swissuniversities

swissuniversities
Effingerstrasse 15, Case Postale
3001 Berne
www.swissuniversities.ch

Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities

swissuniversities

Mentions légales

Mandant	
Responsable de projet	Günther Dissertori
Version du rapport	15.09.2025
Auteur/e du rapport	Dimitri Sudan / dimitri.sudan@swissuniversities.ch

swissuniversities

Table of contents

Annex

swissuniversities

Executive Summary

This report examines the critical challenges and opportunities facing Switzerland's higher education and research ecosystem in the context of evolving knowledge security requirements. As international research collaboration intensifies within an increasingly complex geopolitical landscape, Swiss institutions must balance their commitment to academic freedom and openness with necessary security measures to protect sensitive knowledge and technologies. This analysis provides a comprehensive framework for implementing effective knowledge security measures while preserving Switzerland's research excellence and international competitiveness. In this sense the working group recommends a comprehensive three-axis approach to enhancing knowledge security in Switzerland:

- The first axis focuses on building security awareness and capabilities within Swiss higher education institutions.
- The second axis addresses the need for improved regulatory frameworks that support knowledge security measures.
- The third axis focuses on developing national-level coordination mechanisms and strategic oversight capabilities. This approach recognises that knowledge security challenges require coordinated responses across multiple institutions and government agencies.

swissuniversities

1. Introduction and Definition of Knowledge Security

1.1 Mandate to and composition of the national working group on knowledge security

The Swiss Higher Education Council has tasked swissuniversities with coordinating the position of higher education institutions on knowledge security at the academic level, while considering scientific freedom, the autonomy of higher education institutions and, therefore, the responsibility incumbent upon each institution. The main task of the working group is to develop consistent criteria to help all institutions in the higher education sector to establish their knowledge security control processes, particularly in the context of student admission, staff recruitment or exchange, invitations to foreign researchers and, more generally, the launch of new international collaborations, but also in the context of data protection, sensitive know-how and technologies, and the prevention of undesirable knowledge/data transfer. The criteria to be defined must focus in particular on the following areas:

a) Criteria for defining sensitive countries, institutions and sources of funding;
b) Criteria for defining research areas, technologies and infrastructure critical to national security;
c) Criteria for restricting student admission based on security concerns.

The working group must also draw up an inventory of the knowledge security resources available to higher education institutions at national and international level.
Composition of the national working group:

- Günther Dissertori, Rektor ETHZ (chairperson)
- Crispino Bergamaschi, Direktionspräsident FHNW
- Ambrogio Fasoli, Vice-président pour les affaires académiques EPFL
- Christian Schwarzenegger, Prorektor, Univ. Zürich, Präsident der Delegation Open Science
- Frédéric Herman, Recteur Univ. Lausanne
- Stéphane Berthet, Président de la délégation relations internationales, Vice-recteur UNIGE
- Primo Schär, Vizerektor Forschung Univ. Basel
- Silvia Nast, Export control and international shipping, ETHZ
- Thomas Gächter, Professor für Staats-, Verwaltungs- und Sozialversicherungsrecht, Univ. Zürich
- Floriane Gasser, canton FR
- Dorothea Christ, Kanton ZH
- Jacques Ducrest, Chef de la division relations internationales
- Dimitri Sudan, swissuniversities (secretary)

1.2 Scope and Structure of the Report

This report addresses the multifaceted challenge of knowledge security in Switzerland's higher education and research sector. The analysis follows a structured approach examining the current state of knowledge security in Swiss institutions, international best practices, and concrete recommendations for implementation. The report serves as a strategic guide for university administrators, policymakers, and research funding organisations to develop comprehensive knowledge security frameworks that protect sensitive research while maintaining academic freedom.

The analysis is structured around six core components: definitional foundations, problem assessment, international comparative analysis, strategic recommendations, implementation roadmap, and concrete deliverables. Each section builds upon previous findings to create a coherent framework for action.

1.3 Definition of Knowledge Security

Before any strategy and initiatives can be developed, it is important to have a common understanding of the concept that is at the heart of the strategy: knowledge security. Both

‘knowledge security’ and ‘research security’ have been widely used to address similar issues, raising questions on the differences and nuances between the two concepts. The working group shares the perspective of the German Council of Science and Humanities, as set out in their most recent position paper (May 2025), which refers to knowledge security. They perceive this to be broader than research security, encompassing not only research activities, but also all scientific activities, including the exchange of personnel and students.[1]

For the purposes of this report, **knowledge security** is defined as “*the **prevention of the unwanted transfer of sensitive information, know-how, and technology, the mitigation of foreign interference** in higher education and research, and the reduction of dependencies that could endanger national security and competitiveness. **Ethical concerns** are also important aspects. The aim of knowledge security is to **protect core scientific values, ensure that international cooperation remains ethical and safe, and safeguard national interests and values**”.*[2] This definition encompasses several critical dimensions:

Institutional Security: Measures to protect research facilities, data systems, and intellectual property from unauthorised access or exploitation. This includes cybersecurity protocols, physical security measures, and access control systems designed to safeguard sensitive research environments.

Information Security: Protection of research data, findings, publications, and related documentation from unauthorised disclosure or manipulation. This encompasses both digital and physical information assets, including research methodologies, experimental data, and preliminary findings that could have strategic value.

Personnel Security: Vetting and monitoring procedures for researchers, students, and staff members who have access to sensitive research areas. This includes background checks, security clearance procedures, and vigilance over individuals who have access to sensitive technology to prevent the uncontrolled leakage of research data and findings prior to publication that may also be subject to export control.
Technology Security: Specific measures to protect dual-use technologies, critical infrastructure research, and emerging technologies that could have significant implications for national security or economic competitiveness. This includes export control compliance, technology transfer restrictions, and enhanced oversight of research with potential military or security applications.

Collaborative Security: Frameworks for assessing and managing risks associated with international research partnerships, joint ventures, and collaborative projects. This encompasses due diligence procedures for international partners, contractual safeguards, and ongoing monitoring of collaborative relationships.

The working group's approach to knowledge security emphasises proportionality, ensuring that security measures are commensurate with actual risks while avoiding unnecessary restrictions on legitimate research activities. The framework recognises that knowledge security is not about restricting research or limiting international collaboration, but rather about implementing appropriate safeguards that enable continued openness while protecting against genuine security risks.

Research integrity vs knowledge security: While research integrity is primarily concerned with ethical conduct and scientific rigor, knowledge security is about protecting valuable research assets and maintaining competitive advantages or national security interests. These two concepts can sometimes create tensions - for example, between the scientific

1 Wissenschaftsrat, Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche (Positionspapier 2025) 23.
2 Leo Eigner, Knowledge Security at Stake, March 24, p. 1.

principle of open sharing of knowledge (integrity) and the need to protect sensitive research (security). But both, integrity and security, are essential for ensuring trust in science and international collaboration.

2. Description of the Problem

2.1 The Fundamental Tension: Openness versus Security

Switzerland's research and innovation ecosystem has historically thrived on principles of openness, international collaboration, and academic freedom. These values have contributed to the country's position as a global leader in research excellence, with Swiss institutions consistently ranking among the world's top universities and research centres.

swissuniversities

However, the contemporary geopolitical landscape presents unprecedented challenges to this traditional model of open science. Increasing concerns about technology transfer, intellectual property theft, foreign interference in research, and the potential militarisation of civilian research have created pressure for enhanced security measures. This evolving context has shaped the understanding of openness in research under the guiding principle “as open as possible, as secure as necessary”, with a noticeable shift in emphasis from the first half of the phrase toward increasing attention on the latter.[3] The challenge for Switzerland lies in developing approaches that maintain research excellence and international competitiveness while addressing legitimate security concerns.

The tension between openness and security manifests in several key areas. First, international collaboration, which has been essential to Swiss research success, now requires careful risk assessment and management. Indeed, potential incompatibilities between international collaborations need to be carefully analysed. Second, the recruitment of international talent, particularly from sensitive countries, necessitates enhanced vetting procedures that may conflict with traditional academic hiring practices. Third, the sharing of research results and methodologies, fundamental to scientific progress, must be balanced against concerns about unwanted technology transfer and knowledge leakage.

2.2 Current Strengths of the Swiss System

Switzerland's knowledge security framework benefits from several inherent strengths that provide a foundation for enhanced knowledge security measures. The country's federal structure allows for flexible implementation of security measures tailored to local conditions while maintaining national coordination. Swiss institutions have developed sophisticated governance structures and risk management capabilities through their experience in managing complex international partnerships and high-value research projects.

The Swiss research ecosystem demonstrates remarkable resilience and adaptability, characteristics that will be essential for implementing new security measures without compromising research excellence. Institutions like ETH Zurich and EPFL have already begun developing internal protocols for managing sensitive research and assessing collaboration risks. These early initiatives provide valuable models for broader implementation across the Swiss higher education sector.

