National knowledge security guidelines

Secure international collaboration

July 2026

National knowledge security guidelines

Secure international collaboration

July 2026

NWO

KNAW

Vereniging Hogescholen

umcnl

TQ federatie

Rijksoverheid

Universiteiten van Nederland

Table of contents

Preface 5

Section 1 Introduction 7
- Rationale for these guidelines 8
- What is knowledge security? 9
- Explanation 9
- A common challenge 11
- Role of the central government 11

Section 2 Protecting core academic values 13
- 2.1 Academic freedom 14
- 2.3 Open science 15
- 2.4 Ethics in science 16
- 2.5 Inclusivity and non-discrimination 16

Section 3 Threat assessment 18
- 3.2 Activities aimed at influence and interference 22
- 3.3 Ethical and integrity violations 23

Section 4 Statutory frameworks and guidelines 24
- 4.1 Sanctions and dual-use regulations 25
- 4.3 Knowledge security screening bill 27
- 4.4 Additional codes of conduct, frameworks, models and recommendations 27
- 4.5 Open Government Act 29
- 4.7 General Security Requirements for Central Government Contracts (ABRO) 31

Section 5 Assessing risks 32
- 5.1 Which domains of knowledge within your institution are at increased risk? 33
- 5.2 Which countries represent an increased risk? 34
- 5.3 Know your partners, clients and funding providers 35
- 5.4 What to bear in mind when entering into a collaboration 36
- 5.5 Knowledge security in procurement and tendering 37

Section 6 Risk management 39
- 6.1 Organise risk management within your organisation 40
- 6.4 Measures to improve security 43
- 6.5 Culture of security: awareness and alertness 44

Section 7 Guest researcher policy and human resources policy 46
- 7.1 Knowledge security in recruitment and selection 47
- 7.2 Education and training 49
- 7.3 Risk of stigmatisation and inappropriate behaviour 50
- 7.5 Access by visitors, guest researchers, guest lecturers and external staff 51
- 7.6 Business trips abroad 52
- 7.7 Termination of employment 53

Annex Indicators for Assessing the Knowledge Security Risks of International Collaborations **54**
Preface 55
1. Statutory frameworks 56
2. Affiliations and organisation type 57
3. Discipline and research type 59
4. Dependency and influencing 59
5. Ethics and integrity 60

Sources **62**
Contact details 63

Preface

In January 2022, the National Knowledge Security Guidelines were published to coincide with the opening of the National Contact Point for Knowledge Security. This marked the start of a shared, learning strategy, in which the knowledge sector and the Dutch central government committed to working together to promote knowledge security.

The first version of the guidelines contained points requiring attention, recommendations and guiding principles. The guidelines defined the scope of the knowledge security policy and offered institutions in the knowledge sector guidance to develop their own knowledge security policies. On 4 April 2022, Robbert Dijkgraaf, the Minister for Education, Culture and Science, sent a letter calling on the knowledge sector to implement the guidelines by carrying out a risk assessment, appointing an administrative portfolio holder and setting up an advisory team, among other measures[1].

Since then, both the knowledge institutions and the central government have accumulated a great deal of experience with knowledge security. It is important that the guidelines continue to adequately reflect that experience and the needs of the knowledge institutions. That is why the knowledge sector and the central government have now jointly developed a new version of the guidelines.

As was the case with the previous version, these guidelines focus on the knowledge sector as a whole and are thus useful for a wide target group. The document gives executive boards suggestions to help them develop knowledge security policies and offers advisers, policymakers and scientists practical frameworks to implement that policy in practice.

These new guidelines differ from the previous version in several respects. Out-of-date texts have been updated and information has been clarified or supplemented as necessary. A clearer distinction has been made between information that is intended as a guide and descriptions of stricter frameworks. Some specific details have also been amended. The most important of these are:

- The definition of knowledge security in section 1 is more precise and has been brought into line with the definition in the associated EU Council Recommendation as much as possible.
- Section 2 describes the various relevant core academic values in greater detail. The fact that tensions may arise between knowledge security and other important core academic values is mentioned more explicitly, as is the need to specifically tackle those tensions.
- Section 3 contains an updated and more detailed threat assessment for each of the three elements in the definition of knowledge security.
- Several statutory frameworks that are currently in development have been added to section 4. The relationship between the Open Government Act (*Wet Open Overheid*) and the knowledge security policies of institutions is also explained.

1 https://open.overheid.nl/documenten/ronl-4e8f21a7fb3fc26476104cc45731911138ab359/pdf (in Dutch)

- In this version, section 5 is based on the 'Indicators for Assessing the Knowledge Security Risks of International Collaborations', which were published in the spring of 2025. These indicators have also been included as an annex to these guidelines. The relevant content in section 7 of the previous version has been moved to section 5.
- Section 6 has been expanded to include a summary of what is required to provide executive boards with an accurate factual basis about high-risk foreign collaborations. In addition to the undesirable transfer of technology, section 6 contains a starting point for the implementation of measures to address the other aspects of knowledge security.
- The new section 7 (section 8 in the previous version) describes more relevant aspects of human resources policy, and also more specific aspects of human resources policy that require attention. This section now also makes an explicit distinction between mandatory and supplementary due diligence requirements in the HR policies of institutions.
- Section 9 has been removed. These guidelines describe the importance of cyber security as part of knowledge security elsewhere, but refer to more specialised sources for information about cyber security.

This document has been translated from Dutch to make it accesible for a wide audience.
In the event of any discrepancy or doubt, the Dutch-language version (*Nationale leidraad kennisveiligheid Veilig internationaal samenwerken, juli 2026*) shall prevail.

Section 1

Introduction

Higher education and research cannot take place without international cooperation and scientific talent from all over the world. Dutch knowledge institutions have a good reputation and play a leading role on the global stage. This is due to factors including the academic freedom that is guaranteed in the Netherlands, and largely also the openness of our knowledge institutions. We also owe our prosperity to research collaboration to a large extent.

At the same time, the world around us is changing. Geopolitical power shifts are occurring, with economics, geopolitics and security strongly intertwined. In this context, knowledge and technology are increasingly seen as a strategic instrument of power that can be used alongside or in combination with traditional means such as espionage. This means these developments affect everyone who works in the Dutch knowledge sector. We are collectively responsible for safeguarding our knowledge security as effectively as possible.

Rationale for these guidelines

We are pleased to present the Knowledge Security Guidelines developed by the knowledge sector and the central government. This document serves as a guide for all those at universities of applied sciences, universities, university medical centres, applied research (TO2) organisations, Royal Netherlands Academy of Arts and Sciences (KNAW) and Dutch Research Council (NWO) institutions whose work involves knowledge security and weighing up the opportunities and (security) risks of international collaborations. Although the primary focus is the executive boards of knowledge institutions, these guidelines can also help others, including (knowledge) security coordinators, project managers and individual researchers and lecturers.

Although Dutch knowledge institutions differ in the nature, structure and scale of their educational and research activities, they all possess and develop valuable and sometimes sensitive knowledge and technology. They are also all committed to international scientific collaboration, academic freedom and open education and science.

Knowledge institutions themselves are responsible for the structure and implementation of their knowledge security policies. They have a great deal of freedom to do so as they see fit. This means knowledge institutions, taking into account relevant frameworks and criteria, can develop their own knowledge security policies to reflect their specific nature and structure.

As such, these guidelines are not intended as a mandatory regulatory and enforcement framework. They help knowledge institutions fulfil their responsibilities as regards knowledge security. This is why, in addition to context and policy frameworks for the various topics, these guidelines also offer general guidance and practical suggestions.

It must be possible for international collaboration in higher education and research to take place **securely**. That is the overarching objective of knowledge security policies at both the national level and at the level of individual institutions. The objective is to arrive at a good balance between opportunities and risks, with respect and consideration for core academic values. A proportional and tailored approach is essential when implementing protective measures. The basic principle behind knowledge security is ‘as open as possible, as protected as necessary’. It is therefore important to emphasise that these guidelines should not be interpreted as a call to avoid all risks.

What is knowledge security?

Knowledge security means anticipating and managing risks related to:

a) the undesirable transfer of sensitive knowledge and technology that may affect national security and/or the scientific position of institutions.
b) malicious influence on research and education, through which knowledge can be used by or from other countries and state actors to spread disinformation or encourage self-censorship among students and researchers etc., and thus to adversely affect academic freedom and the integrity of research and education in the Netherlands.
c) violations of ethical or integrity standards, in which knowledge and technology is used by state actors to violate or undermine Dutch and European values and applicable treaties.

Explanation

The above categories are based on the description of the term *research security* in the EU Council Recommendation on research security.[2] These guidelines use the nationally more common (but comparable) term *knowledge security*. Several of the terms in the definition are clarified below:

Academic freedom and research integrity

Safeguarding free and open scientific practice is the core of knowledge security policy. Secure international collaboration is a key aspect of this. The essential core values of free and open science are international collaboration, academic freedom and research integrity. These apply to all Dutch knowledge institutions, regardless of their type, nature or structure, and regardless of whether they are engaged in academic, scientific, clinical or applied research.

Knowledge security risks can undermine these core values and can arise in the course of many different types of international scientific collaboration. These include not just collaboration with foreign institutions, but also exchange programmes for students and researchers, collaborations with foreign companies, hosting guest researchers and guest lecturers and hiring and appointing individuals affiliated with foreign institutions. To safeguard free and open science, it is important to manage the knowledge security risks. Section 2 'Protecting core academic values' addresses this topic in detail.

National security

National security concerns the protection of the security interests of the Netherlands[3]. The Security Strategy for the Kingdom of the Netherlands identifies six security interests that affect national security:

1. Territorial security
2. Physical security
3. Economic security
4. Ecological security
5. Social and political stability
6. International rule of law and stability

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510

3 The Security Strategy for the Kingdom of the Netherlands: https://www.government.nl/documents/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands

These security interests may also be threatened in the context of knowledge security, for example if knowledge transfer contributes to the military capacities of a potentially hostile state actor, or if it threatens the continuity of vital processes[4].

State actors

The objective of knowledge security is to protect education and science against threats from state actors. State actors are individuals or (government) organisations that act for or on behalf of a nation state. In this case, this means state actors that represent a threat to national security, as described in the annual State Actor Threat Assessment (DBSA)[5]. Protecting knowledge security also involves dealing with state actors with a poor track record as regards human rights, academic freedom and democracy.

Various state actors are actively seeking knowledge and technology in the Netherlands with the intention of increasing their own military, technological, political and economic power and capabilities. State actors may also engage in activities aimed at influencing and interfering with the work of knowledge institutions. For example, a state actor may use these activities to influence scientific research or censor publications in ways that misuse the openness of Dutch knowledge institutions and the academic freedom guaranteed in the Netherlands. Such activities are not always easy to recognise. There is often a sliding scale, and it is not always easy to distinguish between illegal activities, covert intentions and legitimate collaboration. Section 3 'Threat assessment' describes the threats from state actors in detail.

Examples of high-risk situations

Three illustrative example situations in which knowledge security risks may arise are given here. While these cases are fictitious, institutions and employees may be confronted with similar cases. These guidelines contain suggestions for dealing with such situations.

Risk of undesirable knowledge transfer

Dutch knowledge institutions regularly set up long-term research projects with foreign knowledge institutions. Such collaborations are very common. However, a partner may have links with a state actor that threatens the (knowledge) security of the Netherlands. The agreements concluded before such collaborations commence do not always contain specific details about the research to be carried out or how the results will be used, while it is in fact very important that agreements are made about these issues. After all, the acquired knowledge or the end result of the research may have military applications, including for (un)conventional weapons programmes. Even if the research does not focus on military applications in general terms, risks may still arise.

Other aspects of collaborations may also create risks. For example, the way that research is funded may create undesirable dependencies. Risks may also arise as a result of visits to one another's institutions, for example to use high-tech scientific research instruments.

4 Summary of vital processes: https://english.nctv.nl/topics/c/critical-infrastructure-protection

5 https://english.aivd.nl/documents/2025/09/26/threat-assessment-of-state-actors-2025 (in Dutch)

Risk of covert influence

Knowledge institutions regularly host guest lecturers and guest researchers who may be affiliated with state actors that represent a risk to knowledge security. These state actors may have an interest in ensuring that the research follows a particular course or is interpreted in a particular way, and may attempt to influence their own researchers. For example, the research or education may involve an ideology that is strongly associated with a state actor, or may involve topics that are related to international tensions and criticism. The risk is even greater if the institution with which the guest lecturer or guest researcher is affiliated is funded by the same state actor.

