 – List of Security Sensitive Biological Agents. Canberra, Australia: Department of Health and Aged Care.
- Gov. of Australia (Gouvernement de l'Australie). (2020). Australia's Foreign Relations (State and Territory Arrangements) Act 2020.
- Gov. of Australia (Gouvernement de l'Australie). (2021). Australia's Foreign Relations (State and Territory Arrangements) Act 2020: Fact Sheet 1 – Overview. Canberra, Australia: Department of Foreign Affairs and Trade.
- Gov. of Australia (Gouvernement de l'Australie). (2023a). Australian Government legislation and codes. Extrait en août 2024, de <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/templates-and-tools/australian-government-legislation-and-codes>.

- Gov. of Australia (Gouvernement de l'Australie). (2023b). Critical technologies statement. Extrait en septembre 2024, from <https://www.industry.gov.au/publications/critical-technologies-statement>.
- Gov. of Australia (Gouvernement de l'Australie). (2023c, 19 mai). List of critical technologies in the national interest. <https://www.industry.gov.au/node/92356>. Extrait en septembre 2024, de <https://www.industry.gov.au/publications/list-critical-technologies-national-interest>.
- Gov. of Australia (Gouvernement de l'Australie). (2024a). Defence and Strategic Goods List 2024. Canberra, Australia: Gov. of Australia.
- Gov. of Australia (Gouvernement de l'Australie). (2024b). Explanatory Statement: Customs Act 1901, Defence and Strategic Goods List 2021. Canberra, Australia: Government of Australia.
- Gov. of Australia (Gouvernement de l'Australie). (2024c). Security Sensitive Biological Agents (SSBA) Regulatory Scheme. Extrait en août 2024, from <https://www.health.gov.au/our-work/ssba-regulatory-scheme>.
- Gov. of Australia (Gouvernement de l'Australie). (2012). Defence Trade Controls Act 2012.
- Gov. of Germany (Gouvernement de la République fédérale d'Allemagne, Bundesministerium des Innern und für Heimat). (1949). Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 19 December 2022 (Federal Law Gazette I p. 2478).
- Gov. of Netherlands (Gouvernement des Pays-Bas). (2023). Besluit toepassingsbereik sensitieve technologie.
- Gov. of Netherlands (Gouvernement des Pays-Bas). (2022). National Knowledge Security Guidelines: Secure International Collaboration. The Hague, the Netherlands: Gov. of Netherlands.
- Gov. of New Zealand (Gouvernement de la Nouvelle-Zélande). (2022). Due Diligence Assessments for Espionage and Foreign Interference Threats. Wellington, New Zealand: Protective Security Requirements.
- Gov. of New Zealand (Gouvernement de la Nouvelle-Zélande). (2024). New Zealand Strategic Goods List. Wellington, New Zealand: Ministry of Foreign Affairs and Trade.
- Gov. of New Zealand (Gouvernement de la Nouvelle-Zélande). (2020). Trusted Research: Guidance for Institutions and Researchers. Wellington, New Zealand: Centre for the Protection of National Infrastructure, Science New Zealand & Universities New Zealand.
- Gov. of United Kingdom (Gouvernement du Royaume-Uni). (2024a). National Security and Investment Act 2021.
- Gov. of United Kingdom (Gouvernement du Royaume-Uni). (2024b). National Security and Investment Act: Details of the 17 types of notifiable acquisitions. Extrait en juin 2025, de <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions/national-security-and-investment-act-guidance-on-notifiable-acquisitions>.

- Gov. of United Kingdom (Gouvernement du Royaume-Uni). (2025a). Academic Technology Approval Scheme (ATAS). Extrait en août 2024, de <https://www.gov.uk/guidance/academic-technology-approval-scheme>.
- Gov. of United Kingdom (Gouvernement du Royaume-Uni). (2025b). UK Strategic Export Control List. London, United Kingdom: United Kingdom Department for Business and Trade.
- Gov. of United Kingdom (Gouvernement du Royaume-Uni). (2023). Export controls: Dual-use items, software and technology, goods for torture and radioactive sources. Extrait en août 2024, de <https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources>.
- Gov. of United States (Gouvernement des États-Unis). (2021). Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. Washington, D.C.: Gov. of United States.
- Gov. of United States (Gouvernement des États-Unis). (2022). CHIPS and Science Act.
- Gov. of United States (Gouvernement des États-Unis). (2024). United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential. Washington, D.C.: Gov. of United States.
- Gov. of United States (Gouvernement des États-Unis). (1985). NSDD-189: National Policy on the Transfer of Scientific, Technical and Engineering Information. Washington, D.C.: Gov. of United States.
- ISDE (Innovation, Sciences et Développement économique Canada). (2023a). Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes. Ottawa, ON : Gouvernement du Canada.
- ISDE (Innovation, Sciences et Développement économique Canada). (2023b). Lignes directrices sur la sécurité nationale pour les partenariats de recherche. Ottawa, ON : Gouvernement du Canada.
- JASON. (2019). Fundamental Research Security. McLean, VA: MITRE Corporation.
- JASON. (2024). Protectioning the Research Enterprise. McLean, VA: MITRE Corporation.
- KNAW (Royal Netherlands Academy of Arts and Sciences). (2023). Knowledge Security: Academy Position Paper. Amsterdam, Netherlands : KNAW.
- Korn, H., Pironneau, O. et Fagot-Largeault, A. (2019). Recherches duales à risque : Recommandations pour leur prise en compte dans les processus de conduite de recherche en biologie. Paris, France : Académie des sciences.
- Leibniz Association. (2021). Risk Management in International Scientific Collaboration. Berlin, Germany: Leibniz Association.
- Leopoldina et DFG (Académie nationale des sciences Léopoldine et Fondation allemande pour la recherche). (2022). Scientific Freedom and Scientific Responsibility Recommendations for Handling of Security-Relevant Research. Halle, Germany: Leopoldina & DFG.
- MPG (Société Max-Planck pour le développement des sciences). (2017). Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks. Munich, Germany: MPG.

