RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

This document provides an overview of select laws, regulations, policies, and guidance governing sensitive research in Canada, Aotearoa New Zealand, Australia, the European Union, France, Germany, the Netherlands, the United Kingdom, and the United States. These jurisdictions were selected by the *Expert Panel on Sensitive Research of Concern* based on their connections to Canada through close international cooperation in the domains of national security and science, sociopolitical similarities, and/or because they have enacted legislation and policies that transcend jurisdictional borders and apply to Canadian researchers.

References reviewed in this document were identified based on the expertise of the *Expert Panel on Sensitive Research of Concern* and literature searches using several databases and websites of relevant government departments and agencies in Canada and foreign jurisdictions. This document provides a snapshot of key policies that informed the CCA's report *Balancing Research Security and Open Science,* assembled between July 2024 and June 2025, and is not intended to give an exhaustive overview of all national and subnational approaches to ensuring research security or list all methods for identifying and safeguarding sensitive research. The quickly changing geopolitical context may result in some of the documents reviewed in this appendix being altered or entirely removed in the near future.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

Canada: Laws, regulations, policies, and guidance for identifying and safeguarding sensitive research

Policies adopted by the Government of Canada

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of Canada	*Export and Import Permits Act* (EIPA) (GC, 1985a) and *Export Control List* (GC, 2021).	Empowers the Government of Canada to restrict exports of certain goods.	Research outputs that can jeopardize national security and sovereignty, endanger the safety of people in Canada, disturb the provision of essential services, or harm a foreign country or region of the world.	Identify: A list of goods and items. Safeguard: Limitations on exports to certain countries, people, and entities.	All researchers and research institutions.
Government of Canada	*Special Economic Measures Act* (GC, 1992) and *United Nations Act* (GC, 1985b).	Empowers the Government of Canada to restrict activities with sanctioned persons and entities.	All research that can violate government sanctions (e.g., making goods available to a sanctioned party or transferring/exporting technology and technical data).	Identify: Sanctioned persons and entities. Safeguard: Prohibits activities with sanctioned persons and entities.	All researchers and research institutions.
Government of Canada	*Defense Production Act* (DPA) (GC, 1985c) and the Canadian Controlled Goods Program (CGP) (GC, 2016; PSPC, 2024, 2025).	Controls research activities with goods deemed to have military or national security significance.	Research that can involve access to or the development of controlled goods.	Identify: Controlled goods are listed in the schedule to the DPA. Safeguard: Registration in the CGP is necessary to examine, possess or transfer controlled goods in Canada.	All researchers and research institutions.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of Canada	*Nuclear Safety and Control Act* (GC, 1997) and *Nuclear Non-Proliferation Import and Export Control Regulations* (GC, 2010).	Empowers the Canadian Nuclear Safety Commission "to regulate the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment, and prescribed information" (GC, 1997).	Research involving controlled nuclear substances, equipment, and information.	Identify: A list of controlled nuclear substances, equipment, and information. Safeguard: Import and export restrictions.	All researchers and research institutions.
Government of Canada	*Chemical Weapons Convention Implementation Act* (GC, 1995).	Implements the *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction* in Canada.	Research involving listed toxic chemicals or precursors.	Identify: Lists of toxic chemicals or precursors. Safeguard: Import and export restrictions; restrictions on producing, using, acquiring or possessing a toxic chemical or precursor.	All researchers and research institutions.
Innovation, Science and Economic Development Canada (ISED)	Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) (ISED, 2023a).	Leverages federal research funding to prohibit those aiming to advance sensitive technology research areas from maintaining active affiliations with named research organizations.	Sensitive technology areas.	Identify: 11 sensitive technology areas and named research organizations. Safeguard: The requirements for affiliation, funding, and in-kind support apply to the entire research team; however, only researchers with named roles are required to submit an attestation confirming their compliance with the STRAC policy's requirements.	Researchers applying for federal funding.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
ISED	National Security Guidelines for Research Partnerships (NSGRP) (ISED, 2023b).	Integrates national security considerations into the development, evaluation, and funding of research.	Sensitive technology research areas, sensitive research areas covered by EIPA, and additional research areas that "can be considered sensitive."	<u>Identify</u>: • 11 sensitive technology research areas, and other areas, including critical minerals, critical infrastructure, large datasets and personal data listed in Annex A of the NSGRP that "can be considered sensitive"; • Research with a qualifying partner <u>Safeguard</u>: Risk mitigation measures, including building a strong research team; assessing partners' motivations; cybersecurity and data management; and agreement on the intended use of research findings.	Researchers applying for federal funding.
Government of Canada	*Human Pathogens and Toxins Act* (HPTA) (GC, 2009) and *Human Pathogens and Toxins Regulations* (HPTR) (GC, 2024).	HPTA establishes "a safety and security regime to protect the health and safety of the public against the risks posed by human pathogens and toxins." HPTR specify how the Public Health Agency of Canada (PHAC) will implement the HPTA and authorizes controlled activities with human pathogens and toxins (PHAC, 2024).	Scientific research with human pathogens and toxins.	<u>Identify</u>: Human pathogens and toxins, and prescribed human pathogens and toxins having dual-use potential (i.e., security-sensitive biological agents or SSBAs) (PHAC, 2018). <u>Safeguard</u>: Licensing and security clearances.	"Organizations and individuals conducting activities with human pathogens and toxins. This includes universities, public health laboratories, industry, hospitals, and diagnostic services for human and animal health" (PHAC, 2024).

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
PHAC	Canadian Biosafety Standard (PHAC, 2022) and Canadian Biosafety Guideline–Dual-Use in Life Science Research (PHAC, 2018).	Helps regulated parties identify research with dual-use potential and mitigate the risks.	Research with dual-use potential.	Identify: Research with dual-use potential is identified based on several questions, including the characteristics of an organism or toxin, harmfulness, novelty, modification risks, and misuse potential. Safeguard: Risk assessment to evaluate if existing biosafety and biosecurity measures are adequate for dual-use research. Additional precautions may be necessary, including stricter administrative controls, higher containment levels, training on the dual-use potential of research, periodic reviews of research for dual-use applications, and an information-sharing plan.	"Facilities that have been issued a Pathogen and Toxin Licence (hereafter, licence) under the HPTA and the HPTR" (PHAC, 2022).