Switzerland's strong tradition of regulatory compliance, developed through experience with financial services and other regulated industries, provides institutional knowledge that can be adapted to knowledge security requirements. The country's expertise in managing dual-use technologies through export control regimes offers relevant experience for broader knowledge security applications.

3 Van der Molen, I., Gheorghe, D., Daouti, C., & Eechaudt, V. (2023). Keeping science open? Current challenges in the day-to-day reality of universities (M. Björnmalm & J. Moynat, Eds.).

The Swiss research funding system, with its emphasis on peer review and scientific excellence, provides mechanisms[4] that can be adapted to incorporate security considerations without compromising research quality. The Swiss National Science Foundation (SNSF) has begun developing capabilities for assessing security implications of its funded research projects.

2.3 Current Weaknesses and Vulnerabilities

Despite these strengths, the Swiss system faces significant vulnerabilities that require systematic attention. The decentralised nature of Swiss higher education, while promoting innovation and flexibility, creates coordination challenges for implementing consistent security measures across institutions. Different universities may develop varying approaches to similar security challenges, potentially creating gaps in protection or inconsistent standards. Many Swiss institutions lack dedicated expertise in knowledge security assessment and risk management. Traditional academic administrators may not have the specialised knowledge required to evaluate complex security implications of research projects or international partnerships. This capability gap represents a fundamental challenge that must be addressed through training, recruitment, or external support mechanisms.

swissuniversities

The Swiss academic system currently lacks comprehensive legal frameworks specifically designed for knowledge security. While existing regulations cover some aspects of export control and classified research, gaps remain in areas such as foreign interference prevention, technology transfer oversight, security screening of individuals and due diligence requirements for international partnerships and admission of students and researcher. Information sharing and coordination mechanisms between institutions, government agencies, and security services require enhancement. Current systems may not provide adequate channels for sharing threat intelligence, coordinating responses to security incidents, or developing consistent approaches to emerging challenges.

2.4 Evolving Threat Landscape

The threats facing Swiss higher education institutions have evolved significantly in recent years, requiring updated security approaches. State-sponsored espionage targeting higher education institutions has increased, with particular focus on emerging technologies such as artificial intelligence, quantum computing, biotechnology, and advanced materials. These threats often involve sophisticated approaches that may not be immediately apparent to traditional academic security measures.

Economic espionage targeting Swiss innovations has intensified, with foreign actors seeking to acquire competitive advantages through unauthorised access to research results, methodologies, and intellectual property.[5] This threat extends beyond traditional military technologies to include civilian research with potential dual-use applications.

Foreign interference in higher education institutions has become more prevalent, involving attempts to influence research agendas, suppress unfavourable findings, or gain access to sensitive research networks. These activities may involve seemingly legitimate academic exchanges or collaboration proposals that serve as covers for intelligence collection or influence operations.[6]

Cybersecurity threats specifically targeting higher education institutions have proliferated, with attackers seeking to access research data, intellectual property, and sensitive

4 The Swiss National Science Foundation (SNSF) is the most important institution in funding public research and funds excellent research at universities and other institutions.
5 Examples in Prophylax-Programm des NDB - Technolpol *Academia as a Target* pp. 20 and ff.
6 One example: https://www.nzz.ch/schweiz/drohnen-fuer-die-diktatur-wie-schweizer-forschung-in-iranische-waffen-technologie-floss-ld.1892049

communications.[7] Switzerland has updated its Digital Switzerland Strategy for 2025, with a focus on cybersecurity and emerging technologies, recognising the critical importance of protecting digital research assets.

This evolving landscape raises crucial issues for Switzerland's scientific and technological future. Indeed, in an increasingly tense geopolitical context where knowledge security and protection of sensitive technologies have become national priorities, Switzerland must demonstrate its ability to maintain the highest standards of knowledge security. Exclusion from major international research programs, as has already occurred with certain European projects, could seriously compromise Switzerland's position as a global innovation hub and affect the competitiveness of its academic institutions and high-tech companies.[8] This proactive approach is all the more critical since Switzerland, as a small country, largely depends on its ability to attract international talent and participate in global research networks to maintain its competitive advantage in the knowledge economy.

swissuniversities

3. Selection of Schemes in Partner Countries and at International Level

Most European countries similar to Switzerland have adopted bottom-up systems that fall into the two categories of 'public awareness campaigns and other outreach activities' and 'science and technology regulation and soft law'. The Netherlands and the UK are exceptions with their much more holistic approach and are the only ones among our main European partners to offer a single national contact point for universities. However, their approach remains largely bottom-up and respects the autonomy of universities and academic freedom. Canada, the United States and Australia have the most extensive and interventionist systems.

For a systematic overview, see factsheets annex 1 "*Enhancing Knowledge Security in Switzerland: Initiative factsheets (2025)*".[9] While this chapter takes a country-by-country approach to identifying how knowledge security is addressed and enhanced nationally and regionally, the factsheets provide concrete examples of alternative models and key aspects of popular initiatives, as well as critical thinking questions for reflection. The purpose is to provide practical guidance and a point of reference for implementing certain initiatives. The OECD-STIP-COMPASS on Research security shares 206 policy initiatives around the world to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination. The portal is regularly updated.

3.1 European Union Framework

The European Commission proposed a Council Recommendation on enhancing knowledge security on 24 January 2024 as part of the European Economic Security Strategy, establishing a comprehensive framework for member states to address knowledge security challenges while maintaining scientific excellence and openness.

7 See for example the chapter "Threat to critical infrastructure" of the Situation Report of the Federal Intelligence Service, 2025.

8 The Council Recommendation is a good example, offering fourteen recommendations to EU member states: These include the development of national approaches, which may include the formulation of national guidelines or a list of relevant measures and initiatives; the creation or reinforcement of support services to help actors in the R&I sector to deal with risks related to international cooperation in research; the reinforcement of cross-sectoral cooperation within the government; or the development of the evidence base for research security policymaking. The Recommendation also includes a dedicated set of proposed measures for member states' engagement with research funding organisations and research-performing organisations. Furthermore, the Council Recommendation directs eleven recommendations specifically to the EC, including exploring and assessing options for more structural support, like the possible establishment of a European Centre of Expertise on Research Security. The Recommendation mentions that the monitoring of the implementation will be done by the EC, in cooperation with the Member States. Over time, dealing with this issue could become a condition for participation in EU research programmes.

9 Manon Hufschmid, *Enhancing Knowledge Security in Switzerland: Initiative factsheets*, July 2025.

The EU approach emphasises several key principles that are relevant to Swiss considerations. First, the framework recognises that knowledge security measures must be proportionate to identified risks and should not unnecessarily restrict legitimate research activities. Second, the EU emphasises the importance of maintaining academic freedom, international collaboration and openness —guided by the principle "as open as possible, as closed as necessary" — while implementing appropriate safeguards. Third, the framework calls for enhanced coordination between member states, Higher Education Institutions (HEI's), and security services.

swissuniversities

EU knowledge security standards focus on the protection of classified information, security assessments that review potential misuse of research for malevolent purposes, and other security concerns including national security implications. The EU framework provides detailed guidance on risk assessment methodologies, due diligence procedures for international partnerships, and information sharing mechanisms.

The EU approach includes specific provisions for critical technology identification and protection. The framework establishes processes for regularly updating lists of sensitive research areas and technologies that require enhanced security measures. This dynamic approach allows for adaptation to evolving threat landscapes and emerging technological developments.

3.2 Netherlands: The National Contact Point Model

The Netherlands recognises that science cannot exist without international cooperation, and that the leading position and good academic reputation of Dutch knowledge institutions are linked to academic freedom and openness guaranteed in the Netherlands. However, the Dutch approach also acknowledges growing security concerns that require systematic attention.

The Government of the Netherlands has established a National Contact Point for Knowledge Security that serves as a central coordination mechanism for knowledge security issues. This model provides several advantages that could be relevant for Swiss implementation. The contact point serves as a single point of coordination for government agencies, higher education institutions, and security services, facilitating information sharing and coordinated responses to security challenges.

The Dutch approach emphasises building security awareness within HEI's rather than imposing rigid restrictions on research activities. The contact point provides guidance, training, and support to help institutions develop appropriate security measures tailored to their specific research activities and risk profiles.

Knowledge security has been a prominent topic in public discourse in the Netherlands in recent years, with increased attention to risks associated with international exchanges while maintaining the viewpoint that academia thrives with international collaboration. This balanced approach provides a model for managing the tension between openness and security. The Netherlands has developed comprehensive guidance materials and assessment tools that help HEI's to evaluate the security implications of their activities. These resources provide practical frameworks for conducting due diligence on international partners, assessing technology transfer risks, and implementing appropriate safeguards for sensitive research areas.