Ethical issues

Ethical aspects may threaten knowledge security. Imagine, for example, that a Dutch knowledge institution conducts research into security in relation to the secure design and surveillance of public spaces in collaboration with international partners. Those international partners may have links to state actors with a poor track record as regards human rights, academic freedom and democracy. This creates the risk that knowledge and skills developed during the research may be used, for example, for (mass) surveillance programmes or to repress specific population groups.

A common challenge

It is of great importance that we achieve a structural increase in awareness of security and resilience against the knowledge security risks faced by Dutch universities, universities of applied sciences and research institutes. This task must be approached based on the institutional autonomy of these knowledge institutions. As such, self-regulation plays a key role. This means that, within the boundaries of the statutory frameworks, the knowledge sector itself monitors security risks, formulates its own strategy and develops its own instruments to invest as actively as possible in the resilience of knowledge institutions.

Various organisations, including the Association of Universities of Applied Sciences (VH), Universities of the Netherlands (UNL), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Dutch Research Council (NWO), the Netherlands Federation of University Medical Centres (UMCNL) and the Federation of Applied Research Organisations (TO2 Federation), can act as initiators and facilitators in this regard, through efforts such as bringing institutions into dialogue with each other and identifying and exchanging best practices. For example, UNL, NWO, KNAW, UMCNL and the TO2 Federation have their own knowledge security working groups.

Role of the central government

Protecting national security is one of the core duties of the government. As such, the central government has an active role to play. The central government works in partnership with the knowledge sector to develop practical frameworks for action. These help knowledge institutions fulfil the responsibility that arises from their institutional autonomy, which is statutorily guaranteed in the Netherlands. The central government informs, contributes ideas, facilitates and advises. However, where necessary for the purposes of national security, the central government also establishes frameworks and monitors compliance with these frameworks.

The various branches of the government have adopted a ‘whole of government approach’ to knowledge security. This means the government as a whole strives to promote coherent and compatible objectives.

Knowledge institutions depend on services provided by the central government for various aspects of their knowledge security policies. As far as is reasonably possible, knowledge institutions must be given the tools they need to successfully fulfil their responsibilities. They must be able to have confidence in the timeliness and accuracy of recommendations, instructions and essential information.

In the international context, the central government strives to create a level scientific playing field, in which allied countries implement comparable knowledge security policies so that Dutch knowledge institutions are not priced out of the market.

National Contact Point for Knowledge Security

A National Contact Point for Knowledge Security has been established to ensure that knowledge institutions have access to a single point of contact for questions about knowledge security. All relevant central government departments are affiliated with this service. This allows the broad expertise of the ministries and services to be accessed from a central location by everyone at knowledge institutions who is involved in international collaboration and who encounters dilemmas. The contact point issues information and recommendations, which institutions can use when weighing up opportunities against risks.

These guidelines are an example of the collaboration between the knowledge sector and the central government to strengthen security awareness. They are a joint initiative of the Dutch knowledge sector (KNAW, NWO, UNL, VH, UMCNL and the TO2 Federation) and various branches of the central government (the Ministry of Education, Culture and Science (OCW), the Ministry of Economic Affairs and Climate (EZK), the National Coordinator for Security and Counterterrorism (NCTV), the Ministry of Foreign Affairs (BZ), the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD). This broad collaborative effort reflects the fact that knowledge security is a challenge for which we all bear responsibility at the national level.

The threat assessment is continually changing, and increasing attention is being devoted to the associated risks. New policies are being developed both nationally and internationally. These guidelines are explicitly intended as a living document that can serve as a basis for discussions with peers and experts. It will be updated in response to new experiences and insights.

Section 2

Protecting core academic values

Academic freedom, research integrity and openness are important core academic values. Together with striving to work in an inclusive, non-discriminatory and generally ethical manner, these core values serve as the foundation for the actions of knowledge institutions.

The objective of knowledge security policies is to protect these core values against threats from state actors. However, measures to promote security may adversely affect these values. A conscious and careful balancing of interests is required to mitigate these negative effects as much as possible. This section addresses the core academic values and the sometimes complex relationship between these values and knowledge security.

2.1 Academic freedom

Academic freedom constitutes the foundation for higher education and science in the Netherlands. Research in the Netherlands must be conducted in accordance with nationally and internationally accepted standards of academic performance. Respect for these core values is a prerequisite for full participation in the academic community.

What does academic freedom mean?

Academic freedom is the principle that staff members at academic institutions are free to conduct their scientific research, disseminate their findings and teach as they see fit[6]. This freedom extends to aspects including:

- the choice of topics to be studied.
- the choice and application of research questions and methods.
- access to sources of information.
- the publication and sharing of information through conferences, lectures and membership of academic groups.
- the choice to enter into collaborations with academic partners.
- the provision of academic higher education.

Academic freedom is essential for the pursuit of science and is statutorily safeguarded by Article 1.6 of the Higher Education and Research Act (WHW) and Article 13 of the EU Charter. In addition, academic freedom is inextricably linked with the professional standards and values described in the Netherlands Code of Conduct for Research Integrity. Academic freedom does not exist in isolation; it is embedded in the wider responsibilities of institutions and the government, including the responsibility to protect national security. Institutional boards may conclude that certain collaborations represent an excessive risk to academic freedom. In exceptional cases, the government may also impose restrictions if there are risks to national security. There must be a statutory framework for such restrictions, which must serve a legitimate purpose.

6 Royal Netherlands Academy of Arts and Sciences (KNAW) 'Academic freedom in the Netherlands: a conceptual analysis and guide' https://storage.knaw.nl/2022-05/20210217-summary-webversie-advies-Academische-vrijheid.pdf (Summary in English, full report in Dutch)

2.2 Codes of conduct for research integrity

The Dutch knowledge sector has committed to national and international codes of conduct for research integrity. These codes serve as guiding principles for education and research in the Netherlands, including activities with foreign parties.

They provide guidance when entering into international partnerships or research projects, e.g. when drawing up a collaboration contract with an international partner (see section 5). (Guest) lecturers and researchers must also endorse and comply with these codes, regardless of where they come from.

Netherlands Code of Conduct for Research Integrity

The Netherlands Code of Conduct for Research Integrity was developed by the knowledge sector (KNAW, UMCNL, NWO, TO2 Federation, VH and UNL). The code sets out the five principles that form the foundation for research integrity (honesty, diligence, transparency, independence and responsibility), which are elaborated into 61 standards of good research practice. The code also contains guidelines for addressing alleged violations of research integrity.[7]
The Code of Conduct states that research integrity is related to knowledge security. Knowledge security can affect the integrity of research, and vice versa.

European Code of Conduct for Research Integrity

There is also a European code of conduct: the *European Code of Conduct for Research Integrity*. It was developed by the European Federation of Academies of Sciences and Humanities (ALLEA), in which the Netherlands is represented by the Royal Netherlands Academy of Arts and Sciences (KNAW). The European Commission recognises this code as the reference document for research integrity for all EU-funded research projects and as a model for organisations and researchers throughout Europe.

Various knowledge institutions have their own codes of conduct, in which their internal research integrity and/or security rules are set out in greater detail. For example, the University Medical Centres have 'research codes'.

2.3 Open science

The Netherlands endorses the European objective of making the results of publicly funded research accessible to all. This includes providing open access to publications and ensuring that research data are 'FAIR' (Findable, Accessible, Interoperable and Reusable). The free sharing of new insights is an important principle of scientific practice and an important driver of the development of new knowledge and innovations.

Within the European Union, it has been agreed that open science should become the standard in scientific research. This does not mean, however, that all international partners also practice open science. Moreover, there may be legitimate reasons to protect some research results and to make them public only in part, if at all. Examples include privacy, national security, intellectual property and commercial interests.

---

7 This version of the guidelines refers to the 2018 version of the Code of Conduct for Research Integrity. The Code of Conduct was being rewritten at the time of writing. When using these guidelines, it is advisable to consult the most recent version of the Code of Conduct.

It is important to identify whether there are restrictions on the level of openness of research at the institution and to identify which agreements about these restrictions can be made with your international partners. For example, agreements can be made about the extent to which data is to be shared or only viewed (known as 'data visiting').

Sharing research data can create dilemmas. For example, subsidy providers may insist that research results are published in accordance with the principles of open science, while subsidy recipients may in fact identify risks to knowledge security. To ensure that this does not discourage institutions from submitting applications, it is important that subsidy providers discuss the conditions required for responsible, secure publication with applicants at an early stage. Making proportional and effective agreements about these aspects in advance can ensure that tensions do not arise later in the process between the desire for maximum openness and legitimate reasons for implementing protective measures.

2.4 Ethics in science

The role of ethics in the national knowledge security strategy is limited to the risks that are directly related to the use of the associated knowledge and technology.

Other ethical dilemmas unrelated to knowledge security may also play a role in international collaborations.

It is important to be, and remain, alert to this possibility at all levels of the institution, both when entering into and during the course of collaborations. It is advisable to set up structures to discuss ethical issues within your institution, so that researchers can report and discuss complex ethical questions concerning international collaborations. The Minister for Education, Culture and Science has asked the universities and universities of applied sciences to follow a number of principles when considering ethical issues; see the Letter to Parliament sent to the Dutch House of Representatives in May 2024 for more information.[8]

2.5 Inclusivity and non-discrimination

Dutch knowledge institutions are responsible for maintaining an inclusive, safe and secure learning and working environment for students and staff. They must guarantee their staff a safe working environment, regardless of their position. There is no place for discrimination at Dutch knowledge institutions[9]. The government is preparing legislation to promote safety and security in further and higher education and research (secondary vocational education, higher professional education and university education). The new legislation will make the responsibility that institutions have to protect (social) safety more explicit, and also their obligation to develop appropriate policies with a learning cycle. Several obligations that support these objectives will also be imposed, including the obligation to monitor perceptions of safety and security and to record incidents. The objective of this policy is to ensure that attention is continually paid to creating a safe and secure learning and working environment and actively engaging in dialogue about this, for example with participation councils.

---

8 Annex to Letter to Parliament on the current situation with regard to security at universities and universities of applied sciences following the protests on the situation in Gaza (31 May 2024).

9 Article 1 of the Constitution of the Netherlands.

Duty of care at knowledge institutions

The Netherlands Code of Conduct for Research Integrity describes the duty of care for researchers as follows: 'Institutions provide a working environment that promotes and safeguards good research practices. They ensure that researchers can work in a safe, inclusive and open environment where they feel responsible and accountable, can share concerns about dilemmas and can discuss mistakes without fearing the consequences ("blame-free reporting")'. The duties of care relate to training and supervision, research culture, data management, publication and dissemination, as well as ethical standards and procedures'.[10]

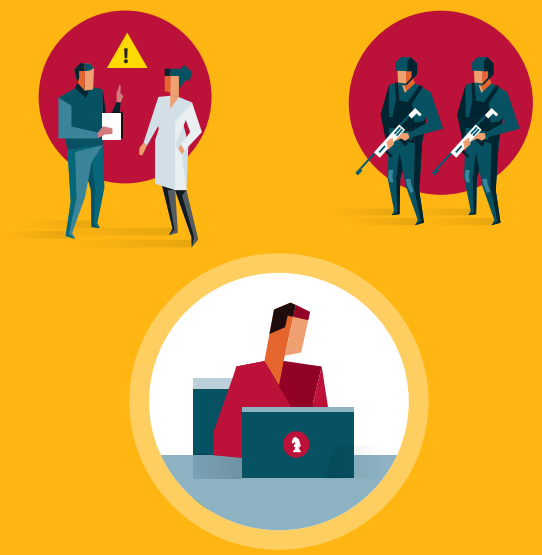
The development of knowledge security policy and communications about knowledge security often involve threat assessments and risk profiles that mention specific countries as potential sources of threats. The danger is that addressing knowledge security risks may lead to prejudice, stigmatisation and discrimination. This must be avoided at all times, and demands alertness and awareness. All measures must be objective, proportional and must address an actual risk. It is important to engage in an open discussion about this within your institution and to take any and all signs seriously. See also the National Action Plan for Greater Diversity and Inclusion.[11]

10 This version of the guidelines refers to the 2018 version of the Code of Conduct for Research Integrity. The Code of Conduct was being rewritten at the time of writing. When using these guidelines, it is advisable to consult the most recent version of the Code of Conduct.

11 The National Action Plan for Greater Diversity and Inclusion in Education and Research will conclude in late 2026. A follow-up is currently being developed.

Section 3

Threat assessment



Dutch knowledge institutions may become the target of attempts to acquire sensitive knowledge and technology.