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Canada: Laws, regulations, policies, and guidance for identifying and safeguarding sensitive research

Reports by non-governmental organizations

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
U15	Safeguarding Research in Canada: A Guide for University Policies and Practices (U15, 2023).	"A collection of suggested institutional guidelines based on leading policies and practices for safeguarding research from the potential risks in global research engagement."	All university research.	Identify: No specific mechanisms. Safeguard: Five institutional practices: • Governance and risk frameworks; • Due diligence, risk assessment, and management; • Communication, education, and knowledge sharing; • Network and device security; and • Research security and campus security.	Universities.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Aotearoa New Zealand: Policies, regulations, and guidance in New Zealand for identifying and safeguarding sensitive research.

Documents adopted by the Government of New Zealand

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of New Zealand; Centre for the Protection of National Infrastructure; Science New Zealand; Universities New Zealand	Trusted Research: Guidance for Institutions and Researchers (Gov. of New Zealand, 2020)	Focuses on international research collaboration, lists and describes risks from foreign bad actors in contexts such as international travel, funding, visiting scholars, cyber security, and overseas research.	All university research.	Identify: Joint research and applied research are specifically mentioned here. The onus for identifying what is sensitive research is placed on the researcher and may occur through export controls or privacy legislations. The identification of risky partnerships takes place through due diligence and conflict of interest checks. Safeguard: It is the researcher's responsibility to abide by export controls and privacy legislation, compartmentalize research and control access, make security considerations a feature of funding proposals, protect partners, demonstrate transparency and maintain visibility, and manage cyber security and overseas research.	Research institutions and researchers, and particularly researchers working in STEM, innovation, dual-use technologies, emerging technologies, and commercially sensitive research areas.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of New Zealand, Ministry of Foreign Affairs and Trade	New Zealand Strategic Goods List (Gov. of New Zealand, 2024)	New Zealand controls the export of the goods on this list. Controlled items may not be exported from New Zealand, including the electronic export of listed software and technology, unless an export licence or permission has been obtained.	Controlled goods included in this list.	Identify: The goods on this list. Safeguard: An export license is required.	All researchers and research institutions.
Government of New Zealand; 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)	Provides an overview of partnership risks and the importance of risk management within due diligence. Guidance on what questions to ask when entering new business relationships, advice on governance arrangements, funding requirements, and data and IP risks.	Research conducted in partnership with foreign actors.	Identify: *Sensitive technologies* are defined as having dual use, now or in the future. For determining if a technology is included, this document refers to New Zealand export controls, looking at sensitive technology lists from other countries, public information on technologies, and expert advice. Safeguard: Asking questions about what is known about the partnering organization, new and existing partners and their motivations, and other high-risk factors (e.g., breaches of integrity or law).	Individuals, organizations, and businesses partnering with foreign actors.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Aotearoa New Zealand: Policies, regulations, and guidance in New Zealand for identifying and safeguarding sensitive research

Reports by non-governmental organizations in New Zealand

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Universities New Zealand	Trusted Research Protective Security Requirements: Guide for Senior University Leaders in Aotearoa New Zealand (UNZ, 2022).	Targets protecting academic values while avoiding the misappropriation or misuse of research for military use or foreign interference. Concerns international research and ensuring the integrity and security of collaborations, protecting IP, research infrastructure assets, Indigenous knowledges, research data, personal information and researchers.	All university research, especially with international collaboration.	Identify: Sensitive research is linked only to export and catch-all controls, while collaborative and applied research are listed as particularly vulnerable to misappropriation or misuse by foreign individuals and organisations. Onus is on the institution to conduct due diligence, risk assessments, risk audits, and to use the Risk Management Framework provided in this document to educate and train researchers and others implicated in managing risks. Safeguard: Restrict access to facilities and data, ensure adequate cyber security protocols, adhere to export and catch-all controls.	Primarily senior university leaders, however relevant guidance may be useful for faculties, departments, and service divisions within universities. Additionally, some advice may implicate university councils and specifically council audit and risk subcommittees.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Australia: Policies, regulations, and guidance in Australia for identifying and safeguarding sensitive research

Documents adopted by the Government of Australia

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of Australia	Defence and Strategic Goods List 2021 (Gov. of Australia, 2024a, b).	The Government of Australia controls the export of goods listed in this document. This list is "amended from time to time to reflect changes in the various multilateral non-proliferation and export control regimes of which Australia is a member" (Gov. of Australia, 2024a)	Research to do with defence and related goods, or dual-use goods.	<u>Identify</u>: Provides lists of military, non-military lethal, and dual-use goods. <u>Safeguard</u>: An export license is required.	All researchers and research institutions.
Government of Australia	*Defence Trade Controls Act* (Gov. of Australia, 2012).	"Controls the supply, publication and brokering of tangible, intangible military and dual-use goods and technologies" (Gov. of Australia, 2023a)	Data and technologies considered military or dual-use.	<u>Identify</u>: Employs lists of military, non-military lethal, and dual-use goods. - <u>Safeguard</u>: "It allows the Minister for Defence to permit or prohibit the supply, publication and/or brokering of goods and technologies" (Gov. of Australia, 2023a).	All researchers and research institutions.
Government of Australia	Critical Technologies Statement (Gov. of Australia, 2023b); List of Critical Technologies in the National Interest (Gov. of Australia, 2023c).	Outlines some of the benefits and risks of the critical technologies as well as the actions being taken by the government to manage these risks.	Research involving critical technologies.	<u>Identify</u>: The technologies implicated are provided in the list of critical technologies (Gov. of Australia, 2023c). <u>Safeguard</u>: N/A, however the list is not intended to regulate or control the technologies.	Government of Australia.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of Australia, Department of Health and Aged Care	Security Sensitive Biological Agents (SSBA) Regulatory Scheme (Gov. of Australia, 2024c).	Designates SSBAs that are of concern, provides a legislative framework for the regulation of SSBAs, and maintains access for those with legitimate need to handle SSBAs in secure labs while limiting acts of bioterrorism.	Research involving SSBAs.	Identify: List of SSBAs is provided in the List of Security Sensitive Biological Agents (Gov. of Australia, 2016). Safeguard: The SSBA Standards "set out the requirements that must be met by the entity to ensure physical security around handling, storage, disposal and transport of SSBAs and biological agents suspected of being SSBAs, as well as personnel and information security" (Gov. of Australia, 2013).	Entities and facilities that work with known or suspected SSBAs.
Government of Australia; Department of Foreign Affairs and Trade	*Australia's Foreign Relations (State and Territory Arrangements) Act 2020* (Gov. of Australia, 2020).	"Creates a scheme to ensure that arrangements between State or Territory governments and foreign government entities do not adversely affect Australia's foreign relations and are not inconsistent with Australia's foreign policy" (Gov. of Australia, 2021).	Public universities that are entering partnerships with foreign entities that do not have institutional autonomy.	Identify: Provides criteria for determining whether a foreign university does not have institutional autonomy. Safeguard: Universities must notify the Minister for Foreign Affairs if they propose to enter, or enter, a foreign arrangement. The Minister must consider the proposed negotiation or entry into the arrangement, and make a decision whether to approve.	Public universities.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Australian Research Council (ARC); Government of Australia	ARC Countering Foreign Interference Framework (ARC, 2023).	Describes the roles and responsibilities of the ARC, academic institutions, researchers, and government actors relating to granting processes at various stages of the research lifecycle.	All research proposals submitted to ARC for funding.	<u>Identify</u>: If researchers apply for funding for research on technologies on the Critical Technologies list, ARC considers a range of factors to determine what risks may be present. <u>Safeguard</u>: If the ARC identifies a potential risk, national security agencies may become involved, and the host university's administration will be notified and required to provide a risk mitigation strategy or plan.	Universities and researchers.
Australian Security Intelligence Organisation (ASIO); Government of Australia	Protect your Research, Collaborate with Care (ASIO, n.d.).	Focuses on protecting research from foreign bad actors trying to gain access to sensitive information or data, or steal IP. Describes methods by which foreign actors or their proxies may approach researchers or universities for partnerships, details what types of behaviour to be suspicious of, and provides advice on safeguarding research within academic institutions. Provides case studies, information on how to report security concerns, and links to additional resources.	All university research.	<u>Identify</u>: Focus on areas of research in which Australia has excellence, and types of critical technology or dual-use research that are desirable to foreign powers and their proxies. Provides guidance on developing risk policies that identify areas of research and which research partners are highest risk. <u>Safeguard</u>: Training staff on threat awareness, helping staff identify security threats, ensuring that collaborative research complies with government requirements and acts (e.g. export controls), ensuring that staff declare affiliations, and offering training on how to protect research when travelling overseas.	Administrators and security managers at universities.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Australia: Policies, regulations, and guidance in Australia for identifying and safeguarding sensitive research