3.3 Germany: Institutional Integration Approach

Germany has implemented a comprehensive approach to knowledge security that integrates security considerations into existing institutional structures and processes. The German

model emphasises building security capabilities within higher education institutions rather than relying primarily on external oversight or control mechanisms.

German universities have been encouraged to establish dedicated knowledge security offices that provide specialised expertise in risk assessment, security planning, and compliance management. These offices work closely with research administrators, faculty members, and security services to develop tailored approaches to knowledge security challenges.

swissuniversities

The German approach includes specific provisions for enhanced due diligence in international research partnerships. German institutions are required to conduct thorough assessments of potential international partners, including evaluation of their governance structures, funding sources, and potential connections to foreign governments or military organisations. The Federal Ministry of Education and Research has developed sophisticated frameworks for identifying and protecting critical technologies and sensitive research areas. These frameworks are regularly updated to reflect evolving threat landscapes and emerging technological developments. The German approach emphasises transparency and consultation with research communities in developing and implementing these frameworks.[10]

The German model includes provisions for regular security training and awareness programs for researchers, administrators, and students. These programs help build security consciousness throughout higher education institutions while maintaining focus on research excellence and academic freedom.[11]

3.4 Norway and Sweden: Nordic Coordination Model

The Nordic countries have developed coordinated approaches to knowledge security that emphasise regional cooperation and information sharing. This model recognises that security threats often transcend national boundaries and require coordinated responses from multiple countries.
The Norwegian Directorate for Higher Education and Skills has implemented comprehensive frameworks for assessing and managing security risks in higher education institutions. The Norwegian approach emphasises building security capabilities within higher education institutions while maintaining strong coordination with government security services. Norwegian institutions are required to conduct regular security assessments and develop security plans tailored to their specific research activities.

Sweden has focused on developing sophisticated threat assessment capabilities that help higher education institutions understand and respond to evolving security challenges. The Swedish approach includes regular briefings for research administrators and faculty members on current threat landscapes and emerging security concerns.

The Nordic model includes provisions for regular coordination meetings between knowledge security officials from different countries. These meetings facilitate information sharing about emerging threats, best practices in security implementation, and coordinated responses to regional security challenges.

3.5 Canada: Comprehensive and Prescriptive Framework

Canada has developed a comprehensive knowledge security framework to protect its research ecosystem while maintaining academic freedom and international collaboration. The government recognizes that the open nature of Canadian research, while valuable, can pose

10 See for example: Wissenschaftsrat, *Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche. Positionspapier*, 2025 and Federal Ministry of Education and Research, Technological sovereignty for Germany and Europe, 2025.
11 See initiative KIWi Compass, No red lines of the DAAD.

national security risks through foreign interference, espionage, and intellectual property theft.

The cornerstone of Canada's knowledge security approach is the Policy on Sensitive Technology Research and Affiliations of Concern, which came into effect in early 2024. This policy applies to all federal research funding and requires researchers to disclose affiliations with foreign entities that may pose security risks. The policy specifically targets sensitive technologies and requires due diligence in research partnerships while allowing consideration of research affiliations in funding decisions.

swissuniversities

Canada has also implemented the National Security Guidelines for Research Partnerships (NSGRP), which provides a framework for consistent, risk-targeted due diligence to identify and mitigate potential national security risks related to private sector partnerships. These guidelines balance the need for security with the principles of academic freedom and open research.

The Research Security Centre, located within Public Safety Canada, serves as the central hub for knowledge security efforts. The Centre provides guidance and advice to the research community and institutions on protecting their research. It operates through a Research Security Advisors Network located across regions, offering direct support to researchers and institutions.

The Centre conducts "Safeguarding Science" workshops aimed at sharing research security best practices within Canada's scientific and academic communities. These workshops help faculty understand and implement measures to protect research and intellectual property.

3.6 Australia: Government Prescriptive Model

Australia has developed a comprehensive approach to knowledge security that evolved significantly since 2018, when the Australian government made serious strides in countering espionage and foreign interference through policy and legislative reforms targeting the research and university sectors. The framework addresses the reality that foreign states have actively targeted Australia's research ecosystem—seeking to influence research agendas, extract sensitive information and exploit institutional vulnerabilities.
Australia's knowledge security framework is built around several core instruments. The Guidelines to Counter Foreign Interference in the Australian University Sector provide a foundational approach, offering enduring, specific and measurable guidance that considers the evolving risks and threats of foreign interference. These guidelines support universities in developing or examining existing tools, frameworks and resources to assess and mitigate foreign interference risks.

The Protective Security Policy Framework (PSPF) underwent major updates in 2024, with the first PSPF Release issued on 1 November 2024. This framework prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally.

The Department of Education serves as a central coordinator, working with Australia's higher education and research sector to counter risks of foreign interference. The Australian Research Council (ARC) has integrated research security considerations into its funding processes, recognizing that Australian world-class research is an important contribution to developing technologies that underpin our future.

The Department of Home Affairs brings together federal law enforcement, national and transport security functions, working to keep Australia safe through comprehensive security oversight. Individual universities have also implemented their own foreign interference

policies, with institutions like James Cook University establishing frameworks that integrate cybersecurity, information security, and defence collaboration protocols.

Australia's approach emphasizes that the presence of a foreign interference risk in relation to a research project does not mean a project should not be funded. Instead, when potential risks are identified, the relevant administering organization is contacted and provided the opportunity to outline risk mitigation strategies. This balanced approach allows research to continue while ensuring appropriate security measures are in place.

swissuniversities

The framework recognizes the limited scope of sensitive research within universities. According to data released by the Australian Bureau of Statistics in May, in 2022 spending by the higher education sector on research and development related to 'defence' stood at $305 million, just 2 percent of their total R&D spending worth $14 billion.

Australia has implemented several legislative measures to support knowledge security. The Defence Trade Controls Amendment Bill 2024 passed parliament in March to facilitate technology sharing among AUKUS partners while maintaining appropriate security controls. The Cyber Security Act 2024 provides additional protective measures for critical infrastructure and sensitive information.

3.7 United States: prescriptive and enforcement-oriented

The United States has developed a comprehensive framework to protect critical research and technology from foreign interference, particularly following concerns about economic espionage and technology transfer to strategic competitors.

The U.S. maintains robust export control systems through the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR), which restrict the transfer of dual-use technologies and defense-related research. The Commerce Department's Entity List identifies foreign entities subject to specific restrictions.

The National Science Foundation (NSF) and other federal agencies have implemented disclosure requirements for international collaborations, foreign funding sources, and potential conflicts of interest. The CHIPS and Science Act of 2022 strengthened these measures by requiring grant recipients to disclose foreign government ties and establishing research security training programs.

The Committee on Foreign Investment in the United States (CFIUS) expanded its scope to review certain university partnerships and technology transfers. Federal agencies now require universities to report foreign gifts exceeding $250,000 and maintain databases of international research collaborations.

The U.S. government has implemented visa restrictions and enhanced vetting procedures for researchers from certain countries, particularly in sensitive fields like artificial intelligence, quantum computing, and biotechnology. The China Initiative (later restructured as the Strategy for Countering Nation-State Threats) targeted alleged technology theft and research misconduct.

3.8 Japan: institutional responsibility and self-regulation

Japan has adopted a more recent but increasingly comprehensive approach to research security, balancing openness with national security concerns while maintaining strong international research collaboration.

The Economic Security Promotion Act (2022) established a legal foundation for protecting critical technologies and research. This legislation created mechanisms for screening foreign investment in sensitive sectors and regulating technology transfers that could affect national security.

The Ministry of Education, Culture, Sports, Science and Technology (MEXT) issued guidelines encouraging universities to establish internal review systems for international

collaborations. These guidelines emphasize institutional responsibility for assessing risks associated with foreign partnerships while maintaining academic freedom.
Japan has identified key technologies requiring protection, including semiconductors, AI, quantum technologies, biotechnology, and advanced materials. The government established screening mechanisms for research involving these areas, particularly when foreign entities are involved.
Japan actively participates in multilateral export control regimes and has strengthened coordination with like-minded partners, particularly through the Quad partnership (with the U.S., Australia, and India) and G7 mechanisms. This includes sharing best practices and coordinating approaches to research security.
While maintaining relatively open policies for international researchers, Japan has enhanced background checks and monitoring for certain categories of foreign researchers, particularly those working in sensitive technological areas.

4. Recommendations for Switzerland

The Swiss system is still very modest compared to the importance and excellence of its education and research system, not to mention its high level of internationalisation. At the national level we have in particular the "Code of Conduct for Scientific Integrity (2021)" and the guide "Towards Responsible International Collaborations: A Guide for Swiss Higher Education Institutions (2022)". The guidelines are intended to support Swiss Higher Education Institutions and their communities when engaging in international collaborations. They should help them to clarify important aspects of the collaboration in advance to ensure that it is based on mutual values and shared interests.