Various state actors are actively seeking knowledge and technology with the intention of increasing their own military, technological, political and economic power, including in the Netherlands. This threatens the national security of the Netherlands, for example because those state actors may later use the sensitive knowledge that has been transferred for purposes that directly threaten our national security (e.g. in the form of military end uses) or that conflict with our core values.

A state actor may also use Dutch knowledge institutions and open science as a vehicle to acquire such sensitive knowledge and technology.

In some countries, science is increasingly being made to serve the strategic (military) interests of the state. Academic institutions and individual scientists in these countries collaborate (voluntarily or involuntarily) with state programmes and are subject to numerous obligations. These may adversely affect core academic values, including academic freedom, openness and reciprocity. Collaboration with individuals or institutions with links to such countries leads to risks, particularly if their interests conflict with our national security interests.

Even if our national security is not seriously affected in the short term, undesirable knowledge and technology transfer will eventually affect the knowledge position and innovative capacity of the Netherlands, for example because institutions lose their key positions in strategic development processes. If the Netherlands becomes dependent on other countries for access to knowledge, research infrastructure and technological goods and services, this will have an adverse effect on science.

As well as acquiring knowledge and technology, state actors are also involved in influencing and interfering with knowledge institutions. For example, an actor may try to influence opinions and publications, or may attempt to censor scientific research and research results.

Finally, there is a risk that knowledge, technology or the symbolic value of scientific collaboration itself may be misused by state actors for purposes that violate or undermine Dutch and European values and applicable treaties.

To arrive at a broader picture of the existing threats and to raise awareness, this section presents the current threat assessment. Not all threats can be clearly identified by knowledge institutions themselves. For example, clandestine influence is often difficult to detect. As such, some threats cannot be directly addressed with knowledge security policy, or they may not be covered by a strict interpretation of the definition. This does not diminish the fact that information from the threat assessment presented below may contribute to raising awareness and implementing risk assessments at institutions.

3.1 Acquisition of knowledge and technology

State actors may use open academic collaboration to acquire strategic knowledge that can be used for both civilian and military purposes. They may use grants and talent programmes to create financial incentives and dependencies. For example, students and scientists may be given incentives to acquire certain knowledge abroad, and later forced to use that knowledge for the benefit of the state actor. Some countries also impose statutory restrictions on scientists, which they are obliged to adhere to while collaborating with Dutch knowledge institutions.

Association with strategic state (military) programmes

In some cases, foreign knowledge institutions, students and scientists are affiliated with strategic state (military) programmes in their home countries. This is particularly common in countries such as China, Iran and Russia, where research institutions are more commonly part of the military-industrial complex or where the state exerts an above-average influence. See also the most recent version of the State Actor Threat Assessment (DBSA) for more information. Sometimes knowledge institutions are even directly controlled by the government or armed forces.

The connections between a partner and a state actor are not always easily identifiable. Knowledge institutions, foundations or companies may be part of a network that also includes state-controlled entities. In such cases, there is also a risk that sensitive information may reach an undesirable state end user, for example for the development of the military, to improve the effectiveness of digital attacks or for use in mass surveillance. There may also be structural links between individual students or researchers and high-risk entities in countries of concern. These links are not always immediately visible on a CV. In such cases, a direct link with strategic state (military) programmes is more difficult to establish.

Legislation and regulations

Some state actors have introduced national legislation and regulations that oblige citizens, organisations and companies to collaborate with national intelligence and security services. A collaboration with a knowledge institution may allow the state actor to lay claim to research results or intellectual property. In such cases, research results or data from research initiated and/or funded by a Dutch knowledge institution may be copied by a state actor, for example because use is made of shared laboratories or other shared (physical/digital) research facilities. If this occurs, the Dutch knowledge institution cannot always rely on statutory protections, particularly in the case of collaborations with a state/state-controlled partner.

Grants and talent programmes

State actors may use grant programmes to direct students and researchers towards strategically relevant research and educational positions. By imposing conditions on these programmes, the state actor creates a dependency that can be used to oblige the recipient to perform some service in return. For example, they may be forced to report the research results to the state actor or to take on a particular position after the research concludes. In such cases, they may be assigned to defence-aligned entities and thus be obliged to contribute to the realisation of the military-technological ambitions of the state actor. Scientists are not always aware of the interest shown by a state actor. The obligation to perform a service in return for the funding may be seen as a standard condition, or the individual may simply be unaware that the research is relevant for a strategic state (military) programme.

3.1.1. Acquisition through recruited individuals (insider risk)

There are various ways in which state actors attempt to recruit students, scientists and other relevant individuals for the purposes of (facilitating) knowledge and technology acquisition. This may be done in semi-open and semi-legal ways, such as talent recruitment.This may also take place through intimidation or by engaging in status-raising or flattering actions to recruit someone to carry out acts on behalf of the actor.

Talent recruitment

State actors recruit and facilitate talented students and scientists to study or work in their countries. While talent recruitment is a normal phenomenon in science, it may also be a threat, for example if there are unclear conditions or if countries of concern recruit talented individuals for research that may be used for strategic (military) projects. In countries such as China, Iran and Russia, certain research institutions are closely linked with the military-industrial complex or are subject to excessive state influence. This situation creates risks. During or after collaborations with the Netherlands, scientists may eventually be assigned to defence-aligned entities and may unintentionally contribute to the realisation of the military-technological ambitions of the state actor.

Student, trade and professional associations in the Netherlands may also play a role in facilitating talent recruitment. For example, associations may organise events such as conferences, lectures or competitions to recruit talent, sometimes specifically focused on individuals from the recruiting country. The offer to work abroad can be made attractive by providing grants and establishing favourable research facilities (e.g. with large, specialised centres of innovation). It is not always made clear that participants will work for a state-controlled project.

Directed recruitment

Once recruited, individuals can be deployed for a wide range of objectives. Sometimes they help to identify who does what at a knowledge institution, sometimes they are incited to direct individuals for (the facilitation of) illegal knowledge and technology acquisition. Individuals in strategic positions at Dutch knowledge institutions can be valuable targets for state actors, either because of their own knowledge or because of their access to knowledge, technology or laboratories. Potential targets include professors, (senior) lecturers, post-docs, PhD candidates, students and staff members. To recruit these individuals, state actors employ methods including social engineering, financial compensation, blackmail, intimidation or by engaging in status-raising or flattering actions to make them feel important, so that a reciprocal service can be demanded. Recruits are certainly not always aware that they are working for a state actor, and do not always do so voluntarily. Sometimes they may not be aware that they are dealing with a party with links to a state actor. Recruitment can also be very gradual. The target may be slowly ‘reeled in’, sometimes over an extended period, until there is no way back.

Various state actors are known to be willing to intimidate or force (current or former) compatriots who have emigrated to cooperate with the interests of the state. Some state actors (such as China) have introduced legislation and regulations that oblige citizens, organisations and companies to cooperate with national intelligence and security services. Scientists from countries of concern may also be vulnerable to pressure from their home country because they often have financial or personal interests there. In practice, state actors have proven to be willing to put relatives of the victim who still live in the home country under pressure to force their cooperation. If compulsory military service must still be performed in the home country, this may also be used to apply pressure to enforce cooperation with the state. It must be emphasised that not all scientists from countries of concern are potential targets. As described in the previous paragraph,

anyone who is strategically positioned and who is involved with, or who has access to, sensitive knowledge and technology is a potential target for recruitment by a state actor.

Knowledge acquisition using cyber tools

Like all other potential targets who possess valuable digitised knowledge and information, students, researchers and staff members of knowledge institutions can become targets for digital espionage activities by state actors. Intelligence and security services have identified that several state actors have offensive cyber programmes directed against Dutch interests. Some state actors are conducting extensive and structural espionage campaigns aimed at obtaining high-level knowledge and technology. This includes targeting specific researchers and staff members of knowledge institutions with access to relevant knowledge. For example, phishing (or spear-phishing) attacks aimed at specific targets can be used to gain access to systems and files. The risk can also come from the inside. Recruited individuals may play a facilitating role in cyber attacks, for example by giving a 'cyber actor' access to a network. Human-supported cyber attacks of this nature are even more dangerous if there is no network segmentation and users can obtain access to sensitive research data through an innocuous route.

3.2 Activities aimed at influence and interference

Some state actors use resources to influence how they are seen, understood or portrayed internationally. They may also attempt to seek global legitimacy for their policies. Students, researchers and staff members of Dutch knowledge institutions may become the targets of such attempts at interference. Institutes where research is conducted on topics that are objectionable to a state actor, or that a state actor fears will result in the publication of objectionable findings, are particularly at risk.

Such influence may be exerted in various ways. For example, an actor may attempt to influence opinions and publications or to censor scientific research and research results. An actor may also deploy financial resources, either as an incentive or as a means of applying pressure. Some actors also keep an eye on whether their compatriots at Dutch knowledge institutions voice dissident or objectionable opinions about their homeland (e.g. at lectures or conferences).

The pressure that state actors apply can cause staff members of Dutch knowledge institutions to feel unsafe, or may lead to mutual mistrust and self-censorship. There have been cases in which students were afraid of being reported to their country of origin by their peers. Even the idea that their home country can monitor them can cause some students, researchers, lecturers and staff members to feel unsafe. This can lead to self-censorship, the erosion of social safety and the undermining of core academic values. It can also have major consequences for the general well-being of victims. Such activities aimed at interference also represent a threat to fundamental freedoms and research integrity.

These activities can sometimes occur in unexpected places. For example, international student associations can be used as instruments of repression and to monitor critical diaspora and fellow students.

Activities aimed at interference do not always involve repression. Scientific experts may be attractive as credible mouthpieces for state actors. By virtue of their expertise, they can be enticed to express views that are in line with the actor's interests. For example, they may be invited to write articles in certain foreign media or to speak at symposia.

3.3 Ethical and integrity violations

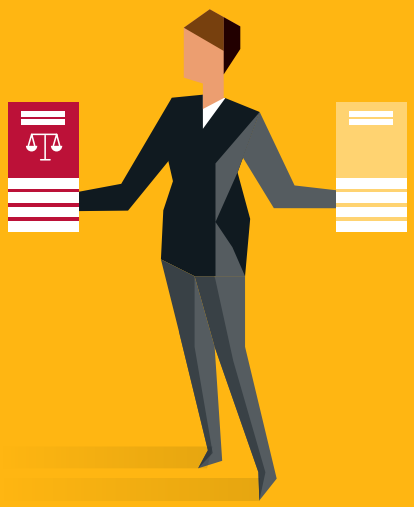
There is a risk that international academic collaboration may lead to the violation of fundamental (academic) values and treaties in the Netherlands and beyond. These may include the protection of human rights and of the climate and environment, principles of the rule of law and other democratic values, diversity and inclusion, the protection of (cultural) heritage, the position of minority groups and cultural pluralism.

Knowledge and technology developed during the collaboration can be used by partners and affiliated (state) actors, either intentionally or unintentionally, for purposes and interests that violate these fundamental values or treaties. This is not only problematic for those directly affected; it also weakens the status and authority in general terms, and thus also the protective effect, of these values and treaties.

The risk of becoming involved with or contributing to ethical and integrity violations is greater in the case of collaborations with partners in countries with a weaker rule of law, or with a poor track record as regards human rights, academic freedom and democracy. See also the list of sources in section 5.2 for more information.

Section 4

Statutory frameworks and guidelines



There are both national and international statutory frameworks and guidelines that contribute to the security of the Netherlands. All institutions are required to comply with legislation and regulations, which constitute the 'hard' frameworks within which collaboration with international partners must take place.

This section addresses statutory obligations, such as export controls and sanctions regimes, as well as legislation that is currently in preparation. It also devotes attention to the various codes of conduct that have been developed in the knowledge sector. These codes serve as guiding principles and can contribute to decision-making.

4.1 Sanctions and dual-use regulations

Two of the most important statutory systems that knowledge institutions must take account of are sanctions regulations and dual-use regulations. While the purpose of these regulations includes monitoring undesirable knowledge and technology transfer, they differ fundamentally from knowledge security policy. They do however exist in the same context, and in practice the same individuals and support departments are often responsible for compliance.

Compliance with sanctions regulations and dual-use regulations is a separate responsibility, in which the regulations themselves always serve as the guiding legal principle. As such, these guidelines do not cover this responsibility, although several key principles are explained below to provide some insight into the various tasks and obligations that these regulations impose on knowledge institutions.

Both sanctions regulations and dual-use regulations are imposed internationally, either by the EU or by the UN. They also apply directly to scientists and knowledge institutions. In principle, scientists and knowledge institutions themselves are also responsible for compliance with these regulations.