Reports by non-governmental organizations in Australia

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
University Foreign Interference Taskforce (UFIT) with input from the Government of Australia, Universities Australia, and Group of Eight Australia	Guidelines to Counter Foreign Interference In the Australian University Sector (UFIT, 2021).	Supports universities to strengthen or create tools, frameworks, and resources for identifying and mitigating risks from foreign interference. Issues of concern include: compromised data, loss of IP, reputational damage, risks to the economy and national security, self-censorship, and conflicts with academic freedom. Guidelines aim to provide a balanced approach to identifying and mitigating potential risks, without compromising academic freedom and an open science culture.	All university research	Identify: Focus on foreign interference with research activities, without describing specific technologies or areas that may be at higher risk. Guidance on due diligence and risk assessment processes for determining risks associated with foreign influence. Safeguard: Targeted advice on how best to manage risks, with guidance on: governance and risk frameworks; communication, education and knowledge sharing; and cybersecurity.	Universities and researchers.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

European Union: Policies, regulations, and guidance in the European Union for identifying and safeguarding sensitive research.

Regulations, policies, guidelines, and tools adopted by the EU

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
European Commission (EC)	*Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)* (Regulation 2021/821) (EC, 2021a).	Defines "dual-use items"; lists technologies and topics falling within regulatory scope; establishes parameters for export control regime in the EU, including harmonization with international agreements and treaties.	Software and technology that can be used for both civil and military purposes, including research on or involving listed items.	Identify: Provides a list of controlled items. Safeguard: Export authorization by competent authorities. Controls on technology transfers do not apply to information in the "public domain" and "basic scientific research."	All researchers and research institutions in EU member states.
EC	*Commission recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation 2021/821 (EC, 2021b).*	Guides the application of Regulation 2021/821 to researchers and institutions.	See above.	Identify: Risk assessment guidelines; screening of research partnerships; assessment of technological readiness level; lists of sensitive research areas; list of scenarios; list of potential red flags during due diligence. Safeguard: "Catch-all" controls (i.e., controls for non-listed dual-use items); reporting and auditing instructions; guidance on physical and information security.	Research organizations, researchers, research managers, and staff at research organizations responsible for compliance.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
EC	Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States (EC, 2023).	Proposes a risk assessment process to be carried out jointly by EU member states on four key technology areas.	Research in critical technology areas.	Identify: Lists high-risk technology areas: advanced semiconductors, artificial intelligence, quantum technologies, and biotechnologies. Safeguard: Establishes guiding principles for risk assessments in high-risk technology across EU member states	Research organizations, researchers, research managers, and staff at research organizations responsible for compliance.
EC	Council Recommendation on Enhancing Research Security (EC, 2024).	Provides guidance on bolstering research security across the EU.	Research in "critical knowledge and technology" refers to knowledge and technology, including know-how, in emerging and disruptive areas and in domains that are key to economic competitiveness, social welfare and the security of the Union and itsMember States and in which, consequently, overdependency on third countries is undesirable."	Identify: Risk analysis based on the institutional profile of the EU organization, research topic, and risk profile of partner countries and organizations. Safeguard: Use of partnership agreements to outline intellectual property protections, define exit strategies for non-compliant partners, and establish physical and cybersecurity measures, including compartmentalization.	EU, EU member states, research performing organizations, and research funding organizations.
EC	EU Grants: How to Complete Your Ethics Self-Assessment (EC, 2021c).	Guidance on adherence to research ethics, including potential misuse of research results.	Research proposals and research supported by a number of EU funding programs.	Identify: Requests applicants to submit a risk assessment along with their proposal. Safeguard: Suggests measures such as research security training, restrictions on publication, and adjustments to research design.	Applicants and beneficiaries of EU grant programs.

European Union: Policies, regulations, and guidance in the European Union for identifying and safeguarding sensitive research

Tools by non-governmental organizations in the EU

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
European Federation of Academies of Sciences and Humanities (ALLEA)	The European Code of Conduct for Research Integrity (ALLEA, 2023).	Offers high-level principles and ethical responsibilities that support safe and responsible research.	All research.	Safeguard: Promotes responsible research by encouraging risk awareness, compliance with legal and ethical standards, data protection, and formal collaboration agreements.	EU researchers.