4.1 Framework for Implementation: The Three-Axis Approach

Based on the analysis of international best practices and Swiss institutional capabilities, this report recommends a comprehensive three-axis approach to enhancing knowledge security in Switzerland. This framework balances the need for enhanced security measures with preservation of academic freedom and research excellence.

Axis 1: Institutional Awareness and Compliance Infrastructure

The first axis focuses on building security awareness and capabilities within Swiss higher education institutions. This approach recognises that effective knowledge security requires active engagement and ownership by higher education institutions themselves, rather than relying solely on external oversight or control mechanisms.

Introduction of Compliance Officers[12] or specialised internal units: Swiss higher education institutions should establish their own specialised internal units (Fachstelle/Service spécialisé) for managing knowledge security issues within their organisations. A specialized internal unit similar to the one at ETH Zurich which has been developing and implementing an internal control system for dual-use goods since 2016 to manage knowledge security and compliance issues. Such specialist unit should be tailored to the size of the institution, its research portfolio and its risk profile. Large research universities, such as ETH Zurich and EPFL, may need several subject-specific specialist units to deal with different compliance issues, while smaller institutions can share resources or draw on external expertise.

The Compliance officers or the internal unit should possess expertise in knowledge security, risk assessment, and regulatory compliance. They should maintain regular contact with the national coordination platform, and other higher education institutions to stay current on evolving threat landscapes and best practices. The compliance officer or specialized internal

12 The working group chose this category while being aware that it can take different forms depending on the institution and that it is on a different level from the financial and control services that already exist in higher education institutions.

unit role should include responsibility for conducting security assessments, developing institutional security policies, providing training and guidance to researchers, and serving as liaison with government agencies

Training and Awareness Programs: Institutions should implement comprehensive training programs for researchers, administrators, and students on knowledge security issues. These programs should cover threat awareness, risk assessment methodologies, compliance requirements, and best practices for managing international collaboration safely. Training should be tailored to different audiences and updated regularly to reflect evolving threats and requirements.

Policy Development and Implementation: Institutions should develop comprehensive knowledge security policies that address all aspects of their research activities. These policies should cover due diligence procedures for international partnerships, technology transfer protocols, information security measures, and procedures for reporting security concerns. Policies should be developed through consultation with research communities and should emphasise proportionality and transparency.

Axis 2: Legal and Regulatory Framework Enhancement
The second axis addresses the need for improved regulatory frameworks that support knowledge security measure. This approach recognises that effective security measures require appropriate legal foundations and clear regulatory guidance.

Legal Basis for Admission Restrictions: The Confederation and the cantons should develop legal frameworks that enable higher education institutions to restrict admission or access for individuals who pose demonstrable security risks. These frameworks should include clear criteria for risk assessment, due process protections, and appeal mechanisms. The legal basis should be developed through consultation with higher education institutions and relevant government agencies. Pending these various legislative changes, a pragmatic and transitional solution consists of adapting the "Ordinance of the Swiss Higher Education Council on the coordination of teaching in Swiss higher education institutions" by introducing the possibility for higher education institutions to refuse admission for reasons of knowledge security. The advantage of this transitional solution is that it can be introduced quickly and allows for a certain degree of harmonisation of practices in this field.
Export Control and Technology Transfer Regulations: Switzerland should review and enhance its export control and technology transfer regulations to address evolving threats and emerging technologies. This review should include consultation with higher education institutions, industry representatives, and international partners to ensure that regulations are effective and proportionate.

Information Sharing Frameworks: Legal frameworks should be developed to facilitate appropriate information sharing between higher education institutions, government agencies, and security services. These frameworks should include clear guidelines on what information can be shared, under what circumstances, and with appropriate privacy protections.

Axis 3: National Coordination and Strategic Oversight
The third axis focuses on developing national-level coordination mechanisms and strategic oversight capabilities. This approach recognises that knowledge security challenges require coordinated responses across multiple institutions and government agencies.

National Coordination Mechanism: Switzerland should establish a national coordination mechanism for knowledge security, potentially modelled on the Dutch National Contact Point approach. This mechanism should serve as a central point for information sharing, policy coordination, stakeholder support and strategic planning. The establishment of such a national

resource assists also the progressive introduction of the Compliance Officer or specialised internal unit position in the Swiss academic institutions who is in charge managing the knowledge security issues. The National Contact Point/Platform is not responsible for assessing individual cases from different academic institutions.

Enhanced Collaboration with Immigration Authorities: Higher education institutions should strengthen their collaboration with the State Secretariat for Migration (SEM) to enhance vetting procedures for international researchers and students. This collaboration should include development of streamlined information sharing mechanisms, enhanced background check procedures, and coordinated responses to security concerns.[13]

swissuniversities

Strategic Threat Assessment: Switzerland should develop capabilities for conducting regular strategic threat assessments that inform knowledge security policies and priorities. These assessments should draw on intelligence from multiple sources and should be shared appropriately with higher education institutions and other relevant stakeholders.

International Cooperation: Switzerland should strengthen its participation in international knowledge security cooperation mechanisms. This could include formal agreements at different levels with key partner countries for information sharing and coordinated responses to security challenges. Switzerland should also actively participate in relevant international organisations and forums addressing knowledge security issues.

4.2 Critical Technology Identification Process

The implementation of effective knowledge security measures requires systematic approaches to identifying critical technologies and sensitive research areas that require enhanced protection. This process should be dynamic, transparent, and developed through consultation with research communities and relevant stakeholders.

Technology Assessment Framework: The national coordination platform should develop a comprehensive framework for assessing the security implications of different research areas and technologies. This framework should consider multiple factors including potential military applications, technical readiness level, economic strategic value, vulnerability to foreign exploitation, and importance to Swiss national interests.

Several countries take the EU's criteria (see below) and list of critical technologies into account but recognise that critical technologies are unique to a national context, thus necessitating an individual, national approach.[14] These lists are not meant to replace the exercise of evaluating every project and cooperation on a case-by-case basis, nor should it prevent the ongoing work of pursuing a mindset shift among the research community when it comes to knowledge security. In her analysis of different countries' practices in defining critical technologies (CT), Manon Hufschmid identified the following three characteristics[15]:

- Identification is not a top-down process – requires an all-stakeholder approach (also supports institutional autonomy)
- Identifying CTs as an additional measure to enhance knowledge security – not a tool to accept/reject international collaborations & research projects
- CT lists are living documents – flexibility to adapt lists to new & emerging technologies is crucial. They are living documents, which should be flexible to adapt to technological developments.

13 See for example see Fact Sheets ETHZ.

14 For examples: Federal Ministry of Education and Research, Technological sovereignty for Germany and Europe, 2025 and National Science and Technical Council (USA), Critical and emerging technologies list update, 2024.

15 Manon Hufschmid, SwissCore: *Enhancing Knowledge Security in Switzerland: Providing a source of inspiration for SwissCore funders and partners*, 2025.

Criteria	Assessment focus
The technology's enabling & transformative nature	This criterium specifically looks at the technology's potential & relevance for driving significant increases of performance and efficiency, as well as its potential for driving radical changes for sectors, capabilities, etc.
The risk of civil & military fusion	This assesses the technology's relevance for the civil & military sectors & its potential to advance both domains, as well as risk of uses of certain technologies to undermine peace & security.
The risk of misusing the technology for human rights violations	This criteria assesses the technology's potential misuse in human rights violations, as well as restricting fundamental freedoms.

Table 1: The EU's criteria for critical technologies

The assessment framework should include regular review processes to ensure that technology classifications remain current and relevant. The framework should also include provisions for emergency classifications in response to rapidly evolving threats or emerging technologies.

Consultation and Transparency: The critical technology identification process should include meaningful consultation with research communities and industry representatives. This consultation should ensure that technology classifications are based on sound technical analysis and that implementation measures are proportionate to identified risks.
The process should maintain appropriate transparency while protecting sensitive information about specific threats or vulnerabilities. Regular public reporting on the process and its outcomes should be provided to maintain public confidence and accountability.

Implementation Safeguards: Critical technology designations should trigger enhanced security measures rather than research restrictions. The focus should be on protecting sensitive research through improved security protocols, enhanced vetting procedures, and careful management of international collaboration, rather than prohibiting research activities. If Switzerland fails to establish a clear framework for identifying and protecting critical technologies, the country risks finding itself increasingly marginalized from strategic international research partnerships and collaborations that are becoming essential for maintaining competitiveness in advanced research and innovation fields.