Sanctions regulations

Sanctions are primarily intended to change the behaviour of the government of a particular country. Sanctions regulations apply to specific goods, services, knowledge and technology, and to individuals and other entities within a specific country. Each sanctioned country is covered by a specific regulation, which includes specific prohibitions and exceptions. The *EU Sanctions Map*[12] contains an up-to-date overview of applicable sanctions regulations. The exact details of what is sanctioned can generally be found in the annexes to the relevant regulation.

Sanctions may also apply to specific individuals and organisations. It is important to check this before hiring or inviting individuals or entering into collaborations.

Dual-use regulation

The dual-use regulation is primarily intended to ensure that European countries do not contribute to the production and development of weapons of mass destruction or military aggression anywhere in the world. The dual-use regulation is based on a list of goods and technology. Anyone who wishes to export items on this list to countries outside the EU must request a permit.

12 https://www.sanctionsmap.eu/#/main

The goods and technologies for which a permit must be requested are listed in annexes I and IV to the EU dual-use regulation (2021/821).

Technical assistance

Technical assistance is an important element of the prohibitions and permit obligations imposed by both sanctions regulations and the dual-use regulation. This means that supplying something that contributes to the installation, use, repair or maintenance of goods or technologies subject to sanctions may be prohibited or may require a permit.

Technical assistance is a broad term. It includes instructions, advice, training, transfer of practical knowledge, skills and advisory services, including verbally. This may occur in many places throughout the knowledge sector: when appointing members of staff, sharing research methods and results, educating students, during staff exchanges and when organising and attending conferences etc. As such, knowledge institutions must devote particular attention to the provision of technical assistance that is prohibited or for which a permit is required.

Verscherpt Toezicht

Verscherpt Toezicht applies to a small number of sanctioned technologies, specifically the risk of supplying technical assistance to North Korea, Iran, Belarus and Russia. A knowledge embargo exemption must be requested for students and researchers who wish to engage in particular studies or activities. For whom and for which studies and activities this is required can be found on the website of the Knowledge Embargo Contact Point[13], where you can also read how to apply for an exemption.

Regulations of non-European countries

Countries outside Europe enforce their own export control rules. It is important to note that the export control rules of the United States apply extraterritorially. This means the American export control rules apply not just to goods and services that were developed or produced in the US, but also to goods and services that include American components, software or technology. This regulation also applies if such goods and services were developed outside the US.

Further information

If you have any questions about applicable sanctions regimes, please contact the National Contact Point for Knowledge Security. Be aware that the contact point cannot investigate individuals. Due to the criminal law aspects of sanctions regulations, it is also not possible to test specific cases against sanctions regulations and to provide definitive answers. If you wish to know whether a permit is required for something or whether it is covered by a sanctions regulation, you may submit a request for classification to the Central Import and Output Office (CDIU) at the Ministry of Foreign Affairs[14].

13 https://www.government.nl/faq/secondary-vocational-education-mbo-and-tertiary-higher-education/do-i-need-an-exemption-from-the-knowledge-embargo

14 https://www.douane.nl/kennisbank/documenten/aanvraag-indelingsverzoek/

4.2 Investments, Mergers and Acquisitions Security Screening Act (Wet Vifo)

State actors can also acquire sensitive knowledge through foreign investments, mergers or acquisitions that involve Dutch companies. To prevent risks to

national security, the Investments, Mergers and Acquisitions Security Screening Act (Wet Vifo) came into force in 2023. The legislation focuses on vital suppliers and companies that have access to sensitive technology[15].

Knowledge institutions may need to take account of this legislation while performing their research and teaching tasks, for example if they have a stake in start-ups operated by current or former students or staff members. Investments in, mergers with or acquisitions of these companies may fall within the scope of the security assessment.

4.3 Knowledge security screening bill

For disciplines in which the risks to national security are greatest, the government is developing a knowledge security screening bill. Individuals in the Netherlands who wish to handle sensitive knowledge will soon be required to undergo government screening.[16] The legislation is intended to prevent the undesirable transfer of knowledge and technology by individuals and thus to reduce the risks to national security.

The draft bill was published for consultation in April 2025[17]. The explanatory memorandum contains an extensive justification for and explanation of the intended operation of the bill. The bill also identifies the knowledge and technology domains where the risks to our national security are greatest.

4.4 Additional codes of conduct, frameworks, models and recommendations

Guidelines such as codes of conduct, frameworks, models and recommendations are generally not binding, although they do provide direction. Such instruments are well-suited to the knowledge sector, which is characterised by a high degree of autonomy and self-regulation. The Dutch knowledge sector itself plays a proactive role, both by implementing measures on its own initiative and by actively contributing to joint initiatives with the government. Several important Dutch and European guidelines are summarised below.

Uniform set of risk indicators

A level playing field for knowledge institutions in the Netherlands improves the resilience of the Dutch knowledge sector as a whole. To achieve this, it is important that knowledge institutions collectively employ a common risk assessment framework.

15 https://www.rvo.nl/onderwerpen/veilig-en-weerbaar-ondernemen/11-checks-voor-weerbaar-ondernemen

16 Current status of the bill: https://wetgevingskalender.overheid.nl/Regeling/WGK025662 (in Dutch)

17 Overheid.nl | Consultation on Knowledge Security Screening Act (in Dutch)

For this reason, the *Indicators for Assessing the Knowledge Security Risks of International Collaborations*[18], also known as the 'set of uniform risk indicators', were developed in 2025. Executive boards and staff members of knowledge institutions can use these indicators as a reference to develop or evaluate a risk assessment framework. These indicators were developed in partnership with the central government and experts from the knowledge sector. They are included as an annex to these guidelines.

Universities of the Netherlands (UNL) Knowledge Security Framework and Maturity Model

To assist universities with decision-making and the development of knowledge security policies, the Universities of the Netherlands (UNL) published a Knowledge Security Framework for Universities in 2021 on its own initiative. The text provides a framework to which Dutch universities can commit and within which they can develop their own institutional policies.

The framework addresses opportunities and risks associated with international cooperation, governance and policy frameworks, and provides specific recommendations for risk management. It enables universities to take well-informed, justified decisions about international collaborations.

In 2024, following a recommendation in the report on 'Knowledge in conflict' 2022 by the Advisory Council for Science, Technology and Innovation (AWTI), the universities themselves developed a maturity model. The maturity model, which was published in April 2024, helps universities develop, implement and evaluate their own knowledge security policies. It is an internal tool that can be used to continually improve security measures at the academic and institutional level.[19]

EU recommendations and guidelines on dealing with foreign interference in R&I

The European Union has published recommendations to help knowledge institutions set up their internal compliance procedures. These recommendations are crucial for the implementation of export controls and dual-use regulations in the context of scientific research and knowledge institutions.[20]

The European Council also published recommendations on research security in 2024[21]. This document contains recommendations that are intended to help the European Commission, the member states and the European knowledge sector strengthen their knowledge security policies. These recommendations can help to bring the knowledge security policies of EU member states to a comparable level.

The European Commission has also developed a 'Staff Working Document on Tackling R&I foreign interference', which is aimed at preventing foreign interference in the European knowledge sector[22].

---

18 See annex, but also here: Indicators for Assessing the Knowledge Security Risks of International Collaborations | Report | Rijksoverheid.nl (in Dutch)

19 Knowledge Security | Universities of the Netherlands (in Dutch). The maturity model does not serve as a foundation for the subsequent knowledge security assessment, which will evaluate the extent to which the guidelines have been implemented.

20 EU recommendations for knowledge institutions on internal compliance programmes for controls of research involving dual-use items (2021): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021H1700

21 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510

22 EU guidelines on Tackling R&I foreign interference (2022): https://data.consilium.europa.eu/doc/document/ST-5396-2022-INIT/en/pdf

This document is intended for a broad target group: national authorities, research institutions and organisations, higher education institutions and individual researchers and other staff members of knowledge institutions. The document covers four themes: values, governance, partnerships and cyber security. An integrated approach is presented for each theme, along with examples of possible measures that may be implemented.

Knowledge security in other countries

Other countries are also taking measures to improve knowledge security. Guidelines and checklists are being developed in various countries. Just as the Dutch Guidelines for Knowledge Security, these are intended to provide insight into aspects that should be considered when entering into international collaborations and establish practical frameworks for action. Examples of such countries include Australia, Germany, the United Kingdom, Sweden and Canada.

The fact that both the EU and individual partner countries have developed such texts makes it easier to discuss them during collaborations; our partners are also looking for ways to increase awareness of and resilience against state threats in higher education and science.

4.5 Open Government Act

Everyone has the right to information about what the government does, how it does it and why. If that information is not yet publicly available, government organisations must provide it themselves or in response to a request (an Open Government Act request). The information is then made public. This is mandated by the Open Government Act (*Wet open overheid*).

Although the connection may not be immediately obvious, the Open Government Act is also relevant in the context of knowledge security. The act applies to knowledge institutions that are governed by public law. Public knowledge institutions are undoubtedly covered by the Open Government Act, because they are established under public law. Special universities and universities of applied sciences are established under private law, and are only covered by the Open Government Act insofar as they exercise public authority. Knowledge institutions themselves are responsible for the correct processing of Open Government Act requests.

The principle of public accessibility also applies to documents about knowledge security policy. The Open Government Act does however provide for exemptions. If someone requests information about knowledge security, then an assessment must be made at the document level – and where possible at the paragraph level – as to whether grounds for exemption apply. The grounds for exemption can be found in section 5 of the Open Government Act. Several grounds that are specifically relevant to knowledge security are given below.

When an exemption is applied, the general interest of public accessibility must be weighed up against the interests that the grounds for exemption protect. Knowledge institutions themselves are responsible for carrying out this assessment.

Grounds for exemption that are relevant to knowledge security include:

Personal details
Personal details are not (with some exceptions) published based on Article 5.1, second section of the Open Government Act.

The security of the state, Article 5.1, first section, under b of the Open Government Act
Risks related to knowledge security, such as the undesirable transfer of knowledge and technology, may have adverse effects on the security of the state. Access to documents of a knowledge institution, such as risk assessments, lists of sensitive domains of knowledge or summaries of high-risk international collaborations, may be useful to state actors. If making particular information public permits such misuse and threatens the security of the state, there is a reason not to make documents public. If information is connected to the security of the state, this represents an absolute reason for refusal. This means other interests do not need to be considered. In such cases, you are not permitted to make the document public. It is therefore advisable to apply this reason for refusal in such instances.

International relations, Article 5.1, second section, under a of the Open Government Act
Many documents about knowledge security refer to relations with other countries. This automatically affects international relations, as these may worsen if certain countries become aware that the Netherlands considers them 'high-risk', for example. This may be a reason not to make certain information public. It is possible to redact the name of the country (or institution/company) in question, but it may also be necessary to redact other data. It is important to always consider whether international relations will be adversely affected.

Please be aware that requesting points of view from parties in other countries may in some cases have a negative effect on international relations.

Proper functioning of the state, Article 5.1, second section, under i of the Open Government Act
It is important that administrative bodies can communicate securely with other administrative bodies about knowledge security. The same applies to communications between knowledge institutions and the government. If making information public would mean that this can no longer occur in a secure and trusted manner, for example because other parties would no longer be willing to talk to an institution or the government, this may adversely affect the proper functioning of the State.

The other grounds for exemption in the Open Government Act *may be* applicable to documents that are part of the knowledge security policy of knowledge institutions. This is entirely dependent on the content of the documents. It is important to always assess each document, or even each paragraph, and to weigh up the relevant interests. The guiding principle is always: public, unless.

It can be challenging for knowledge institutions to correctly assess the effects of making documents public on, for example, national security or international relations. This can make it difficult to effectively weigh up the importance of openness against the various grounds for exemption. You can contact the National Contact Point for Knowledge Security for advice about issues such as these.

4.6 Cyber security

Effective efforts to combat cyber risks, both in relation to knowledge security and in general terms, depend on cooperation and the continuous sharing of knowledge and information about these risks. For those involved with cyber security, the SURF security communities are a good platform for exchanging knowledge, frameworks, standards and experience. These include the SURFnet Community of Incident Response Teams (SCIRT) and the SURF Community for Information Security and Privacy (SCIPR).

Cyber Security Act

In 2025, the government decided that state-funded universities of applied sciences and universities would henceforth be covered by the scope of the Cyber Security Act[23] (Cbw). The objective of this legislation is to implement the European Network and Information Security directive, or NIS-2 directive[24], in the Netherlands. The NIS2 directive is intended to improve the cyber security and resilience of essential services in EU member states.

The new legislation imposes a duty of care, which means that appropriate and proportional measures must be implemented to mitigate the risks associated with securing networks and information systems. It also introduces an obligation to report significant incidents, the right to assistance and advice from a Computer Security Incident Response Team (CSIRT) in the event of threats and incidents, a registration obligation and independent external monitoring of compliance with these obligations.