- NASEM (National Academies of Sciences, Engineering, and Medicine). (2022). Protecting U.S. Technological Advantage. Washington, D.C.: National Academies Press.
- NPSA et NCSC (National Protective Security Authority and National Cyber Security Centre). (2022). Trusted Research: Guidance for Industry. London, United Kingdom: NPSA & NCSC.
- NPSA et NCSC (National Protective Security Authority and National Cyber Security Centre). (2024a). Trusted Research: Guidance for Academics. London, United Kingdom: NPSA & NCSC.
- NPSA et NCSC (National Protective Security Authority and National Cyber Security Centre). (2024b). Trusted Research: Guidance for Senior Leaders. London, United Kingdom: NPSA & NCSC.
- NSTC (National Science and Technology Council). (2022). Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development. Washington, D.C.: Subcommittee on Research Security; Joint Committee on the Research Environment.
- OCW (Ministère de l'Éducation, de la Culture et des Sciences des Pays-Bas). (s.d.a). About us: submit your question to the National Contact Point. Extrait en mai 2025, de <https://english.loketkennisveiligheid.nl/about-us>.
- OCW (Ministère de l'Éducation, de la Culture et des Sciences des Pays-Bas). (s.d.b). National Contact Point for Knowledge Security. Extrait en août 2024, de <https://english.loketkennisveiligheid.nl/>.
- OSTP (White House Office of Science and Technology Policy). (2024). Guidelines for Research Security Programs at Covered Institutions. Washington, D.C.: OSTP.
- RIVM (Dutch National Institute for Public Health and the Environment). (s.d.a). Biosecurity Office. Extrait en août 2024, de <https://www.bureaubiosecurity.nl/en>.
- RIVM (Dutch National Institute for Public Health and the Environment). (s.d.b). Dual-Use Quickscan. Extrait en mai 2024, de <https://dualusequickscan.com/en/>.
- RIVM (Dutch National Institute for Public Health and the Environment). (s.d.c). Pillars of good practice. Extrait en septembre 2024, de <https://www.bureaubiosecurity.nl/en/pillars-of-good-practice>.
- SGDSN (Secrétariat général de la défense et de la sécurité nationale). (2012). Circulaire Interministerielle de mise en oeuvre du dispositif de protection du potentiel scientifique et technique de la nation. Paris, France : SGDSN.
- SGDSN (Secrétariat général de la défense et de la sécurité nationale). (2018). Protection numérique du potentiel scientifique et technique de la nation. Paris, France : SGDSN.
- SPAC (Services publics et Approvisionnement Canada). (2024). Marchandises contrôlée : examen, possession ou transfert. Extrait en juillet 2024, de <https://www.canada.ca/fr/services-publics-approvisionnement/services/securite-industrielle/marchandises-controlees.html>.

- SPAC (Services publics et Approvisionnement Canada). (2025). S'inscrire au Programme des marchandises contrôlées. Extrait en juin 2025, de <https://www.canada.ca/fr/services-publics-approvisionnement/services/securite-industrielle/marchandises-controlees/a-propos-programme/inscrire.html>.
- Stibbe. (2023). Ready, set, go! The Dutch national security screening FDI regime takes off. Extrait en août 2024, from <https://www.stibbe.com/publications-and-insights/ready-set-go-the-dutch-national-security-screening-fdi-regime-takes-off>.
- U15. (2023). Protéger la recherche au Canada : Guide des politiques et des pratiques universitaires s.l. : U15.
- UFIT (University Foreign Interference Taskforce). (2021). Guidelines to Counter Foreign Interference in the Australian University Sector. Canberra, Australia: Government of Australia.
- UKRI (UK Research and Innovation). (2025). UKRI Trusted Research and Innovation: Principles and Expectations. London, United Kingdom: UKRI.
- UKRIO (United Kingdom Research Integrity Office). (2023). Code of Practice for Research: Promoting Good Practice and Preventing Misconduct. Croyden, United Kingdom: UKRIO.
- Universities UK. (2020). Managing Risks in Internationalisation: Security Related Issues. London, United Kingdom: Universities UK.
- UNL (Universities of the Netherlands). (2024). Capability Maturity Model: Knowledge Security. The Hague, the Netherlands: UNL.
- UNZ (Universities New Zealand – Te Pōkai Tara). (2022). Trusted Research Protective Security Requirements: Guide for Senior University Leaders in Aotearoa New Zealand. Wellington, New Zealand: UNZ.
- US BIS (Bureau of Industry and Security of the U.S. Department of Commerce). (2024). Export Administration Regulations, 15 CFR.
- US DOD (United States Department of Defense). (2023). Policy on Risk-Based Security Reviews of Fundamental Research. Washington, D.C.: US DOD.