4.3 Motivations and Justifications

The recommended approach reflects several key motivations that should guide Swiss implementation of enhanced knowledge security measures. First, the primary goal is to protect Swiss research assets and national interests while preserving the openness and excellence that have made Swiss institutions world leaders in research and innovation.
Second, the approach recognises that knowledge security threats are evolving rapidly and require adaptive responses that can evolve with changing threat landscapes. Static security measures are likely to become obsolete quickly and may impose unnecessary restrictions on legitimate research activities.
Third, the approach emphasises building security capabilities within higher education institutions rather than imposing external restrictions or oversight. This approach recognises that effective security requires active engagement and ownership by research communities themselves.

Fourth, the approach prioritises international cooperation and coordination, recognising that knowledge security challenges transcend national boundaries and require coordinated responses from multiple countries and institutions.
Fifth, it is essential for Switzerland to address this issue very seriously in order to remain a reliable partner and thus avoid being excluded from certain collaborations and/or research programmes. This is a crucial issue in the actual geopolitical developments.

5. Next Steps for Concrete Implementation

5.1 Implementation Timeline and Phases

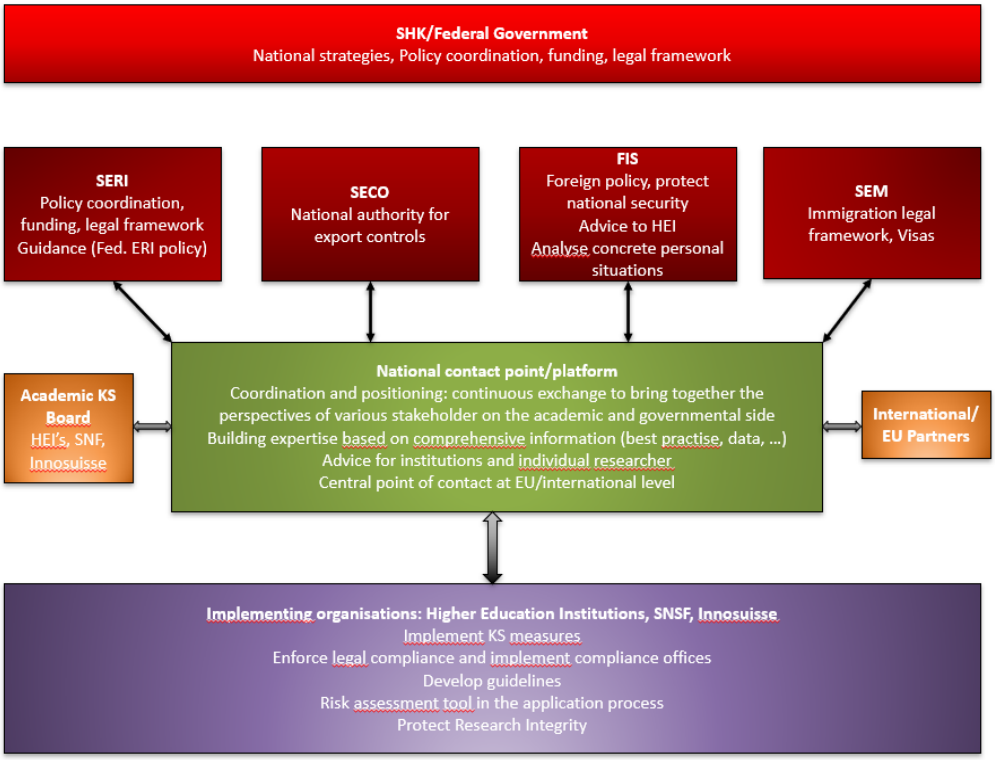
swissuniversities

Implementation must be carried out in steps and involve all relevant stakeholders:

1. Initial steering (2026) – Based on this report, the Higher Education Council, SERI and swissuniversities should formally give a new mandate to a new working group to implement the national coordination platform. One initial task of the platform could be to draft minimum national research safety guidelines, including the definition of "critical technologies" and respective responsibilities. At the same time, close cooperation with SEM and the FDFA should be established to harmonize admission criteria based on security risk. Universities should now begin planning staff training and the election of compliance officers.
2. Legal reinforcement (2026-2027) – Submit to Parliament the necessary legislative amendments (e.g., in legislation on foreigners and export controls) that would explicitly empower HEIs to refuse or monitor certain projects. Federal approval must be obtained for these adjustments before the end of 2027.
3. Institutional rollout (2026–2028) – Establish national coordination in concrete terms, with a budget and resources. Universities will gradually introduce compliance officers or a similar structure/position. Funding agencies (SNSF, Innosuisse) will begin to require clearance for strategic projects from compliance officers.
4. Monitoring and adjustment (2028 and beyond) – Set deadlines (e.g., review in 2028) to assess the effectiveness of the measures. A joint report by the federal government and universities could be published annually, detailing known security incidents and progress made. This will include measuring whether enhanced security has been implemented "without unnecessarily restricting research," as called for by the European Parliament and the OECD.

5.2 Roles and Responsibilities

The successful implementation of enhanced knowledge security measures requires clear definition of roles and responsibilities across multiple stakeholders. Each stakeholder group has specific capabilities and responsibilities that contribute to overall program success. For an example, see annex 2 from the G7 recommendations "G7 Best Practices for Secure and Open Research." Applied to Switzerland, such a division of responsibilities and tasks could be visualised as follows:



5.3 Resource Requirements and Funding

For small and medium-size universities, officer implementation presents financial challenges requiring resolution. It is difficult to provide specific funding information, as each higher education institution must assess its own needs and required resources. It is also possible for several institutions to pool their resources.

6. Products and Outputs

6.1 Compliance Officer or Specialised Units Specifications

The successful implementation of knowledge security measures depends critically on establishing effective capabilities in knowledge security across Swiss HEI's. Compliance officers, specialised units or persons with a similar profile (see example annex 3) are responsible for conducting comprehensive security assessments of research projects, international partnerships, and personnel. This includes developing and implementing due diligence procedures, coordinating with other partners on security matters, and providing guidance to researchers on security requirements and best practices.

Officers or units should maintain current knowledge of threat landscapes and security requirements through regular training and professional development activities. They should also participate in professional networks and information sharing mechanisms with other compliance officers and security professionals.

6.2 Standard Operating Procedures and Guidelines

Comprehensive standard operating procedures should be developed by the national coordination platform to ensure consistent implementation of knowledge security measures across Swiss institutions. These procedures should cover all aspects of knowledge security operations while maintaining flexibility for institutional adaptation.

An ongoing project from swissuniversities addressing the specific challenge of aligning knowledge security with open science may provide a useful foundation. By summer 2026, the project is expected to submit a report to the Delegation Open Science of swissuniversities, featuring a practical toolbox for HEIs and researchers that provides initial orientation and guidance for conducting research in line with Open Science principles and knowledge security requirements.

swissuniversities

Risk Assessment Procedures: Detailed procedures should be established for conducting security risk assessments of research projects, international partnerships, and personnel. These procedures should include standardised assessment criteria, documentation requirements, and decision-making processes. Regular updates should be incorporated to reflect evolving threat landscapes and regulatory requirements.

Due Diligence Protocols: Comprehensive protocols should be developed for conducting due diligence on international research partners, visiting researchers, and collaborative arrangements. These protocols should include information gathering requirements, assessment criteria, and documentation standards. Procedures should balance thoroughness with efficiency to avoid unnecessary delays in legitimate research activities.

Incident Response Procedures: Clear procedures should be established for responding to security incidents, including detection, assessment, response, and recovery activities. These procedures should include coordination mechanisms with government agencies, communication protocols, and documentation requirements. Regular training and exercises should be conducted to ensure effective incident response capabilities.

Information Sharing Guidelines: Detailed guidelines should be developed for sharing security-related information between institutions, government agencies, and international partners. These guidelines should address legal requirements, privacy protections, and operational procedures for information sharing. Regular review and updates should be conducted to ensure effectiveness and compliance with evolving regulations.

6.3 Training and Awareness Materials

Comprehensive training and awareness materials should also be developed by the coordination platform to support implementation of knowledge security measures across Swiss institutions. These materials should be tailored to different audiences and regularly updated to reflect evolving requirements and best practices.

Executive and Leadership Training: Specialised training programs should be developed for institutional leaders, including university presidents, research administrators, and senior faculty. These programs should focus on strategic aspects of knowledge security, governance requirements, and leadership responsibilities. Case studies and scenario-based exercises should be included to provide practical experience in managing knowledge security challenges.

Compliance Officer Training: Comprehensive training programs should be developed for compliance officers, including initial certification requirements and ongoing professional development activities. Training should cover technical aspects of risk assessment, regulatory compliance, and operational procedures. Regular updates and refresher training should be provided to maintain current knowledge and capabilities.

Researcher and Faculty Awareness: General awareness programs should be developed for researchers and faculty members across all disciplines. These programs should focus on practical aspects of knowledge security, including recognising potential threats, following security procedures, and seeking appropriate guidance. Programs should be designed to integrate with existing professional development activities and should be regularly updated to reflect current threats and requirements.