France: Policies, regulations, and guidance in France for identifying and safeguarding sensitive research

Regulations, policies, and guidelines adopted by the Government of France

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of France	*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* (Gov. of France, 2020).	Implementation of EU dual-use export control regime into French national law (EC, 2009).	Follows from EU export control regulations (EC, 2009).	Identify: Lists dual-use technologies in alignment with EU regulations.	All researchers and research institutions.
Government of France	*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* (Gov. of France, 2024).	Ministerial order enacting additional export control requirements for specific technologies, such as quantum computing and adjacent technologies.	Quantum technologies.	Identify: Lists quantum technologies subject to export control. Safeguard: Export authorizations.	All researchers and research institutions.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of France	Protection du potentiel scientifique et technique et intelligence économique (PPST) (SGDSN, 2012).	Provides a national framework for overseeing sensitive research; Introduces restricted research zones (ZRR) subject to information and physical security requirements.	Research in "biology, medicine, agronomy, ecology, geology, space sciences, computer science and information technology, and engineering" (Gattolin, 2021). [free translation]	Identify: Provides a list of topics covered by PPST (Gattolin, 2021). Invites researchers to assess the applicability of PPST according to four criteria: economic interests of the nation, military arsenals, proliferation of weapons of mass destruction, and terrorism (SGDSN, 2012). Safeguard: Physical and cybersecurity requirements for access to ZRRs; nationality-agnostic screening of individuals applying for access to ZRR; research partnerships involving ZRR are subject to government review (SGDSN, 2012).	All researchers and research institutions.
Government of France	Protection Numérique du Potentiel Scientifique et Technique de la Nation (SGDSN, 2018).	Guide for establishing compliance with digital and cybersecurity requirements set by PPST.	Research falling within the scope of PPST.	Identify: Risk assessment to identify "informations à régime restrictif" (IRR), a label for sensitive data that carries similar legal protections to those that apply to ZRR. Safeguard: Reporting requirements for cybersecurity incidents or other incidents relating to IRR; institutional protocols for identifying and labelling IRR; regularly reviewed risk management processes; tailoring digital and cybersecurity requirements to the operating context of ZRR.	Researchers in ZRRs or working with IRR.

France: Policies, regulations, and guidance in France for identifying and safeguarding sensitive research

Reports by non-governmental organizations in France

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
National Consultative Council for Biosecurity	Recherches duales à risque: Recommandations pour leur prise en compte dans les processus de conduite de recherche en biologie (Korn *et al.*, 2019).	Overview of DURC oversight in France.	Academic research in life sciences.	Identify: Integrating dual-use risk assessments into research processes, creating local oversight committees, and training researchers to recognize potential misuse. Safeguard: Independent monitoring of sensitive projects, ethical oversight of publications, and stricter control over the transfer and access to sensitive biological data.	Researchers.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Germany: Laws, policies, and guidance in Germany for identifying and safeguarding sensitive research

Laws adopted by the Government of Germany

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of Germany	*Basic Law for the Federal Republic of Germany* (Gov. of Germany, 1949).	Codifies constitutional protections for freedom of research in Germany.	All research.	N/A	All researchers in Germany.

Reports and guidelines by non-governmental organizations in Germany

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Max Planck Society (MPG)	Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks (MPG, 2017).	"[Aims] to prevent misuse of research and avoid risks through self-regulation based on ethical principles...[establishes] a procedure to enable researchers to better resolve ethical uncertainties and prevent accusations of unethical conduct."	All research.	<u>Identify</u>: "Researchers should … take account of the consequences and opportunities for application and misuse of their work and its controllability. Research projects that are potentially susceptible to risk should … be preceded by an evaluation of the associated risks to human dignity, human life and human welfare, the environment and any other significant values protected under the constitution." <u>Safeguard</u>: Minimization of risks across the research lifecycle; documentation and communication of risks to ethics committees and other institutional actors; withholding information from publication; foregoing research as a last resort; training.	"Everyone working at the Max Planck Society's institutions, or with their resources at other locations."

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
German National Academy of Sciences Leopoldina (Leopoldina); German Research Foundation (DFG)	Scientific Freedom and Scientific Responsibility Recommendations for Handling of Security-Relevant Research (Leopoldina & DFG, 2022).	Offers assistance to researchers and research institutions "in answering ethical questions" and "contribut[e] to defining standards and codes of conduct beyond statutory norms for researchers dealing with security-relevant research."	Security-relevant research and security-relevant research of concern.	Identify: Risk analysis "should … take account of the consequences and opportunities for application and misuse of [research] and its controllability." Safeguard: Risk minimization through physical and cybersecurity measures; pre-publication review of research results; screening partnerships; documentation and communication of risks; foregoing research as a last resort.	Government-funded research.
German Aerospace Center (DLR)	Due Diligence in Science (DLR, 2024).	Supports institutions and universities in the development and implementation of due diligence instruments to assess the risks associated with scientific cooperation.	Scientific research involving partnerships.	Identify: Systematic assessments of partners, research topics, and institutions using filter criteria—such as country of origin, topic sensitivity, and access to infrastructure—alongside background checks and self-disclosure forms to detect potential security, ethical, or legal risks.	Managers of universities and research institutions. Principal investigators at universities and institutions.
Leibniz Association	Risk Management in International Scientific Collaboration (Leibniz Association, 2021).	Provides guidance on establishing "internal processes …that can be used to carry out standard, pragmatic and unbureaucratic assessments of collaborations with individual partners or countries on a case-by-case basis."	Scientific research involving international partnerships.	Safeguard: Legal compliance (e.g., with export controls), maintaining transparency and clear agreements with partners, protecting intellectual property and data through access controls and encryption, raising awareness among researchers, and establishing exit strategies and emergency plans for high-risk collaborations.	Leibniz Association institutes

Netherlands: Policies, regulations, and guidance in the Netherlands for identifying and safeguarding sensitive research

Regulations, policies, guidelines, and tools adopted by the Government of the Netherlands