4.7 General Security Requirements for Central Government Contracts (ABRO)

The *General Security Requirements for Central Government Contracts* (ABRO) came into force on 1 January 2026. The ABRO builds on the General Security Requirements for Defence Contracts (ABDO) introduced in 2019. As is the case with the ABDO, the ABRO consists of a working method and an extensive set of security requirements. The ABRO applies to contracts for the central government in which national security plays a role, which means they may affect knowledge institutions.

The National Industrial Security Agency (NBIV) checks whether a company or institution is compliant with the requirements in the ABRO.

Knowledge institutions affected by the ABDO or ABRO have been obliged to set up highly robust risk management processes. This means they can serve as a source of inspiration for knowledge institutions that may not be involved with defence contracts but would nevertheless like to strengthen their internal procedures and processes.

23 https://www.ncsc.nl/en

24 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

Section 5

Assessing risks

This section contains suggestions for how to identify and assess risks of undesirable knowledge transfer. Three factors play an important role:

- The specific details of the research.
- The collaboration partner.
- The collaboration type.

These factors are related, and should be addressed in an integrated manner when identifying and assessing risks.

In 2025, the central government and the knowledge sector jointly developed a set of indicators to allow risks related to knowledge security in the context of international collaborations to be assessed. These indicators flesh out the points requiring attention as described in the guidelines. They represent a minimum common base, with the objective of creating a level playing field in Dutch higher education and science and improving the resilience of the Dutch knowledge sector as a whole. The indicators can be found online and are included as an annex to these guidelines.[25]

5.1 Which domains of knowledge within your institution are at increased risk?

Within your institution, it is important to accurately identify the domains of knowledge that may be affected by knowledge security risks.

The risk of the undesirable transfer of sensitive knowledge and technology applies in particular to knowledge that is specifically developed for military applications or for dual-use technologies (see section 4.1). The Ministry of Education, Culture and Science is developing legislation to introduce an obligatory screening, which includes a more specific list of sensitive technologies. Institutions can access this list by visiting the public internet consultation (in Dutch). This list is authoritative from the perspective of preventing undesirable knowledge and technology transfer. While the bill covers the screening of individuals, this list may also be used in the context of international collaborations with organisations. It may be subject to change during the passage of the legislation.

Risks of malicious influence on research and education primarily apply to topics that affect the international image of particular state actors, or if state actors wish to monitor the loyalty of their citizens. See also section 3.2 for more information.

Finally, in some domains of knowledge, there may be an increased risk that research results will be used for unethical purposes, or a risk that unethical practices may be followed during the research collaboration.

All these risks are even greater in domains where the Netherlands or your own institution has a unique knowledge position. These include domains of knowledge in which your institution has accumulated a reputation and in which research is conducted that is internationally recognised as leading or excellent.

25 https://www.rijksoverheid.nl/documenten/rapporten/2025/06/13/bijlage-2-uniforme-set-risico-indicatoren-voorjaar-2025 (In Dutch, English version in Annex below)

Knowledge security risks may overlap with threats to economic security as part of national security (see also section 1). This may affect, for example, domains of knowledge in which knowledge and technology is used that affects the continuity of vital processes that the Netherlands depends on, or where critical knowledge and technology can be used to exert political pressure. For knowledge institutions, knowledge security is therefore not just about protecting the earning capacity of the Netherlands.

A brief risk assessment can be conducted for each sensitive domain of knowledge. This is not only for national security reasons, but also in the interests of the safety and security of your staff and to protect the core academic values and the reputation of your institution. Ask yourself the following questions:

- Where can unique, sensitive knowledge be found within your institution?
- Which threats exist?
- Which measures can you implement to mitigate these threats?

It is important to note that knowledge and technology can become either more or less sensitive over time. It is therefore advisable to work with a dynamic list of sensitive domains of knowledge and to revise it periodically. See also section 6 for more information about setting up your risk management system and potential measures to counter various threats.

5.2 Which countries represent an increased risk?

It is advisable to develop a risk management policy that is based on threats, regardless of the countries from which they emerge. If your policy only focuses on 'high-risk countries', you may miss potential threats, as they can also emerge from less obvious countries. It is also advisable to ensure that not everything related to a 'high-risk country' is automatically seen as suspicious. That would adversely affect science and is contrary to the principle of non-discrimination.

Publicly available threat information can be used to assess the risk profiles of specific countries. For example, the National Coordinator for Security and Counterterrorism (NCTV), the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) regularly publish a joint 'State Actor Threat Assessment'. The annual reports of the AIVD and the MIVD also contain current information on threats. Another example is www.sanctionsmap.eu, which lists countries that are subject to sanctions (see also section 4.2).

Relevant international rankings and indices of NGOs, research institutes and international organisations can also be consulted. These provide information about the degree of academic freedom, freedom in general and the state of democracy and the rule of law. They can assist in making a broader assessment.

If a country scores poorly in these rankings, that does not necessarily rule out the possibility of collaboration with institutions from that country. In principle, it is possible to cooperate with researchers from such countries, provided that appropriate precautions are taken and the context within which the prospective partner operates is understood. See section 6 for more information about risk management.

The 'Indicators for Assessing the Knowledge Security Risks of International Collaborations'26 contains a summary of relevant sources. These indicators have been included as an annex to these guidelines.

5.3 Know your partners, clients and funding providers

If you are entering into a new agreement, or renewing a collaboration, it is important for the researcher or project manager involved to be familiar with the background of the foreign partner organisation or client. 'Due diligence' is the term used internationally in this regard. What is the institution's scientific reputation? Who exactly will be involved with the project? Who is the ultimate beneficial owner (UBO)? How will the costs be covered? It is also important to consider knowledge security.

Although it is always advisable to pay attention to these aspects, it is absolutely necessary for institutions or companies from countries with high-risk profiles (see section 5.2) and for collaborations involving sensitive domains of knowledge (see section 5.1). In this case as well, it is advisable not to categorically exclude institutions or companies in advance. The objective is to ensure that the staff members involved are aware of the risks and threats and consciously take measures to manage them.

They do not have to be security experts: alertness and open sources can go a long way. Keep a sharp eye out for signs that something may be amiss, for example a partner that no one is familiar with or about which little information can be found on the internet. If the prospective partner is already known within your organisation or to colleagues at other institutions, these sources can be approached for information. Which experiences have they had? Have any incidents occurred? Your institution's security coordinator can help you retrieve this type of information. The following are a few examples of factors to be considered:

- Is the partner affiliated with the government? For example state-controlled companies or institutions.
- Is the partner affiliated with the army or the defence industry?
- Do sanctions apply to the partner?[27]
- Does the institution have a demonstrable reputation in the relevant discipline? If expertise is lacking or if it is unclear how the intended collaboration relates to the partner's usual activities, this gives cause for alertness.
- What other research do the researchers involved in the collaboration carry out? Are they affiliated with multiple institutions/organisations?
- How and with whom is contact about the collaboration maintained? Does the contact occur through an entity other than the actual partner organisation (different name, different address), or has this changed during the process?
- Is it clear what the conditions are and how the research will be used in practice? Does the partner give vague answers to questions about the intended application of the research results? Does the partner object to standard provisions in the agreement for vague reasons or does the partner propose excessive confidentiality provisions?

---

26 Indicators for Assessing the Knowledge Security Risks of International Collaborations | Report | Rijksoverheid.nl (in Dutch, English version in annex below)

27 Checking this is not optional: it is legally required. See also section 4.

There are specialised investigation agencies that can carry out security-related analyses or due diligence investigations. Pay attention to how up to date and reliable the data in the analyses and sources used are.

The same precautions apply to clients and research funders as to research partners. In principle, the type of funding provider (e.g. gifts from donors) does not matter. Start with basic questions such as: 'Where does the money that the partner wishes to invest come from?' and 'Which motives may the partner have for funding the research?' Does the funding provider have economic or political interests in a particular research outcome? The following are a few examples of signs to pay attention to:

- Little or no information can be found about the client or funding provider (e.g. no website).
- The entity being used for funding is atypical for this type of research.
- The client or funding provider makes exceptionally large sums of money available, or proposes particularly favourable funding conditions and asks little in return.
- The client or funding provider does not want the results to be published, imposes exceptionally strict intellectual property requirements or stipulates confidentiality about end users and specifications.

It is advisable to bear in mind that you may also gradually find yourself in a situation of financial or scientific dependence. In such cases, there may be little wrong with the projects and activities individually, but taken together, they allow the funding provider to assume a position that makes it possible to take control of the collaboration and its content. The funding provider may exert personal pressure on your institution and/or the researchers involved, either with positive incentives (e.g. the prospect of rewards) or negative incentives (e.g. threats).

If you believe that security risks are associated with the prospective collaboration partner, client or funding provider, it is important to involve your organisation's security coordinator. Subsequent steps can be considered in consultation with this official. The ultimate decision on whether to enter into a collaboration is the responsibility of your organisation's central decision-making body. When making such decisions, the institution's partner acceptance policy should include explicit consideration of security risks.

5.4 What to bear in mind when entering into a collaboration

Agreements with foreign partners deserve special attention in the risk management systems of your knowledge institution. Clear agreements made 'at the front end' can help to mitigate certain risks and provide a base to fall back on in the event that things do threaten to go wrong. Risks related to knowledge security can also affect procurement and tendering. Measures can be taken to mitigate these risks as well, provided that they are identified promptly.

Collaborations with foreign institutions or companies can arise in many ways, sometimes quite informally and without obligation through the personal contacts of researchers. Once substantive or financial commitments are made, however, it is important that these are documented in an agreement.

Collaboration agreements are a good opportunity to weigh up opportunities and risks. The conclusion or renewal of an agreement or the acceptance of an assignment are excellent points at which to perform risk assessments and mitigate any risks. This includes all forms of collaboration, from broad to specific.

If your institution (or a part thereof) is entering into collaboration with a foreign knowledge institution or a foreign company, your first priority should be to conduct a thorough investigation of exactly whom the institution will be doing business with (see section 5.3). It is important to subsequently make clear agreements that mitigate knowledge security risks as much as possible. If undesirable developments arise during the course of the collaboration, you can talk to your collaboration partner about these. If the risks are not eliminated, you may terminate the collaboration early (exit strategy).

Templates and standard agreements provide a certain level of basic protection against the most common legal and financial risks. If you have determined that the collaboration will involve a domain of knowledge with an increased risk, then standard legal provisions alone will not be enough in many cases. In addition, a comprehensive agreement and other mitigation measures cannot always prevent a situation in which the residual risks remain unacceptable for the responsible risk owner (often the executive board). In such cases, collaboration is not possible.

The Indicators for Assessing the Knowledge Security Risks of International Collaborations[28] can help you determine which specific issues to pay attention to. These indicators were jointly developed by the central government and the knowledge sector. They are included as an annex to these guidelines.

Once the contract has been signed, the agreements made must be respected. This demands regular consultation with the collaboration partner, in which it is important to pay attention to both the substantive progress and the *manner in which* the collaboration is taking shape. Problems and incidents should be identified and addressed promptly. It is advisable to schedule regular evaluations of the collaboration and to agree in advance the topics to be addressed during these evaluations.

Collaboration agreements often continue automatically after the initial term. If the collaboration has proceeded without major problems, there is a tendency not to pay attention to these renewal dates. This should be avoided with high-risk collaborations. It is advisable to set up your internal organisation in such a way that you are informed well in advance of the renewal date to allow for a critical review of the agreement. Developments may have occurred since the agreement was concluded that require additional mitigation measures or tighter delineations.

5.5 Knowledge security in procurement and tendering

Some procurement procedures and tenders involve security risks. This depends on the type of product or service, the client and the company to which the contract is awarded. Examples include contracting out your digital infrastructure, research equipment, cloud services and software, or the replacement of systems that are used to store large volumes of personal data. In addition, some procurement contracts require physical access to sensitive locations, where it is appropriate to take protective measures.

28 See annex.

When launching tendering procedures, it is important to start by identifying whether any such risks exist. The National Security Quick Scan can help you identify risks affecting procurement and tendering. Although this instrument was developed for the central government and the vital sector, it can also provide inspiration for other sectors. The quick scan consists of a number of questions aimed at quickly determining whether a contract poses a risk to national security or whether further investigation is required to determine this.