Administrative Staff Training: Specialised training should be developed for administrative staff who support research activities, including grants management, international programs, and student services. Training should focus on their specific roles in implementing knowledge security measures and should include practical guidance on procedures and requirements.

6.4 Assessment and Evaluation Frameworks

Regular assessment and evaluation of knowledge security implementation is essential for ensuring effectiveness and continuous improvement. Comprehensive frameworks should be developed at the national level to measure program performance and identify areas for enhancement.

Performance Metrics: Quantitative metrics should be established to measure implementation progress and operational effectiveness. These metrics should include number of security assessments completed, personnel trained, incidents detected and resolved, and partnerships evaluated. Regular reporting on these metrics should be provided to stakeholders and decision-makers.

Effectiveness Assessment: Qualitative assessments should be conducted to evaluate the effectiveness of security measures in protecting research assets and maintaining research excellence. These assessments should include surveys of researchers and administrators, case studies of security implementations, and comparative analysis with international best practices.

Continuous Improvement: Regular review processes should be established to identify opportunities for improving knowledge security measures. These processes should include feedback from stakeholders, analysis of operational experience, and incorporation of evolving best practices and threat information. Annual reviews should be conducted with comprehensive assessments every three years.

International Benchmarking: Regular benchmarking against international best practices should be conducted to ensure that Swiss knowledge security measures remain current and effective. This should include participation in international conferences and professional networks, regular consultation with international partners, and incorporation of lessons learned from other countries' experiences.

7. Conclusion

The implementation of enhanced knowledge security measures in Switzerland represents a critical investment in protecting the country's research excellence and national interests. The recommended three-axis approach provides a comprehensive framework that balances security requirements with preservation of academic freedom, openness and research excellence.

Success will depend on strong leadership from higher education institutions and government agencies, adequate resources for implementation, and sustained commitment to the principles of proportionality and transparency. The phased implementation approach allows for systematic development of capabilities while minimising disruption to ongoing research activities.

The international examples analysed in this report demonstrate that effective knowledge security measures can be implemented without compromising research excellence or international collaboration. Switzerland's strong institutional capabilities and commitment to excellence provide a solid foundation for successful implementation of these measures.

Regular assessment and continuous improvement will be essential for maintaining the effectiveness of knowledge security measures in an evolving threat landscape. The frameworks and procedures recommended in this report provide the foundation for a dynamic and adaptive approach to knowledge security that can evolve with changing requirements and emerging challenges.

The investment in knowledge security represents not just a defensive measure but an enabler of continued research excellence and international leadership. By implementing

appropriate safeguards, Switzerland can maintain its position as a global leader in research and innovation while protecting its national interests and research assets for future generations.

swissuniversities

Annex 1: Enhancing Knowledge Security in Switzerland: Initiative factsheets (2025), Manon Hufschmid, SwissCore

SwissCore
Contact Office for European Research Innovation and Education

Enhancing Knowledge Security in Switzerland: Initiative factsheets (2025)

Initiative factsheets accompanying the Report *Enhancing Knowledge Security in Switzerland: Providing a source of inspiration for SwissCore funders and partners (2025)*.

Brussels, July 2025
Author/s: Manon Hufschmid

Introduction

These factsheet accompany the report *Enhancing Knowledge Security in Switzerland: Providing a source of inspiration for SwissCore funders and partners (2025)*. While the Report itself follows a country-by-country approach to identify how knowledge security is addressed and enhanced holistically nationally and regionally, the factsheets aim at providing concrete examples of alternative models and key aspects of popular initiatives, as well as critical thinking questions for reflection. The purpose is to provide concrete guidance and a point of reference on how certain initiatives can be implemented in practice. Six initiatives are presented, and the intention is that the factsheets can be read independently from one another.

Initiative factsheets

Central Advisory Service and/or National Contact Points

Establishing a centralised platform for knowledge security is an integral part of the national strategies of several European countries. Considering that the EU is in the process of establishing the European Centre of Expertise on Research Security, **a centralised platform at a Swiss level could also be considered**. Countries have adopted different models & inspiration can be sought from the alternatives for the Swiss approach. While the report discusses the individual models in-depth, this factsheet highlights common elements & themes.

Model	What	Country
National Contact Point for Knowledge Security	A government-wide initiative that created a national contact point for **advice** on questions related to knowledge security, as well as providing **capacity building support**.	Netherlands
Support function for Responsible internationalisation[1]	It is proposed that the support function is the **national node for responsible internationalisation**, provides **capacity building support**, monitors the current environment, updates & develops the national guidelines, provides, tools & meetings places & handles questions.	Sweden
Advisory service (in close contact with the government)	The Research Collaboration Advice Team (RCAT) **works closely with government institutions**, funding agencies & the academic community to provide **advice**.	UK
Non-governmental advisory service	DAAD Centre for International Academic Cooperation (KIWi) provides **advice** to universities/research institutions, pooling the expertise & knowledge from DAAD`s global network.	Germany
Dedicated website	A **comprehensive webpage** containing all information relevant to knowledge security & responsible internationalisation.	Norway

[1] This support function has not yet been established, but was announced by the Swedish Council for Higher Education, the Swedish Research Council, and the Swedish Governmental Agency for Innovation Systems (Vinnova) in the context of a Government assignment to promote responsible internationalisation in education, research, and innovation collaborations. national-support-function-for-responsible-internationalisation---final-report-2025.pdf

Key functions/aspects of a central function

- Handling questions (advisory).
- Providing an easy-to-navigate website with resources & tools related to knowledge security.
- Updating & developing national guidelines.
- Organising events & providing presentations/webinars/resources.
- Overseeing the knowledge-sharing platform for national institutions.
- Acting as the national node for knowledge security & responsible internationalisation (particularly important for when the European Centre of Expertise on Research Security becomes operational [tentatively mid-2026]).

Critical thinking Qs

- Should the Swiss Competence Centre for Scientific Integrity assume the role of the national support function for knowledge security, or should knowledge security have its own, separate centre/platform?
- What level of resources can be dedicated towards establishing a national platform? (e.g. the Swedish advisory groups state that the national support function should receive 7 million krona (SEK) annually, which should also enable the funding of activities).
- The German Council of Science and Humanities recognises the DAAD's important work, but advocates for the establishment of a national contact centre. A key limitation of the DAAD is that government actors are not involved, limiting the amount of access to specific information and government assessments related to knowledge security. It could thus be considered: which government departments should be mobilised and how will coordination take place?

National Guidelines

While each country approaches knowledge security differently, national guidelines seem to be a **popular & effective measure to raise awareness** & to **guide/support institutions** in enhancing knowledge security at their institution. This factsheet provides an overview of **alternative approaches to guidelines**, and points to consider when creating guidelines suitable for the Swiss context. These points span from the drafting process to the actual content of guidelines.

Model	Country	What	Themes covered
National Knowledge Security Guidelines	Netherlands	Aim at guiding individuals & institutions involved in international cooperation to weigh opportunities against risks, to foster safer international scientific cooperation. The advice & guidance comes in the form of things to consideration & recommendations, rather than questions.	Introduction; core academic values; potential risks; legal framework & regulations; risk assessment; risk management for institutions; managing partnerships with foreign entities; the role of human resources & visitor policies; cyber security; list of resources & contacts.
Guidelines and tools for responsible international knowledge cooperation	Norway	Provide an overview of laws & regulations, policy guidelines, existing reports & resources & guidelines in related areas. Depending on the section, assessments & procedures are then proposed for either the (1) institutions' management & administration; (2) academic environments; & (3) researchers & academic environments. These proposals are written as questions, not statements, enabling the targeted group to reflect & independently decide whether they have adequate measures in place. Guidance is also provided on what to include in partnership agreements.	Introduction; academic values & responsibilities; security management at the institution; employees & students; partnerships & agreements; responsibility & coordination at the national level.
Various recommendations & guidance developed by the knowledge sector	**Germany** Leopoldina & DFG targeting research institutions DAAD KIWi targeting higher education institutions (HEIs)	Germany does not have national guidelines yet, but the science community has already developed their own recommendations & guidelines. Leopoldina & DFG (research institutions) The fairly short Recommendations are split in two: Section A is aimed at individual researchers & Section B at research institutions. DAAD KIWi Compass (HEIs) A digital tool for HEIs to assess international partnerships independently. Through six criteria – aimed at different stakeholder groups involved in internationalisation processes - & accompanying guiding questions, HEIs are supported assessing & weighing specific partnerships.	Leopoldina & DFG Section A urges researchers to reflect on cited ethical principles & to consider them in their work. Section B calls on research institutions to implement proposed regulations – after tailoring them to their specific needs & to implement additional subject-specific self-regulatory measures where necessary. DAAD KIWi Compass The 6 criteria are: (1) security situation; (2) wider political imperatives; (3) constitutional & sociopolitical framework; (4) opportunities & risks of the respective academic system; (5) quality of academic partner institutions; & (6) integration into institutional strategies.