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of the Netherlands	*Besluit toepassingsbereik sensitieve technologie* (Decision on the scope of application of sensitive technology) (Gov. of Netherlands, 2023).	Provides details on which technologies are considered sensitive or highly sensitive. This list applies to business activities (e.g., mergers, investments) in sensitive technology areas (Stibbe, 2023).	Sensitive goods and technologies.	Identify: Lists export codes for sensitive and highly sensitive technologies, including those related to military and dual-use goods. Safeguard: Government approval is required in the acquisition or merger of any company working with technologies listed (Stibbe, 2023).	All researchers and research institutions.
Government of the Netherlands	Knowledge security guidelines (Gov. of Netherlands, 2022).	Defines scope of knowledge security, and outlines roles and responsibilities for actors in knowledge security; provides guidance for risk analysis; introduces notion of "crown jewels" that institutions should prioritize protecting; describes strategies for establishing institutional security teams; lists tools and approaches for adaptive risk management.	Sensitive domains of knowledge	Identify: Risk analysis at the institutional level to identify sensitive technologies and knowledge. Requirement to periodically reassess identified technologies. Safeguard: Establishment of institutional security teams tasked with monitoring research partnerships, cybersecurity, and security coordination; tailoring risk management efforts case-by-case; definition of institutional standard (e.g. cybersecurity).	Researchers, public research institutions.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Netherlands Ministry of Education, Culture and Science (OCW)	National Contact Point for Knowledge Security (OCW, n.d.-a, n.d.-b).	Provides advice on knowledge security in international research collaborations.	Research involving international collaboration.	Identify: Provides advice on which research areas could warrant additional vigilance in partnerships, and how to assess country risk profiles. Safeguard: Aggregates resources, tools, and relevant legislation for the appropriate protection of research.	Research institutions, researchers.
Dutch National Institute for Public Health and the Environment (RIVM)	Biosecurity Office (RIVM, n.d.-a).	"Shares knowledge and information about biosecurity and increases awareness about biosecurity, in order to minimise the risk of misuse of high risk pathogens, knowledge and technologies" (RIVM, n.d.-a).	Research involving high-risk biological material.	Identify: Provides dual-use questionnaire to identify sensitive research (RIVM, n.d.b), and aggregates various resources (e.g., pathogen lists, export control rules). Safeguard: Provides key good practices for managing sensitive research in a biosecurity context (RIVM, n.d.-c).	Researchers, individuals responsible for institutional biosecurity.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

CCA | CAC

Netherlands: Policies, regulations, and guidance in the Netherlands for identifying and safeguarding sensitive research

Reports by non-governmental organizations in the Netherlands

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Royal Netherlands Academy of Arts and Science (KNAW)	Knowledge Security: Academy Position Paper (KNAW, 2023).	From the perspective of the Academy, this report discusses use of the term knowledge security and what principles should underpin it; the report then reviews existing and proposed policies based on these principles, and then puts forward further policy recommendations.	Research within the scope of the *Knowledge Security Guidelines.*	Identify: Recommends that risk assessors differentiate between "undesirable transfer of knowledge," "interference," and "ethical and integrity issues." Safeguard: Criticizes the prospect of screening based on nationality or disciplines, arguing that awareness-raising at institutional levels provides greater security.	All researchers and research institutions.
Universities of the Netherlands	Capability Maturity Model: Knowledge Security (UNL, 2024).	This model is designed to "support universities in designing and implementing their knowledge security policies; to internally assess the maturity level for each specific topic and the desired maturity level; to enable an internal strategy and planning towards the desired maturity level; to further improve the alignment of universities' knowledge security policies in terms of the used concepts, and offer an outline of topics."	Research within the scope of the Knowledge Security Guidelines	Identify: Reiterates processes in Netherlands Knowledge Security Guidelines (Gov. of Netherlands, 2022), and discusses legal frameworks, risk assessments, and training and awareness for identification. Safeguard: Provides a framework for graduated risk management approaches that can be tailored to risk profile. Risk management practices of varying intensity are outlined for various priorities encompassed within knowledge security.	Research institutions, researchers

United Kingdom: Policies, regulations, and guidance in the United Kingdom for identifying and safeguarding sensitive research

Regulations, policies, and guidelines adopted by the government of the UK

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
National Protective Security Authority (NPSA); the National Cyber Security Centre (NCSC), in partnership with 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).	Documents are intended to “raise awareness of the risks to research collaborations which may occur when working with organisations or research partners with links to nations whose democratic and ethical values are different from our own” (NPSA & NCSC, 2024a). Documents “[outline] the potential risks to UK research and innovation; [help] researchers, UK universities and industry partners to have confidence ininternational collaboration and make informed decisions around those potential risks; [and explain] how to protect research and staff from potential theft, misuse or exploitation produced in consultation with academia and industry, and [are] designed to help the UK’s world-leading research and innovation sector get the most out of international collaboration whilst protecting intellectual property (IP), sensitive research and personal information” (NPSA & NCSC, 2024a).	All academic research; all industry research, particularly researchers in STEM subjects, dual-use technologies, emerging technologies and commercially sensitive research areas.	<u>Identify</u>: Researcher is responsible for determining if their research is commercially sensitive, is potentially patentable, is related to defence/national security, or if it has future dual use applications. This guidance points to export controls for additional advice, and the National Security and Investment Act for 17 areas of the economy which are riskier for national security (NPSA & NCSC, 2024a). Industry partners are encouraged to use Technological Readiness Levels to determine if their research is sensitive (NPSA & NCSC, 2022). <u>Safeguard</u>: Researcher is responsible for ensuring collaborations are secure and demonstrating this in funding proposals (transparent conflicts of interest, adequate cybersecurity, due diligence for national security concerns) (NPSA & NCSC, 2024a). Senior leaders have responsibilities in managing access to sensitive facilities and IT platforms (NPSA & NCSC, 2024b).	Academic researchers, universities, senior leaders, and industry partners.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of the United Kingdom	Academic Technology Approval Scheme (ATAS) (Gov. of United Kingdom, 2025a).	Researchers and students from certain nations coming to the UK to study sensitive subjects must obtain a certificate.	Sensitive research areas.	Identify: Sensitive research areas are classified through Common Aggregator Hierarchy codes; applicants from certain nations must check to see if their area of study or research is included.	Researchers and universities.
Government of the United Kingdom	UK Strategic Export Control List (Gov. of United Kingdom, 2025b).	Export controls restrict the export and communication of sensitive technology or strategic goods (Gov. of United Kingdom, 2023).	Sensitive technologies on the list.	Identify: List is provided (the consolidated list of strategic military and dual-use items that require export authorisation). Safeguard: Failure to obtain appropriate licenses may result in criminal charges (Gov. of United Kingdom, 2023).	All researchers and research institutions.
Government of the United Kingdom	National Security and Investment Act (Gov. of United Kingdom, 2024a, 2024b).	Enables the government to intervene in the acquisition or sale of sensitive research or technologies if they are deemed to be harmful to national security.	Sensitive technologies on the list.	Identify: If the technology in question appears on the 17 sensitive areas of the economy list, the seller is legally bound to notify the government. Safeguard: Government scrutiny of acquisitions and intervention if threats to national security are likely.	All citizens and businesses.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
UK Research and Innovation (UKRI)	Trusted Research and Innovation: Principles and Expectations (UKRI, 2025).	Trusted research and innovation (TR&I) involves "the protection of the UK's intellectual property, sensitive research, people, and infrastructure from potential theft, misuse and exploitation"; principles for managing TR&I apply to UKRI and expectations apply to grantees.	All research funded by UKRI.	Identify: Grantees are expected to conduct due diligence of project partners Safeguard: Managing information and knowledge sharing through cyber security, data separation, managing access to data; applying intellectual property rights, and complying with export controls.	Researchers, universities, and UKRI.