The following questions can serve as examples:

- Is the prospective contractor equipped with the information needed to carry out the assignment?
- Does the contractor know what to do if security incidents occur, and do the subcontractors also meet the security requirements for the assignment?
- Could a collaboration or agreement with such a company result in a strategic dependency?
- Could sensitive information (e.g. personal data) be leaked?
- Could the continuity of supply be jeopardised and, if so, what would the consequences be?
- Will staff members come into contact with sensitive information?
- What will be done with the information after the contract has terminated?

Once the potential risks of a contract have been identified, measures can be implemented. Examples include imposing additional contract requirements or other measures aimed at risk management (see section 6) and improving digital resilience.

Section 6

Risk management

Knowledge security imposes great demands on the responsibility that knowledge institutions bear due to their institutional autonomy. Within institutions, risk management is a shared responsibility, for which the entire organisation must feel responsible. The objective is always to ensure that awareness of knowledge security permeates into every level of your institution. In this section, we discuss various aspects that contribute to a culture of security and in turn to the resilience of your organisation.

Within knowledge institutions, the board bears ultimate responsibility for risk management. The same applies to the risks associated with knowledge security. Knowledge institutions should therefore have internal procedures and protocols in place, so that they can identify and address risks promptly.

It is important to emphasise that these guidelines should not be interpreted as a call to avoid all risks. It is nevertheless essential to have a good understanding of the threats and risks that exist and to manage them effectively. This section contains several suggestions to help you set up governance and internal procedures.

6.1 Organise risk management within your organisation

Knowledge institutions are often characterised by a layered administrative structure. Action is needed at both the central institution level and the decentralised level to protect knowledge security. Clear agreements must be made about who is responsible for what. Based on the principle that ultimate responsibility rests with the board of the knowledge institution, this means the board delegates decision-making authority. It is advisable to formally document such delegation, as this makes it possible to act quickly in the event of incidents or irregularities.

The knowledge security policy cannot be seen in isolation from other elements of knowledge institutions' responsibility for security. As such, it is important to set up the required processes in a way that takes account of other (security) processes at all relevant levels of the organisation.

Every institution can set up these processes in its own way based on the information in these guidelines. All of these factors and considerations must be developed into working methods, processes and structures that take account of the specific characteristics of your organisation. Risk management demands a tailor-made approach. As the risk level increases, the required risk assessments and controls become stricter and the decision-making authority rises higher and to a more centralised level in the organisation.

Proportionality is essential when developing knowledge security measures. A healthy balance must be found between the threat and risks on the one hand and the measures to be implemented on the other. It is obviously inappropriate to implement too few measures. However, it can also be disadvantageous to implement too many measures, inappropriate measures or measures that are overly intrusive. For example, consider the bureaucracy associated with excessive monitoring and mistrust, and the potential damage to your academic reputation from excessive restrictions on openness and accessibility. The principle of 'as open as possible, as protected as necessary' concisely summarises the importance of proportionality.

6.2 Organisational measures

The ultimate goal is to arrive at an integrated security policy at the institutional level – a policy that brings together the various elements of security. The Integrated Higher Education Security Platform[29] offers many starting points and options for the development of integrated security in higher education.

Knowledge security is strategic and geopolitical in nature and is more than just an operational issue. It requires attention at the administrative level. In specific terms, developing knowledge security policy starts with designating an administrative leader or portfolio holder for knowledge security. This portfolio holder can take responsibility for managing the design and implementation of the knowledge security policy at the strategic level.

The exact way that an institution implements its knowledge security policy is up to the institution itself. There may be differences between institutions, depending on how they are structured and organised. The way that risk assessments are carried out may impose different demands on efficient and effective knowledge security policy at different institutions. Policies must however be designed in such a way that the institution can adequately respond to the various knowledge security risks.

It is advisable to ensure the portfolio holder for knowledge security is assisted and advised by an internal Knowledge Security Advisory Team (i.e. a team consisting of several experts with diverse expertise). The core of this team may consist of: (1) the knowledge security coordinator, (2) the security coordinator or integrated security advisor, (3) an expert in information security (e.g. the Chief Information Security Officer/CISO), and (4) an expert in internationalisation/international collaboration. Depending on the case at hand, other expertise may be added (e.g. an HR adviser). This advisory team should ideally have a formal mandate to provide solicited and unsolicited information and advice to the board about knowledge security issues. For smaller knowledge institutions in particular, it may be useful to combine certain expertise (e.g. about certain countries or domains of knowledge) and to work with a shared service.

It is important that there is an open culture of security within your organisation (see section 6.5 below). It is also advisable to work with confidential advisors or ombudspersons, and to have an effective whistleblower scheme in place. This ensures that staff members can report suspicions of illegal or unethical practices at the institution (anonymously and in confidence). Staff members who have concerns about knowledge security (e.g. if they have serious doubts about the risk assessment for a collaboration agreement) should be aware that they can turn to a confidential advisor to discuss their concerns. The confidential advisors and ombudspersons should be sufficiently aware of the risks associated with knowledge security, and they should periodically refresh their knowledge.

It is of course advisable to ensure that members of staff of the organisation can contact knowledge security advisory teams or coordinators themselves where there is no need for confidentiality, or for mediation by an impartial party.

29 https://integraalveilig-ho.nl/ (in dutch)

6.3 Ensure an accurate factual basis for decision-making purposes

Because the executive boards of knowledge institutions have ultimate responsibility for the risk management of the institution as a whole, it is important that they have access to accurate information. As such, it is advisable that executive boards should receive an up-to-date and complete summary at least once annually of high-risk international partnerships involving research and education. This applies to all relevant types of knowledge security risks, i.e. of undesirable transfer of knowledge and technology, malicious influence on research and ethical and integrity violations. Executive boards should be able to consult the summary at all times. The institutions are responsible for ensuring that these summaries are up to date and confidential.

As mentioned, the institutional autonomy of knowledge institutions gives them a great deal of freedom and responsibility for their own risk management. The exact form that this summary should take, and the exact role of that summary in risk management, may therefore differ. This depends on the needs and requirements arising from the nature of the institution and the way in which it handles risk management. A summary of high-risk collaborations is not a reporting instrument and is not intended to be made public. This means institutions can include confidential information in the summary that may be of importance to the risk management process. See section 4.6 for more information about handling confidential information within the context of knowledge security policy.

Taking this freedom into account, it is the intention that the summary should at least give executive boards the ability to perform a regular assessment of the cumulative risks arising from all current and proposed collaborations, for example if there are undesirable dependencies on foreign knowledge, infrastructure or investments.

It is therefore also advisable that the summary should include at least all current long-term collaborations between organisations or organisational units in the disciplines that the organisation has identified as high risk (see section 5). These must involve one or more partners from outside the European Union and a concluded agreement or investment (for example funding, staff or equipment) by one or both partners.

While the recommendations above can help, knowledge institutions themselves are largely responsible for making their own assessments. They are responsible for ensuring that this summary contains relevant context-dependent details, including:

1. **Severity of the risks**
   There is no clear distinction between relevant and irrelevant risks. For example, whether the risk is significant enough to be important for risk management may vary between institutions, disciplines and risk types.
2. **Nature of the collaboration**
   There are many different forms of collaboration in the sciences. Exactly which collaboration types are relevant for risk management may vary between institutions, disciplines and risk types.
3. **Nature of the foreign interest**
   As well as fully foreign institutions, there may be a foreign interest in collaboration partners in other ways. Examples include collaborations with companies with shared ownership and shareholder structures. The extent to which a foreign interest is relevant from a risk management perspective may also vary between disciplines and risk types.

6.4 Measures to improve security

Physical and digital protective measures

Alongside organisational and administrative measures, physical and digital protective measures can also be effective. Which buildings are freely accessible and which floors or spaces are subject to a restrictive access policy? Ensure that access to areas in which sensitive research is performed (e.g. laboratories) is restricted to those involved with the research.

The same applies to research data. Who has access to such data within the system? Which data and results should also be shielded from peers and colleagues who are not involved with the research? Protecting data (through digital or other means) and restricting access to authorised individuals is an effective and relatively simple way of preventing undesirable leaks.

If highly sensitive research data or results are handled within your institution, it may be advisable to work with document classification. This entails dividing documents into sensitivity classes (e.g. 'confidential' or 'secret'). Classifying documents ensures that all staff members are aware of the sensitivity of the information and the associated security measures. It ensures that everyone within the organisation is speaking the same 'language' with regard to the confidentiality of information, which reduces the risk that sensitive knowledge will be leaked.

Increasing resilience against the undesirable transfer of knowledge and technology demands a mature approach to information security within knowledge institutions. This is particularly the case within organisational units where knowledge or technology are developed that may be valuable to a state actor.

Information security involves various levels of resilience. Various maturity models exist for these levels. To be fully resilient against the most intensive current threats, it is estimated that knowledge institutions and individual organisational units must comply with at least maturity level 3 of the NIST Framework, or maturity level 4 of the NBA Information Security Maturity Model. The lower maturity levels offer insufficient resilience against targeted threats from state actors.

General measures when entering into collaborations

When entering into collaborations, you can implement several measures to mitigate the specific risks. See section 5.4 for more information about what to pay attention to when entering into collaborations.

- Stipulate that the research must be conducted in accordance with internationally accepted standards of scientific conduct, as laid down in national and international codes of conduct, such as the Netherlands Code of Conduct for Research Integrity (see section 2.1).
- Ensure that the agreement contains clearly formulated resolutive conditions. These provisions grant you the right to terminate the collaboration prematurely if matters should arise that are unacceptable to you. A dispute settlement provision may also be useful.
- Determine together in advance which access the partner should have. To which buildings, information or internal networks will the partner have access? What will be shared with the partner? Will access be granted to a complete product, or to a 'light' version without sensitivities? It is advisable to make clear agreements about this in advance. Record these agreements if necessary.
- Investigate whether the collaboration involves dual-use technology (see section 4.1). If so, an end-user statement is desirable. This is a document signed by the end user, declaring that the goods will not be used other than for civilian purposes. It is sometimes known as an End User Statement (EUS).

Measures against malicious influence on research and education

Tackling malicious influence on research and education can be difficult for knowledge institutions. State actors can pressurise or entice individual scientists in various ways. It cannot be assumed that a target for clandestine influence will wish to receive support from the Dutch institution, nor that they will be willing to request it. Neither can it be assumed that knowledge institutions are capable of eliminating the threat from the state actor.

Awareness raising in high-risk areas can contribute to ensuring that victims are not influenced by pressure or enticement. Cases are also known in which victims who had been subjected to pressure did indeed report it and did request support and guidance from the institution. As such, including when carrying out risk assessments, it is useful for institutions to have some understanding of the problem at the point where it becomes apparent.

While this cannot eliminate the threat itself, it can contribute to the (social) safety of scientists and students and increase resilience against the malicious influence of state actors on research and education. The central government and umbrella organisations are working together to raise awareness of this issue and create more practical frameworks for action in the context of protecting knowledge security.

Measures to deal with ethical questions and integrity violations

To increase resilience against the risk that fundamental values and treaties will be violated, you may consider implementing various measures. As is the case with other risks, it is important that researchers and lecturers are aware that there are clear processes and agreements for identifying and addressing these risks. These include training courses, publicity campaigns and the availability and accessibility of information.

Section 2.3 describes one practical framework for action: setting up ethical consultation structures within your institution. These can advise on issues related to the risk that countries will use research results in a way that may violate fundamental values and standards, including human rights.

6.5 Culture of security: awareness and alertness

Creating an open culture of security within your organisation is essential to promote awareness (incident and risk detection) and resilience. Individuals should be able to discuss potential risks openly and in confidence, and they should be aware that internal safety procedures exist for a reason. They should have the opportunity to express concerns and engage in active discussions about potential improvements. Safety and security should not be something that is addressed solely by executive boards and the knowledge security coordinator.

Publicity campaigns can make a useful contribution to raising awareness. They can ensure that the message in these guidelines is conveyed in a way that suits the needs of your organisation.

Awareness raising should never be a one-off exercise: continuous attention is needed to keep everyone alert and to bring new staff members on board. Moreover, because knowledge security (and how it is perceived) is constantly changing, it is important to ensure that knowledge is kept up to date.

The input and expertise available from the central government and various organisations (e.g. UNL and the TO2 Federation) can be used for this purpose. For example, they can provide a platform for learning from experiences at other knowledge institutions, from where you may be able to source useful instruments and checklists. The National Contact Point for Knowledge Security plays an important role in this process.

As well as advising on general questions and specific cases, the contact point manages a 'learning community'. The objective of the learning community is to share expertise from the central government with knowledge institutions and specific target groups at those institutions, for example legal experts and HR staff of knowledge institutions. The learning community is also intended to share and bring together expertise from knowledge institutions. An extensive knowledge bank can be found on the learning community's secure platform. A great deal of relevant information is shared there, as well as good practices from knowledge institutions. The learning community also organises thematic meetings and webinars and develops materials including publicity campaigns, e-learning modules and interactive workshops that are free to use by knowledge institutions.