'Trusted Research' (TR): government guidance for specific target groups	UK	Targeted guidance for: academia; senior leaders; countries & conferences; & industry, to support the integrity of the system of international research collaboration. The specific guidelines (in the form of booklets) provide clear & simple advice, sensitising the target group on the issue & the relevancy for that group. It seems that the approach is to raise awareness of knowledge security, explaining how the issue affects the particular group & their work, using this as a basis to encourage them to take action & prevent the associated risks from materialising. Advice is then presented through general explanations &/or things to consider in the form of guiding questions.	For academia: introduction to TR; why protect your research?; who are you at risk from?; what are the risks to your research?; how much of a target are you?; how to protect your research. For senior leaders: designed for leaders to have key issues & questions at hand (e.g., on good governance, identifying most sensitive research, due diligence) For countries & conferences: advice & guidance for academics on some of the main challenges presented when working/travelling overseas. For industry: introduction to TR; understanding risk; how to protect research; protecting people; & supporting partners.

Designing the Guidelines: things to consider

- Common guidelines at national level must be **co-designed** with HEIs, to preserve institutional autonomy & ensure that they promote responsible internationalisation rather than undermining partnerships for being too burdensome.
- A **public consultation** on the draft Guidelines is critical to ensure transparency, appropriateness & inclusivity of all relevant actors in the process.
- They should not be too burdensome & resource-demanding to administer at institutional level.
- Emphasis should be placed on the fact that the Guidelines are there to support internationalisation & open science, not to limit the ability of national institutions to enter into international partnerships & research projects.
- Conducting a **mapping study** to assess the challenges the research & education sector encounter in international partnerships & collaborations.
- Include a section on **legal obligations & responsibilities** relevant to the knowledge sector.
- Other national Guidelines have largely taken a **thematic approach**.
- Having **dedicated sections for STEM & humanities**, as these disciplines experience knowledge security differently.

Critical thinking Qs

- Who should the Guidelines target?
- What themes should be covered by the Guidelines?
- What model should Switzerland follow? Should there be one set of national guidelines (e.g. NL, NOR), or should several guidelines exist targeting different groups (e.g. UK)?
- Who should be responsible for monitoring the implementation of the Guidelines?
- Who should be responsible for updating the Guidelines & how often should this be done?
- Can the existing *Guide Towards responsible international collaboration* (swissuniversities, 2022) support the development of national guidelines?
- Should the Guidelines become integrated into the funding process?
- How can the SECO's work on export controls be integrated or leveraged?
- What tools, if any, should be included in the Guidelines?
- Should an accompanying PowerPoint presentation be created to aid institutions in understanding the Guidelines (e.g. like Norway has done)?
- STEM & the humanities experience knowledge security differently. Should the Guidelines contain guiding questions & recommendations that are broadly discipline-specific?

Institutional level contact points

National strategies frequently include **nominating a point of contact (CPs) at the institutional level**. Some countries have made this a legal requirement, whereas it is voluntary in others. These CPs are often the ones granted **access to closed knowledge-sharing platforms** & **provide guidance** to an institution's academic & research community. Several Swiss institutions already have a focal point for knowledge security & it could be considered how to connect these CPs to share best practices & challenges encountered, as well as how a centralised platform/national CP can support their work.

Model	What	Country	Case Study
Portfolio holder at board level + internal Knowledge Safety Advisory Team	The Guidelines recommend "designating a portfolio holder at board level for the theme of knowledge security", who should be supported by an "internal Knowledge Safety Advisory Team, i.e., a team consisting of several experts with different types of expertise."	Netherlands	TU Delft has established a central university knowledge security advisory team & decentralised knowledge security coordinators. The coordinators act as first-line CPs for faculties & QuTech (i.e., the interfaculty quantum technology research institute).
Committees for Ethics in Security-Relevant Research (KEFs)	KEFs assist researchers & research institutions upon request, by providing **advice** & **evaluating ethical aspects** of security-relevant research projects. KEFs also **promote awareness** of security-relevant aspects of research within the institution & help develop a culture of responsibility. Several research institutions with established committees with different responsibilities have also taken on the task of a KEF. KEFs have an **advisory** function & **do not decide** whether a research project may be carried out.	Germany	At Forschungszentrum Jülich, security-relevant research projects must consult the local KEF, compliance with which is ensured by the 3rd party funding department, among other things. The KEF's evaluation system focuses on the aims of the researchers/partners & the respective technology readiness level. E.g., a proposed research project with a military partner from a 3rd country related to energy research received a negative advisory vote from the KEF. Considering the research centre's peace clause & the project's unclarified publication modalities, there was a risk that the product could be developed & used primarily for military purposes. The **KEF's negative vote is then communicated to the executive board, which ultimately makes the decision in favour/against the project**.
Institution point of contact	Within research institutions, the nominated RCAT CP is responsible for communication with one of the RCAT's country offices.	UK	The University of St Andrews is served by the RCAT Edinburgh office & has appointed an institutional CP for RCAT.
Contact point within the organisation	The Guidelines advise institutions' management & administration to establish a CP within the organisation with clearly assigned **responsibility for research ethics challenges**. The organisation's community should also be able to **report security breaches/pressure** from external actors to this CP.	Norway	

Critical thinking Qs

- What, if any, level of support can we provide to institutions in establishing an institutional CP?
- Can existing positions be leveraged to include the post of knowledge security within the scope of their work?
- How can these institutional CPs be connected with one another? What role could the centralised platform play here?

Embedding knowledge security into the funding process of international partnerships & research projects

Funding organisations have also **embedded knowledge security considerations into their assessment & decision-making processes**. Some funders have opted for creating their **own principles** (e.g. UKRI), whereas others have **integrated national guidelines** into their processes (e.g. NWO). It might thus consider what role national funding organisations can play in enhancing knowledge security.

Funding agency	How knowledge security measures are integrated
UKRI (UK)	UKRI Trusted Research & Innovation Principles establish the UKRI's expectations of UKRI-funded organisations with respect to due diligence for international collaboration. UKRI-funded organisations "should adopt these principles & be able to evidence the controls & measures that have been put in place that are consistent with these principles."
Biotechnology and Biological Sciences Research Council (BBSRC), Medical Research Council (MRC), Wellcome Trust	The three funders released a joint statement in 2016 on managing risks of research misuse. Five provisions have been implemented in the **grant application processes & funding requirements** of the funders, so that risks of misuse associated with proposals are identified & assessed during the grant funding processes.
Dutch Research Council (NWO)	• Efforts to **raise awareness of knowledge security within NWO**: Two advisory teams have been established (one for staff in the funding process & one for the nine NWO institutes). These teams support policy implementation & knowledge building, act as contact points for internal staff for knowledge security-related questions & deal with dilemmas related to knowledge security. • The funding process: **Applicants must commit to the National Guidelines** – this is included in the call for proposals. To preserve institutional autonomy, applicants must confirm, at the time of submission, that their application complies with the Guidelines's requirements. Only where there are clear indications of knowledge security risks will the NWO ask the applicant to demonstrate how compliance with the Guidelines is achieved.

Critical thinking Qs

- If it is decided to integrate knowledge security measures into the funding process, what should the application entail? Should compliance with (yet-to-be established) national guidelines be required, or should Swiss funding agencies develop their own criteria?
- How can the role of funders be leverage without infringing on institutional autonomy? Should applicants already demonstrate in their submission how they are complying with knowledge security measures, or should the submission merely require a commitment that they do so?
- What process should be in place for funding organisations to discuss proposals that carry knowledge security risks with applicants?

Knowledge Security Training

Some organisations have also begun to initiate **knowledge security training modules**. This factsheet highlights some examples, to provide some inspiration on how knowledge security could be enhanced throughout an institution & to foster the necessary mindset & culture shift.

Organisation	What	Target Group
US Government, Presidential Memorandum on US Government-supported R&D national security policy (14 January 2021)	Requires funding agencies to cooperate with organisations receiving federal funding to ensure that these **organisations have policies & processes in place to identify & manage risks to research security & integrity**. The memorandum also requires funding agencies to ensure that Federal agency personnel conducting R&D activities or participating in the process of allocating Federal R&D funding receive research security training.	Funding agencies.
US National Science Foundation	An online research security training (four modules, total 60 min) for the research community to provide information on **risks & threats** to the global research community, as well as the **knowledge & tools to protect** against these risks.	Recipients of federal research funding.
Harvard University	Harvard's Research Security Training forms a vital part of its Research Security Programme.	Covered Individuals (e.g., PIs, Co-PIs, Senior/Key personnel, individuals named as investigators on a Federally Sponsored project at Harvard).
DLR	DLR developed an **e-learning for research security**, which is around 90 minutes long. Anybody can purchase a licence for this e-learning & can customise it.	Individuals who both do research & have institutional-level responsibilities (e.g., university leaders, administrators, project leaders). Students & purely admin staff are not the target group.
UK, NPSA & NCSC	In their *Trusted Research Guidance for Senior Leaders*, **training of both research & corporate staff** is recommended to create a culture of trusted research.	Research & corporate staff.