Reports by non-governmental organizations in the UK

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Universities UK (UUK)	Managing Risks in Internationalisation: Security Related Issues (Universities UK, 2020).	Provides governing bodies and senior leadership of universities with advice on how to manage internationalization in the university setting. Includes establishing clear governance structures and identifying responsible staff members for managing risks. Strategies for the protection of reputations, values, people, campuses, and partnerships are discussed. Outlines what types of changes may be necessary to deal with internationalization, such as: changes in awareness and understanding among individuals; changes in institutional systems, processes, and behaviours; and changes in cross-sector systems and processes.	All university research.	Identify: Due diligence processes to identify partnership risks, training and education in risk awareness and management. Safeguard: Cybersecurity actions, compliance with export control legislation.	Governing heads and executive bodies of universities.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
UK Research Integrity Office (UKRIO)	Code of Practice for Research (UKRIO, 2023).	Encourages “good conduct in research and help prevent mistakes and misconduct, to help organisations and researchers to conduct research of the highest quality and sustain a healthy research culture.” Covers “areas of good practice in research typically included in organisational policies for the conduct of research, drawing upon existing good practices and the experiences of UKRIO in addressing good research conduct and research misconduct.”	All research.	Identify: Suggests that organizations and researchers conduct risk assessments to determine the potential for risks to “the organisation, the research, or the health, safety, wellbeing and mental health of researchers and research participants, the public, the environment, national security.”	“Individual researchers and to organisations that carry out, fund, host, or are otherwise involved in research.”

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

United States: Laws, regulations, policies, and guidance in the United States for identifying and safeguarding sensitive research

Regulations, policies, and guidelines adopted by the Government of the United States

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of the U.S.	*The CHIPS and Science Act* (Gov. of United States, 2022).	Funds U.S. science and technology and aims to protect them from foreign interference.	Research in many strategic areas, including semiconductors, artificial intelligence, biotechnology, and computing.	Identify: "foreign entities of concern" and "foreign countries of concern." Safeguard: Restricts research collaboration with "foreign entities of concern" and "foreign countries of concern."	The research ecosystem encompasses federally funded research conducted by government departments and agencies, as well as regional research hubs.
Government of the U.S.	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).	NSPM-33 establishes national security policy for U.S. government-supported R&D.	Research supported by federal departments and agencies.	Identify: No specific mechanisms. Safeguard: Standardized approaches to information disclosure (e.g., affiliations, appointments, biographical sketches, digital persistent identifiers for researchers who receive federal funding), digital persistent identifiers, information sharing with law enforcement agencies, and certified research security programs for research organizations receiving federal funding of US$50 million or more.	Federal departments and agencies.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of the U.S. (White House Office of Science and Technology Policy)	Guidelines for Research Security Programs at Covered Institutions (OSTP, 2024).	Research institutions receiving federal funding exceeding $50 million annually must establish a research security program.	Research conducted by institutions receiving federal funding exceeding $50 million per year.	Identify: No specific mechanisms. Safeguard: The research security program should include a cybersecurity program, a travel reporting program, research security training, and export control training.	Research institutions receiving federal funding exceeding $50 million.
Government of the U.S. (The U.S. Department of Commerce's Bureau of Industry and Security (BIS))	Export Administration Regulations (EAR) (US BIS, 2024).	Regulate exports of dual-use items.	All research that involves items and names of foreign businesses, research institutions, government and private organizations, and individuals subject to license requirements for the export, reexport and/or transfer (in-country) of specified items.	Identify: A list of items and names of foreign businesses, research institutions, government and private organizations, and individuals. Safeguard: Dual-use export licenses are required in certain situations involving national security, foreign policy, short supply, nuclear non-proliferation, missile technology, chemical and biological weapons, regional stability, crime control, or terrorist concerns.	All researchers and research organizations exporting dual-use items.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
Government of the U.S. (the Department of Energy, DOE)	Science and Technology Risk Matrix (COGR, 2023). [1] *[1] Parts of this matrix are not publicly available, the analysis presented herein is based on a presentation delivered by DOE staff at the Multi-Agency Panel on Research Security Risk Assessment & Analysis (COGR, 2023) and on JASON (2024).*	Manages risks associated with critical and emerging technologies that lack other control mechanisms.	Specific emerging technology areas.	Identify: Emerging technology areas associated with economic competitiveness, national security, or scientific leadership (e.g., quantum, batteries, AI) and engagements with a specific country of risk (China, Iran, North Korea, Russia). Subject matter experts evaluate progress in each topic area and categorize research into fundamental and non-sensitive, potentially sensitive, and requiring additional protective measures (JASON, 2024). Safeguard: Restriction of activities such as "foreign engagements, cooperative R&D agreements, official travel, and foreign national engagement and access to the projects and data that involve countries of risk (China, Russia, Iran, and North Korea)" (JASON, 2024).	Applies to activities at the DOE National Laboratories.
Government of the U.S. (The Department of Defense, DOD)	Policy on Risk-Based Security Reviews of Fundamental Research (US DOD, 2023).	Identifies and mitigates risks to national security from research funded by the DOD.	Focuses on the affiliations and activities of people who conduct fundamental research.	Identify: Affiliation of concern. Safeguard: Suggests a range of safeguarding strategies, including removing or replacing a co-principal investigator from a multi-investigator proposal, risk awareness training, and increased reporting frequency.	Applies to all projects selected for funding by the DOD.
Government of the U.S. (White House Office of Science and Technology Policy)	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) The Implementation Guidance to the Oversight Policy (Gov. of United States, 2024).	Federal oversight framework for conducting and managing certain types of federally funded life sciences research on biological agents and toxins.	Biological agents or toxins.	Identify: Biological agents or toxins where the research is within Category 1 or 2 as described in the policy. Safeguard: The organizational framework for research oversight by PIs, research institutions, and research funders.	Federal departments and agencies that fund research at research institutions in the U.S.