Any awareness-raising campaign should be adapted to take account of the intended objectives and target groups (e.g. researchers, project managers, support services). It should correspond as closely as possible to their perceptions and realities. An effective publicity campaign should use multiple channels and points of entry. Examples include providing information in posts on the intranet, emails and e-learning modules, as well as interactive meetings and team sessions. Simulations in which (real or fictive) cases are acted out are especially well-suited for training aspects of attitude and behaviour.

It is also useful to consider who should convey the message within the organisation. One essential point in this regard is that managers should set a good example and demonstrate that they are convinced of the importance of knowledge security. In addition, 'ambassadors' may be appointed within the organisation to take on an active role in disseminating the message. Finally, briefings can be provided by the central government. Depending on the objective, these may involve experts from the Ministry of Education, Culture and Science (OCW), the Ministry of Economic Affairs and Climate (EZK), the Ministry of Foreign Affairs (BZ), the National Coordinator for Security and Counterterrorism (NCTV), the General Intelligence and Security Service (AIVD) or the Defence Intelligence and Security Service (MIVD). For more information, please contact the National Contact Point for Knowledge Security.

Section 7

Guest researcher policy and human resources policy

Education, research and science are human endeavours. To manage all relevant knowledge security risk types (see section 1), it is important that institutions are aware of and deal responsibly with staff-related risks.

The institutional autonomy of knowledge institutions gives them a great deal of freedom and responsibility for organising and implementing their own human resources policy. They carry out their own risk assessments and identify their own institution-specific risks. Taking national and joint frameworks and criteria into account, they can subsequently develop their human resources policy in such a way that the identified risks are managed effectively in a way that reflects the nature of the organisation.

To effectively fulfil this responsibility, it must be clear to knowledge institutions what is expected from them based on the relevant legislation and what assistance these guidelines can provide. This section covers the considerations associated with various phases in the appointment of staff members, hosting guest researchers, internal mobility, business trips, departing staff members and human resources policy in general terms.

7.1 Knowledge security in recruitment and selection

Security awareness is very important when recruiting and selecting new members of staff, as the process determines who has access to (sensitive) knowledge and technology, and in which capacity. It starts with the guiding principles and working processes of the human resources policy. It is advisable to incorporate risk assessments from the start of the recruitment process and to share potential security issues with internal stakeholders. Determine as early as possible whether there are specific risks associated with the vacancy, or with other positions. This allows attention to be devoted to mitigating these risks during selection, in the underlying processes and when making decisions. It also makes it easier to specify specific requirements in the vacancy and to discuss them during job interviews, and also to make agreements about any additional measures before the new member of staff commences employment.

It is important to point out that the policy, procedures and decisions connected with recruitment and selection must not be discriminatory. This demands specific attention, because this risk can easily arise when making decisions about individuals in the context of knowledge security risks and compliance with sanctions. There is a risk that unfounded assumptions and prejudices will arise. In the context of Article 1 of the Constitution of the Netherlands and Article 21 of the Charter of Fundamental Rights of the European Union, nationality itself never constitutes a sufficient reason for hiring new members of staff or rejecting applications.

As described in the introduction, the exact details of human resources policies vary between knowledge institutions. As such, it is particularly important that it is clear within the knowledge institution who is involved with various human resources matters and that everyone knows what their roles and responsibilities are in the working processes and in relation to the knowledge security policy.

A human resources policy that protects knowledge security must effectively manage the relevant risks. At the same time, it must be enforceable in practice and the efforts required to do so must be proportional to the identified risks. In other words: when are you doing enough? ‘Due diligence’ is a key term in relation to this dilemma. Whether you are in compliance with the requirements of due diligence depends on the risks, and must be determined on a case-by-case or risk-by-risk basis in the institution’s human resources policy.

The degree of diligence required depends on numerous factors, including the severity, nature and probability of the identified risks. For example, how public, and potentially high-risk, affiliations of a candidate are assessed is strongly dependent on whether the position gives direct access to sensitive knowledge. If the institution does not foresee any significant knowledge security risks, for example because the position does not give access to sensitive knowledge, then the recruitment and selection process may not require any specific due diligence measures. However, if knowledge security risks are identified, it is important that institutions act with care.

Knowledge institutions are not expected to do the impossible or unacceptable. They are subject to unavoidable restrictions, for example as regards the information and the powers at their disposal. They must also comply with relevant legislation at all times. This means that due diligence is limited to that which is possible and acceptable.

It is important that knowledge institutions involve the relevant authorities if they determine that they cannot adequately manage specific risks alone. In such cases, knowledge institutions may contact the National Contact Point for Knowledge Security for advice. The contact point is the central location for all questions about knowledge security. To give organisations appropriate advice, it maintains contact with the relevant government agencies, including the relevant departments at various ministries and security services.

The HR tasks of knowledge institutions can be formulated and described based on two different due diligence levels: (1) Mandatory due diligence (2) Supplementary due diligence.

1. **Mandatory due diligence**
   All knowledge institutions have statutory responsibilities in relation to the selection of staff. See also section 4 of these guidelines. These include, for example:
   a. Compliance with sanctions: The knowledge institution must investigate whether: (1) personal sanctions apply to prospective candidates, guest researchers or lecturers, and (2) there are reasons to assume that there is a risk that technical assistance in relation to specific knowledge and technology that is prohibited, or for which a permit is required[30], will be provided to sanctioned countries.
      It is advisable for knowledge institutions to include the risks of sanctions violations in their general risk assessments to identify which knowledge within the institution requires attention during the HR process.
      To learn more about the various EU and UN sanctions, institutions can use the EU Sanction Map[31]. All current sanctions can be found and searches may be performed to find sanctioned regimes, individuals and entities.
   b. Compliance with Verscherpt Toezicht: The knowledge institution must investigate whether the prospective candidate, guest researcher or lecturer requires a knowledge embargo exemption. This is due to the national sanctions regulations and can, after publication, be found in the list of disciplines covered by the knowledge embargo.[32]

30 EU 2021/821 Article 8 and also Article 2.9, Article 2.10c and Article 4.1.

31 www.sanctionsmap.eu

32 https://www.government.nl/faq/secondary-vocational-education-mbo-and-tertiary-higher-education/do-i-need-an-exemption-from-the-knowledge-embargo

2. **Supplementary due diligence**

   This concerns responsibilities that are not imposed by legislation, but which are very important for the sector in the context of awareness raising and self-regulation. From the perspective of knowledge security, such due diligence is desirable in situations where a vacancy is associated with staff-related risks.

   a. Public affiliations: The knowledge institution investigates whether there are clear knowledge security risks, for example because candidates, guest researchers or lecturers:
      i. have recently worked at institutions in countries that represent an increased risk,
      ii. and worked on technologies with military applications or instruments of strategic power there, for example,
      iii. or currently occupy (secondary) positions involving these topics or at these institutions

   For information about institutions, disciplines and countries, knowledge institutions may contact the National Contact Point for Knowledge Security.

   b. Completeness and verifiability: The knowledge institution investigates whether the CV, letter and interview constitute a transparent and credible whole at the end of the process, and verifies that they contain no problematic and inexplicable gaps or inconsistencies or suggest clandestine activity.
   c. Extensive background check: Knowledge institutions may carry out a more extensive investigation into the personal history or network of candidates based on the supplied CV. This may, for example, include investigating previous activities and collaborations, such as co-authors with whom the candidate has published research.
   d. Integrity assessment: a knowledge institution may choose to ask candidates to cooperate with an integrity assessment. This assessment can give an indication of the honesty and integrity of prospective candidates.

Before the above or other measures are implemented, it is important to carry out a thorough risk assessment to determine what the measures will deliver. Once an institution has chosen to implement particular measures, it is responsible for implementing them in compliance with applicable legislation.

Role of the central government

While the central government itself cannot implement the human resources policies of knowledge institutions, it does offer various facilities that can help knowledge institutions develop and implement their human resources policies. The first of these is the National Contact Point for Knowledge Security. While the National Contact Point for Knowledge Security does not investigate individuals, institutions can ask the contact point for advice, in particular about assessing the risks associated with specific organisations, countries, disciplines or funding, as well as about questions concerning compliance with sanctions. Please be aware that information that can be linked to individuals must not be shared in requests for advice. The institution can use the supplied advice for internal decision-making.

7.2 Education and training

Educational programmes and training courses can contribute to ensuring that all stakeholders at a knowledge institution are capable of effectively exercising the responsibilities associated with the human resources policy. These may include:

- Offering new members of staff a welcome package with relevant knowledge security information and regulations.

- Offering a module or briefing on knowledge security to new members of staff who may encounter knowledge security risks. The basic e-learning module on knowledge security and the e-learning module on knowledge security for researchers can be used. These e-learning modules are available in both Dutch and English on the National Contact Point for Knowledge Security's online platform. The e-learning modules from the National Contact Point for Knowledge Security are also available in a format that can be used in the institution's own learning environment.
- Offering refresher modules at the start of new research projects to maintain the required level of awareness amongst project members.
- Setting up an intranet platform where staff members can find information and test their knowledge and alertness (self-assessment).
- Setting up a special training programme for researchers and students focused on enculturation and integration into the academic community, and the associated principles of research integrity and core academic values.

7.3 Risk of stigmatisation and inappropriate behaviour

Knowledge security is the subject of broad debate across society. There are regular examples in the news, and the intelligence and security services make no secret of the countries they see as the greatest risk to our national security. However, the guiding principle behind knowledge security policy is that it should be country-neutral and non-discriminatory to avoid targeting scientists with a specific background or nationality, even though they do not personally represent a risk.

Experience has shown that it is not always easy for staff members and students to make this distinction. As such, in the context of social safety and inclusion, it is important that knowledge institutions pay attention to the risk of stigmatisation and exclusion of colleagues based on their country of origin. The guiding principle is that staff members and guests should feel welcome and part of a safe social environment, both in the application process and decision-making procedures and during the remainder of their appointment or stay.

It can help if the nuances of the knowledge institution's knowledge security policy are broadly understood among staff members and students, for example. This helps to ensure that they understand that the risks associated with applications must be handled expertly and with care, that you can have confidence in them in general terms as a scientist or student, and that the relevant risks are not based on nationality, for example, but on specific affiliations with high-risk institutions, companies and government agencies.

7.4 Internal mobility and research programming

Access to sensitive knowledge and technology is not only granted during the recruitment and selection process: it can also arise as the result of internal mobility or changes to the research programming of departments. Existing staff members and master's students may join departments or research groups for which risks have been identified at the institution. To keep these risks under control, it is important to raise awareness across the institution. It is also advisable to establish clear agreements and processes to identify when someone moves to a new position or changes are made to research programming at an early stage and to implement measures to increase security as necessary.

In a wider sense, this issue draws attention to the risks that may be associated with existing staff members and (in some cases) master's students. In security jargon, this is known as 'insider risk'. Knowledge institutions may contact the Digital Trust Center at the Ministry of Economic Affairs and Climate Policy[33] for guidance about managing these risks, which generally involves digital security measures. The Digital Trust Center publishes specific recommendations on dealing with (digital) insider risks.

7.5 Access by visitors, guest researchers, guest lecturers and external staff

The organisation's own staff may not be the only individuals with access to specific knowledge and technology at knowledge institutions. Access may also be granted to visitors and for specific activities.

This may involve conference participants, work visits, representatives of companies, guest lecturers, guest researchers, facilities management staff, external staff, caterers etc. Because these individuals are not employed by the organisation, there is often no recruitment procedure. Nevertheless, knowledge institutions can develop policies that cover access by guests and the required decision-making, preconditions and facilities, as is the case for the recruitment and selection of staff. Many of the points mentioned in section 7.1 also apply to access for visitors.

For example, it is advisable to develop a visitor protocol for foreign visits in general. This should devote attention to specific sites within the organisation and to visitors from institutions with an increased risk profile in particular. Visitor policies are not useful unless they are accompanied by physical and digital measures to protect the sites.