Critical thinking Qs

- Should higher education institutions (HEIs) embed knowledge security into their degree programmes (e.g. Masters programmes) to foster a culture of awareness? E.g., The University of Bern has integrated sustainability as a cross-cutting issue in all areas of the university.
- Should funding organisations undergo knowledge security training to be able to evaluate & identify funding proposals that may carry certain risks?

Screening frameworks

Due to the resource intensiveness & desire to preserve institutional autonomy & preference for self-regulation, **centralised screening frameworks are not as widespread** among the analysed countries. The subject of screening can differ: (1) the researchers or students; or (2) the project itself. For lack of a national policy on screening, **some Swiss institutions have developed their own framework** (e.g., ETH Zurich). But to avoid national fragmentation & encourage harmonisation of policies, it could be considered whether & how harmonisation should be achieved & what the legislative implications are if screening is conducted, either nationally or at the institutional level.

Critical thinking Qs

- Is there a need for a national screening framework (irrespective of the subject of screening)?
- If there is a need, what should be the subject of screening?
- If there is no need for a centralised mechanism, how can it be ensured that institutional initiatives do not result in fragmentation & potential infringement of Swiss law & values of open science & non-discrimination?

Annex 2: G7 Best Practices for Secure and Open Research (February 2024) and the role of the individual stakeholders

To support the implementation of the common research security principles and research integrity values, the **G7 members developed a list of best practices contributing to secure and open research**. In addition to this, the development of a Virtual Academy was also announced.[1] The best practices draw from existing initiatives and programs in G7 countries and recognise that the protection of research is a shared responsibility amongst all stakeholders.

Notably, the G7 highlights that "[t]he principle of adaptability must underpin the implementation of any research security best practice, recognising that approaches may need to be adapted to account for new and emerging risks, and be proportionate and flexible enough to maintain and support the autonomy of research activities by research institutions and researchers, while preserving research quality."[2] Table 8 contains some examples of identified best practices, and the role of the individual stakeholder, to provide some inspiration.

Best practice	**The role of the individual stakeholder**			
	Governments	**Research funders**	**Research institutions**	**Researchers**
Establish resources to **promote awareness** & **forums for dialogue & information sharing** on research security & integrity across all research stakeholders. Rationale: Research security is a new and evolving topic for many. Enabling knowledge/resource sharing fosters an ecosystem that enables the current and future needs of the research community to be addressed.	Consider establishing a central resource for the research community to obtain information from & build awareness.	Engage with the government & help shape broader policies which relate to research security and integrity. Support the dissemination & promotion of resources to help build awareness.	Identify the needs of the researchers. Train & update staff regularly on areas of potential risk & how to mitigate them. Disseminate resources to build awareness of risk within the research community.	Become empowered to protect their research & general research ecosystem by engaging in awareness raising & information sharing. Contribute to dialogues at all levels to ensure their needs are well communicated & understood, so that they can be addressed by other stakeholders.
Identify & share information on which **research areas are at risk**. Rationale: Promotes a risk-appropriate	Provide information for the research community to fully understand the risks in	Implement research security & integrity requirements in funding applications in a targeted way that focus on high-risk research areas.	Awareness of what research activities are conducted within their institutions in government-	Consider how their work could be appropriated & misused. Use tools provided by

[1] G7, G7 Best Practices for Secure & Open Research, February 2024.
[2] ibid 3.

Best practice	The role of the individual stakeholder			
	Governments	**Research funders**	**Research institutions**	**Researchers**
approach to research security, as it recognises that some areas of research might need lower levels of security compared to others.	certain subject areas. Collaborate with funders, institutions & researchers to ensure that risk-identification is accurate.	Engage with stakeholders to ensure they fully understand a project & its potential risks.	considered sensitive areas. Support researchers in identifying what research is of higher risk (e.g., through information sharing).	governments, funders, or research institutions to conduct due diligence activities.
Identify areas of risk activity by conducting due diligence & ensuring transparency & the disclosure of relevant information. <u>Rationale:</u> Identifying the source of a threat enables effective risk mitigation measures to be drafted.	Take responsibility for the development of policy frameworks which establish due diligence & transparency requirements for research funders, institutions & researchers. Provide guidance to research institutions & researchers on the most current risks to the research community, regularly assessing the threat environment. Review policy frameworks regularly to determine whether these still meet the needs & intended objectives. Monitor any unintended adverse impacts of policy frameworks to ensure that academic freedom is not undermined	Implement policy frameworks established by governments. Funding applications should be used to identify & disclose of relevant potential risks. Applications should enable researchers to disclose risks easily & with full transparency. Weigh risks against the scientific merit & benefits of a proposal. Could require disclosure of information related to potential conflicts of interests & sources of funding in application forms. Monitor unintended adverse impacts of research security requirements (e.g., harassment/discrimination).	Establish capacity to help researchers identify & evaluate risks (e.g., appointing a lead to take responsibility and ensure a uniform approach). Discuss regularly at senior leadership levels reputational, ethical & national security risks related to research projects. Identify & assess institutional-based risks (e.g., both physical and digital infrastructure-based risks). Monitor adverse impacts when implementing research security & integrity initiatives to avoid discrimination or harassment.	Disclose information to their research institutions & funders, as these may have knowledge on emerging risk trends which might be unbeknownst to the researcher. Understand the motivations & interests of partners can support the identification & mitigation of potential risk areas. Understand that research security & integrity measures should not target specific individuals/communities.

Best practice	The role of the individual stakeholder			
	Governments	**Research funders**	**Research institutions**	**Researchers**
	& discrimination & harassment is not encouraged.			
Implement **risk mitigation measures**, both as standard organisational practice & for individual research projects. Rationale: The research community is generally better positioned to address & mitigate against the identified risks.	Provide guidance on risk mitigation (e.g., develop resources & information-sharing mechanisms).	Consider including specific requirements in their application process or implement policies that certain risk mitigation measures are a standard expectation for funding. As recipients of research proposals, funders can identify and develop broad risk mitigation best practices. In collaboration with the government, these can form the basis of guidance & be circulated across the research community.	Implement measures to protect themselves & their researchers. Establish a code of conduct on research security & integrity for its researchers. Establish policies & processes for staff to report concerns to support information sharing, as well as risk identification & mitigation. Provide training on standards for good cyber & physical security practices.	Develop clear risk mitigation plans, ideally with the support of research institutions &/or funders. Establish training & onboarding procedures to ensure that prior to & during the lifecycle of a project, the risks are managed appropriately.

Table 8: G7 best practice examples and the role of the individual stakeholder

Annex 3: Compliance Officer Profile and Specification: Proposal adaptable to each institutional context

The successful implementation of knowledge security measures depends critically on establishing effective compliance officer capabilities across Swiss HE's. The compliance officer profile should define the qualifications, responsibilities, and operational requirements for these positions.

Educational and Professional Qualifications: Compliance officers should possess advanced degrees in relevant fields such as international relations, security studies, law, or technical disciplines related to institutional research focus. Minimum of five years professional experience in areas such as regulatory compliance, risk management, security assessment, or research administration is required.

Preferred qualifications include previous experience in knowledge security, export control compliance, or related fields. Knowledge of Swiss legal and regulatory frameworks is essential, as is familiarity with international research collaboration practices and potential security implications.

Core Competencies: Compliance officers must demonstrate strong analytical capabilities for conducting risk assessments and security evaluations. Excellent communication skills are essential for interacting with researchers, administrators, government officials, and international partners. Project management capabilities are required for coordinating security implementation activities across complex institutional environments.

Technical competencies should include understanding of cybersecurity principles, export control regulations, and technology transfer processes. Knowledge of threat assessment methodologies and security planning approaches is highly desirable.

Operational Responsibilities: Compliance officers are responsible for conducting comprehensive security assessments of research projects, international partnerships, and personnel. This includes developing and implementing due diligence procedures, coordinating with government agencies on security matters, and providing guidance to researchers on security requirements and best practices.

Officers should maintain current knowledge of threat landscapes and security requirements through regular training and professional development activities. They should also participate in professional networks and information sharing mechanisms with other compliance officers and security professionals.

Institutional Integration: Compliance officers should be integrated into institutional governance structures with appropriate authority and access to leadership. They should have regular interaction with research administrators, faculty leadership, and institutional security personnel. Clear reporting relationships and accountability mechanisms should be established to ensure effective performance and institutional integration.