RESEARCH SECURITY IN CANADA AND FOREIGN JURISDICTIONS

United States: Laws, regulations, policies, and guidance in the United States for identifying and safeguarding sensitive research

Reports by non-governmental organizations

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
National Academies of Sciences, Engineering, and Medicine (NASEM)	Protecting U.S. Technological Advantage (NASEM, 2022).	Examines the need for limitations on open research and "take[s] into account the benefits and drawbacks of technology protection options."	Scientific research.	Identify: Suggests a coordinated risk management approach "that begins with identifying which actors using what means are attempting to use a particular technology against U.S. interests or technology leadership." Safeguard: Defines strategies best equipped to address the resultant risks.	Across the federal government
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 & Arnold, 2021).	Explores how to address the security of research conducted by the private sector.	Research conducted by the private sector.	Identify: No specific provisions. Safeguard: Proposes a public-private research security clearinghouse led by "academia, business, philanthropy, and government" with a presence in the most active R&D hubs. This institution would provide researchers, their managers and funders "with open source information, security-related education and training, decision support resources, and … interface with federal partners."	Researchers, research funders, and research managers.

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
JASON	Fundamental Research Security (JASON, 2019).	Addresses the value and risks associated with openness in fundamental research.	Fundamental research, i.e., “basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons” (Gov. of United States, 1985)	Identify and Safeguard: • Full disclosure of commitments and actual or potential conflicts of interest/commitment • Project-specific tools to facilitate risk assessments in research collaborations, non-federal research agreements, and grants • Education and training on conflicts of interest and commitment. • Cooperation with intelligence and law enforcement agencies to share evidence-based risks of foreign influence and reinforce the value of foreign collaboration.	NSF-supported research

Created by	Title	Summary	Research in Scope	Mechanisms to ID and Safeguard	Applies to
JASON	Safeguarding the Research Enterprise (JASON, 2024).	Identifies "specific steps [NSF] might take to identify sensitive areas of research and describe processes NSF might use to address security in … research areas of concern."	Sensitive and highly sensitive research.	<u>Identify</u>: Recommends a dynamic approach to identifying sensitive research, based on its potential applications, technology readiness levels, and "direct and predictable national security impact of the applications of each research proposal." <u>Safeguard</u>: Risk mitigation strategies for sensitive research projects include: "changes to the scope of a research grant, training (or enhanced training) of the principal investigator … on research security risk and protections, enhanced training regarding publication of potentially sensitive results, enhanced training on identifying individuals of concern who might be considered as possible participants or collaborators, increased frequency or scope of reporting" and physical and cybersecurity standards. Highly sensitive research project should be accompanied by additional controls, including "restrictions on participation for individuals of concern, mandatory pre-approval for conferences or publication, mandatory pre-approval before posting open-source data or software."	NSF-supported research.

REFERENCES

- 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). (n.d.). Protect your Research, Collaborate with Care. Canberra, Australia: ASIO.
- 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.
- EC (European Commission). (2009). Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast).
- EC (European Commission). (2021a). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).
- EC (European Commission). (2021b). Commission Recommendation (EU) 2021/1700 of 15 September 2021 on Internal Compliance Programmes for Controls of Research Involving Dual-Use Items Under Regulation (EU) 2021/821 of the European Parliament and of the Council Setting up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items. Brussels, Belgium: EC.
- EC (European Commission). (2021c). EU Grants: How to Complete Your Ethics Self-Assessment. Brussels, Belgium: EC.
- EC (European Commission). (2023). Commission Recommendation (EU) 2023/2113 of 3 October 2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States. Strasbourg, France: EC.
- EC (European Commission). (2024). Council Recommendation on Enhancing Research Security. Brussels, Belgium: EC.
- Flagg, M. & 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: Senate of France.
- GC (Government of Canada). (1985a). Export and Import Permits Act, RSC 1985, c E-19.
- GC (Government of Canada). (1985b). United Nations Act, RSC 1985, c U-2.
- GC (Government of Canada). (1985c). Defence Production Act, RSC 1985, c D-1.
- GC (Government of Canada). (1992). Special Economic Measures Act, SC 1992, c 17.
- GC (Government of Canada). (1995). Chemical Weapons Convention Implementation Act, SC 1995, c 25.

REFERENCES

- GC (Government of Canada). (1997). Nuclear Safety and Control Act, SC 1997, c 9.
- GC (Government of Canada). (2009). Human Pathogens and Toxins Act, SC 2009, c 24.
- GC (Government of Canada). (2010). Nuclear Non-proliferation Import and Export Control Regulations, SOR/2000-210.
- GC (Government of Canada). (2016). Controlled Goods Regulations, SOR/2001-32.
- GC (Government of Canada). (2021). Export Control List, SOR/89-202.
- GC (Government of Canada). (2024). Human Pathogens and Toxins Regulations, SOR/2015-44.
- Gov. of Australia (Government of Australia). (2012). Defence Trade Controls Act 2012.
- Gov. of Australia (Government of Australia). (2013). Security Sensitive Biological Agent (SSBA) Standards. Canberra, Australia: Gov. of Australia.
- Gov. of Australia (Government of Australia). (2016). SSBA – Fact sheet 5 – List of Security Sensitive Biological Agents. Canberra, Australia: Department of Health and Aged Care.
- Gov. of Australia (Government of Australia). (2020). Australia's Foreign Relations (State and Territory Arrangements) Act 2020.
- Gov. of Australia (Government of Australia). (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 (Government of Australia). (2023a). Australian Government legislation and codes. Retrieved August 2024, from https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/templates-and-tools/australian-government-legislation-and-codes.
- Gov. of Australia (Government of Australia). (2023b). Critical technologies statement. Retrieved September 2024, from https://www.industry.gov.au/publications/critical-technologies-statement.
- Gov. of Australia (Government of Australia). (2023c, May 19). List of critical technologies in the national interest. https://www.industry.gov.au/node/92356. Retrieved September 2024, from https://www.industry.gov.au/publications/list-critical-technologies-national-interest.
- Gov. of Australia (Government of Australia). (2024a). Defence and Strategic Goods List 2024. Canberra, Australia: Gov. of Australia.
- Gov. of Australia (Government of Australia). (2024b). Explanatory Statement: Customs Act 1901, Defence and Strategic Goods List 2021. Canberra, Australia: Government of Australia.
- Gov. of Australia (Government of Australia). (2024c). Security Sensitive Biological Agents (SSBA) Regulatory Scheme. Retrieved August 2024, from https://www.health.gov.au/our-work/ssba-regulatory-scheme.

REFERENCES

- Gov. of France (Government of 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 France (Government of 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.
- Gov. of Germany (Government of Germanydes 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 (Government of the Netherlands). (2022). National Knowledge Security Guidelines: Secure International Collaboration. The Hague, the Netherlands: Gov. of Netherlands.
- Gov. of Netherlands (Government of the Netherlands). (2023). Besluit toepassingsbereik sensitieve technologie.
- Gov. of New Zealand (Government of New Zealand). (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 New Zealand (Government of New Zealand). (2022). Due Diligence Assessments for Espionage and Foreign Interference Threats. Wellington, New Zealand: Protective Security Requirements.
- Gov. of New Zealand (Government of New Zealand). (2024). New Zealand Strategic Goods List. Wellington, New Zealand: Ministry of Foreign Affairs and Trade.
- Gov. of United Kingdom (Government of the United Kingdom). (2023). Export controls: Dual-use items, software and technology, goods for torture and radioactive sources. Retrieved August 2024, from https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources.
- Gov. of United Kingdom (Government of the United Kingdom). (2024a). National Security and Investment Act 2021.
- Gov. of United Kingdom (Government of the United Kingdom). (2024b). National Security and Investment Act: Details of the 17 types of notifiable acquisitions. Retrieved June 2025, from 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 (Government of the United Kingdom). (2025a). Academic Technology Approval Scheme (ATAS). Retrieved August 2024, from https://www.gov.uk/guidance/academic-technology-approval-scheme.

REFERENCES

- Gov. of United Kingdom (Government of the United Kingdom). (2025b). UK Strategic Export Control List. London, United Kingdom: United Kingdom Department for Business and Trade.
- Gov. of United States (Government of the United States). (1985). NSDD-189: National Policy on the Transfer of Scientific, Technical and Engineering Information. Washington, D.C.: Gov. of United States.
- Gov. of United States (Government of the United States). (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 (Government of the United States). (2022). CHIPS and Science Act.
- Gov. of United States (Government of the United States). (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.
- ISED (Innovation, Science and Economic Development Canada). (2023a). Policy on Sensitive Technology Research and Affiliations of Concern. Ottawa, ON: Government of Canada.
- ISED (Innovation, Science and Economic Development Canada). (2023b). National Security Guidelines for Research Partnerships. Ottawa, ON: Government of Canada.
- JASON. (2019). Fundamental Research Security. McLean, VA: MITRE Corporation.
- JASON. (2024). Safeguarding 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., & Fagot-Largeault, A. (2019). Recherches duales a 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 & DFG (German National Academy of Sciences Leopoldina and German Research Foundation). (2022). Scientific Freedom and Scientific Responsibility Recommendations for Handling of Security-Relevant Research. Halle, Germany: Leopoldina & DFG.
- MPG (Max Planck Society). (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.

REFERENCES

- NPSA & NCSC (National Protective Security Authority and National Cyber Security Centre). (2022). Trusted Research: Guidance for Industry. London, United Kingdom: NPSA & NCSC.
- NPSA & NCSC (National Protective Security Authority and National Cyber Security Centre). (2024a). Trusted Research: Guidance for Academics. London, United Kingdom: NPSA & NCSC.
- NPSA & 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 (Netherlands Ministry of Education, Culture and Science). (n.d.a). About us: submit your question to the National Contact Point. Retrieved May 2025, from https://english.loketkennisveiligheid.nl/about-us.
- OCW (Netherlands Ministry of Education, Culture and Science). (n.d.b). National Contact Point for Knowledge Security. Retrieved August 2024, from 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.
- PHAC (Public Health Agency of Canada). (2018). Canadian Biosafety Guideline - Dual-Use in Life Science Research. Ottawa, ON: Government of Canada.
- PHAC (Public Health Agency of Canada). (2022). Canadian Biosafety Standard, Third Edition. Ottawa, ON: Government of Canada.
- PHAC (Public Health Agency of Canada). (2024). Frequently asked questions (FAQs): Regulations. Retrieved August 2024, from https://www.canada.ca/en/public-health/corporate/mandate/about-agency/acts-regulations/public-health-agency-canada-interpretation-policy/frequently-asked-questions-faqs-regulations.html.
- PSPC (Public Services and Procurement). (2024). Controlled goods: Examining, possessing or transferring. Retrieved July 2024, from https://www.canada.ca/en/public-services-procurement/services/industrial-security/controlled-goods.html.
- PSPC (Public Services and Procurement Canada). (2025). Register in the Controlled Goods Program. Retrieved June 2025, from https://www.canada.ca/en/public-services-procurement/services/industrial-security/controlled-goods/about-program/register.html.
- RIVM (Dutch National Institute for Public Health and the Environment). (n.d.a). Biosecurity Office. Retrieved August 2024, from https://www.bureaubiosecurity.nl/en.

REFERENCES

- RIVM (Dutch National Institute for Public Health and the Environment). (n.d.b). Dual-Use Quickscan. Retrieved May 2024, from https://dualusequickscan.com/en/.
- RIVM (Dutch National Institute for Public Health and the Environment). (n.d.c). Pillars of good practice. Retrieved September 2024, from https://www.bureaubiosecurity.nl/en/pillars-of-good-practice.
- SGDSN (French Secretariat-General for National Defence and Security). (2012). Circulaire Interministerielle de mise en oeuvre du dispositif de protection du potentiel scientifique et technique de la nation. Paris, France: SGDSN.
- SGDSN (French Secretariat-General for National Defence and Security). (2018). Protection numerique du potentiel scientifique et technique de la nation. Paris, France: SGDSN.
- Stibbe. (2023). Ready, set, go! The Dutch national security screening FDI regime takes off. Retrieved August 2024, from https://www.stibbe.com/publications-and-insights/ready-set-go-the-dutch-national-security-screening-fdi-regime-takes-off.
- U15. (2023). Safeguarding Research in Canada: A Guide for University Policies and Practices. n.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.