Good practice

Examples of elements for a visitor protocol

- Require all visitors and delegations from abroad to be registered in advance by the staff members who will be receiving them. Do not grant access without registration. Require all visitors to identify themselves upon entry and be registered and met elsewhere, for example at a reception point.
- Be aware of where certain visitors are and ensure that they are not allowed to roam, so that it can be assessed in advance whether a visit can occur in a certain area.
- Announce visits to sensitive areas to colleagues in advance, so that they can take this into account.
- Never leave your visitors alone, especially in sensitive areas. They should always be accompanied while on your premises.
- Clearly inform visitors that they are not allowed to take photographs or videos at the site without permission, or ensure that all equipment in sensitive locations is stored away (e.g. in a safe).
- Determine in advance what will and what will not (and what may or may not) be shared with the visitor, and steer all information-related discussions during the visit away from subjects related to information security or the security of sites.
- For highly sensitive research/places/sites, it is better not to receive visitors, or to exclude visitors from countries with increased risk profiles.

33 https://www.digitaltrustcenter.nl/informatie-advies/wat-zijn-insider-threats (in Dutch)

7.6 Business trips abroad

It is advisable to also develop policy to manage the risks associated with outward trips by staff members of your knowledge institution to other countries. This requires awareness raising, preparation and alertness, particularly when visiting countries with an increased risk profile as regards knowledge security.

Good practice
Examples of elements for a protocol for business trips to countries with increased risk profiles

Prior to departure
Take only a minimum amount of (confidential) data with you on the trip.
Consider in advance which data carriers should be taken. If files containing sensitive information that will not be needed during the trip are stored on your laptop, transfer them to another computer before you leave, or take another (travel) laptop with you.

The same applies to your mobile phone. Delete the call history before you leave, or take a different (travel) phone on the trip.
Use passwords and/or access codes on all devices and turn them off whenever possible. Devices that are activated are particularly vulnerable.

En route
Always disable the Bluetooth function on your phone and laptop.
Always take confidential information and data carriers (e.g. USB sticks, telephones) in your carry-on bag, not in your checked luggage.
Exercise caution when conducting confidential conversations on board planes, trains or in other public spaces. As well as the risk that other passengers may listen in, some airlines and other travel operators have close links with intelligence and security services, for example.

At the destination
Protect confidential information. Do not leave confidential data behind in places where they could be seen by others. The same applies to your hotel room or hotel safe.
Never simply hand over your laptop or telephone to others, and always make sure you can check whether someone has seen your information.

Be selective in providing information. Apply the 'need-to-know' principle with your contacts. Do not tell your conversation partner more than is necessary. The same applies during conferences or meetings where you have been invited to speak.
Exercise caution with any USB sticks received (free) at conferences or events. This is an easy way to install malware on your laptop.

See also the General Intelligence and Security Service (AIVD) brochure 'Travelling abroad: Security risks on the move' (in Dutch).

For those working in highly sensitive domains of knowledge and/or who regularly travel to countries with increased risk profiles, it may be advisable to take a Hostile Environment Awareness Training (HEAT) course and to request information about the security situation in advance.

7.7 Termination of employment

Finally, it is important to be aware of certain risks associated with the departure of staff members. This is of course difficult, as it is not possible for knowledge institutions to remain in contact with everyone who has been affiliated with the institution in the past.

However, there are several measures that can contribute to ensuring that the associated risks are mitigated as effectively as possible.

For example, in the case of sensitive disciplines or highly valuable knowledge, knowledge institutions can use the non-disclosure agreement as defined in the collective employment agreement. It is important to note that this must be agreed at the start of employment. The non-disclosure agreement may remain in effect for several years after the termination of employment. It is advisable to seek legal advice when preparing the non-disclosure agreement.

It is also important to make clear agreements about, and to verify the termination of, access to sensitive knowledge and technology. This involves the termination of specific access rights to the physical facilities of the institution, and also access to the knowledge institution's digital infrastructure and sometimes the infrastructure of research groups and laboratories.

For universities and research institutes, it is advisable to devote specific attention to the processes and policies governing the transition to emeritus status and the associated digital and physical access rights.

Annex

Indicators for Assessing the Knowledge Security Risks of International Collaborations

Annex to the National Knowledge Security Guidelines

Spring 2025

Preface

International collaborations and open knowledge sharing are essential for the pursuit of science. However, in an era of tense and shifting geopolitical relations, this international character creates risks. When entering into international collaborations, Dutch knowledge institutions therefore perform a careful and well-considered assessment of the opportunities and risks to protect knowledge security.

Knowledge security
Knowledge security means anticipating and managing risks related to:

a. the undesirable transfer of sensitive knowledge and technology that may affect national security and/or the scientific position of institutions.
b. malicious influence on research and education, through which knowledge can be used by or from other countries and state actors to spread disinformation or encourage self-censorship among students and researchers, and thus to adversely affect academic freedom and the integrity of research and education in the Netherlands.
c. violations of ethical or integrity standards, in which knowledge and technology is used by state actors to violate or undermine Dutch and European values and applicable treaties.

This publication contains a set of uniform indicators that knowledge institutions can use to assess the risks. The set was developed based on various indicators and procedures that knowledge institutions use. These indicators represent a minimum common base, with the objective of creating a level playing field in Dutch higher education and science and improving the resilience of the Dutch knowledge sector as a whole.

➔ **If knowledge institutions employ similar indicators to assess risks, this will enhance the resilience of the Dutch knowledge sector as a whole.**

The knowledge institutions and the central government have jointly developed these knowledge indicators. They flesh out the points requiring attention as described in the National Knowledge Security Guidelines. This document should be interpreted in that spirit. The indicators are non-binding, are intended to serve the interests of the knowledge institutions and are an expression of our shared ambition to make higher education and science more resilient against threats from state actors. The aim is to ensure that international scientific cooperation can take place securely, with an appropriate balance between opportunities and risks, and with respect for and adherence to our core academic values.

For whom?
This publication is intended in the first instance for executive boards and staff members with responsibility for knowledge security at Dutch knowledge institutions. They may, for example, use these indicators as a reference to develop or evaluate a risk assessment framework. This set of indicators may also be useful for others, including researchers, deans, lecturers or project managers if the institution has not published its own assessment framework and to promote security awareness.

Scope

These indicators apply to new international collaborations. In this document, the term **international collaborations** is understood to mean collaborations with organisations or organisational units with a scientific or educational objective that involve an agreement or investment (for example funding, staff or equipment). A unit may be a research project, research line, programme line, department, research group, team, laboratory, study programme or technological discipline. Grant programmes and hosting (research) visitors are also considered to be forms of collaboration. Individuals are not covered by the scope of this document, except with regard to the statutory frameworks in section 1.

The term risks refers to possibility of the transfer of sensitive knowledge and technology to state actors that subsequently use it in a way that is detrimental to national security. This may include military applications, or by disrupting vital processes. It also includes the risk of foreign interference and clandestine influence, and the impact that this has on the integrity of higher education and science, or on the welfare of staff members and students. Furthermore, it includes the risk that sensitive knowledge, technology or research methods will be misused by state actors to undermine Dutch or European values and treaties. These risks are described in greater detail in the National Knowledge Security Guidelines.

The indicators are points that require attention and questions that must be asked before entering into a collaboration. In some cases, specific standards are included, or steps that may be taken. The sources that institutions can generally consult are also included.

Application

The fact that a risk is identified based on these indicators does not necessarily mean that the collaboration cannot proceed.[34] However, an accumulation of risks may indicate that the collaboration is undesirable in the interests of protecting knowledge security. It is important to weigh up the opportunities and risks associated with the collaboration and to determine whether particular preconditions are required that may mitigate the risk, such as access policies and cyber security policies. Mitigation measures can contribute to managing the identified risks. The National Contact Point for Knowledge Security offers advice on estimating risks and implementing mitigation measures.

1. Statutory frameworks

An initial question when entering into an international collaboration is whether the collaboration is *legally* permissible. The following questions must be answered:

➔ **Is the organisation or individual to be collaborated with on an EU or UN sanctions list?**

Dutch knowledge institutions do not collaborate internationally with organisations or individuals on the EU or UN sanctions lists. Transferring goods, technology and/or providing services ('technical assistance') to organisations or individuals on the sanctions list is not permitted. Infringement of a sanctions regulation is a criminal offence.

34 Unless the collaboration is explicitly prohibited by law – see section 1.

All countries to which EU sanctions apply can be found at www.sanctionsmap.eu. At present (early 2025), the list contains institutions and individuals from countries including Belarus, Iran, North Korea, Russia and Syria. Knowledge institutions are also aware of the risk of indirect violations of the sanctions and the need to mitigate this risk. An indirect violation of sanctions occurs if someone deliberately or negligently contributes to the evasion or circumvention of sanctions. This generally involves intermediaries, indirect routes or structures that allow sanctioned individuals or entities to access goods, services or capital.

➔ **Is the research discipline covered by international sanctions?**

As a member state, the Netherlands is obliged to comply with EU sanctions regulations. Knowledge institutions are also directly bound by these prohibitions. Since 2019, the central government has assisted knowledge institutions with compliance with some of these prohibitions by establishing the Undesirable Knowledge Transfer Task Force (Verscherpt Toezicht). The task force specifically focuses on the transfer of specific knowledge and technology to North Korea, Iran and Russia.

In March 2025, the central government issued an update (in Dutch) on all sanctions regulations to which the Netherlands has committed. New updates can be found here (in Dutch). Here you can find a list of the research disciplines and departments for which an exemption must be requested from the Undesirable Knowledge Transfer Task Force.

➔ **Is the research covered by the dual-use regulation?**

For national security reasons, the Netherlands wishes to prevent the export of certain strategic goods, technologies and services. Strategic goods are military goods, dual-use goods and services and sanctioned goods. To prevent undesirable end use, a permit must be requested to export these goods. If a research project involves dual-use or military goods, products, software or technology, then the results of the research may only be exported with a permit from the Central Import and Output Office (CDIU) of the Customs Administration of the Netherlands. Annex I of the dual-use regulation (EU Regulation 2021/821) lists the goods for which a permit is required.

In this context, the term ‘export’ is quite comprehensive. It covers all forms of transfer, regardless of the means, and thus also transfer by email or cloud services. It is possible that this covers products or technologies that were not initially thought to be affected. As such, it is important to check whether a product, software, technology or service is included in the list of dual-use goods.

2. Affiliations and organisation type

To assess knowledge security risks, it is essential to look beyond legislation and regulations alone. Organisations may have links with or may be acquired by state actors. They may threaten our national security through interference, espionage activities or clandestine influence. In this step, the affiliations of an organisation are thoroughly investigated.

State actors use various methods to acquire knowledge. The intentions of state actors, as described in the Threat Assessment on State Actors (DBSA) II, are to become a technological superpower, to reduce dependencies and to use technology as an instrument of strategic power. These intentions, combined with identified offensive (cyber) programmes and threats, mean that institutions must be aware of how state actors attempt to acquire knowledge and the

circumvention routes they may employ to do so. Affiliations offer a good starting point in the context of international collaborations. Circumvention routes through which state actors use (organisations in) friendly states to indirectly access knowledge and technology can also be identified in this way.

Affiliations mean formal and informal links, relationships or memberships that organisations have with other organisations. These may be organisational, professional, political or social in nature. Affiliations are relevant as they provide information about networks, interests, values and the spheres of interest to which an individual or organisation belongs. Relevant indicators include whether a prospective party has links with a government. This is particularly relevant in the case of state actors that represent a threat. State-controlled businesses or institutions, proven military applications of research results intended for peaceful purposes, a non-verifiable reputation or undesirable confidentiality provisions in contracts may indicate potential risks. This summary is not exhaustive.

Institutions should ask at least the following questions:

- ➔ **Does the collaboration involve a partner from a country with an offensive (cyber) programme directed against the Netherlands and western interests?**
- ➔ **Is, or was, the partner affiliated with an organisation outside the EU with military links and does the country or organisation represent a threat?**

The affiliation check is part of the due diligence process and is carried out *before* entering into the collaboration. Both direct (military) and indirect (civilian) affiliations must be checked. Organisations may have been affiliated with an organisation or individual on a sanctions list in the past, or the organisation itself may have been sanctioned.

A collaboration with an organisation from a country outside the EU/NATO that represents a threat may create risks, particularly if there are military affiliations. Assessing the risks of affiliations always specifically considers countries mentioned by the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) in the State Actor Threat Assessment (DBSA) and the Hybrid and Military Threat Assessment, due to the risk of undesirable knowledge transfer. These are China, Iran, North Korea and Russia. If geopolitical shifts result in changes to the threat landscape, other countries may be added following publication in the DBSA.

While institutions pay attention to geopolitical shifts, they do not themselves categorically exclude all collaborations with specific countries. In situations where the collaboration involves entire countries, the government issues guidance.

Institutions also consult other sources to develop a broader picture of the risks of undesirable knowledge transfer, foreign interference and ethical questions. A summary of various useful sources has been included as an annex.

- ➔ **Where applicable, institutions always consult the sources listed in the annex to this document.**
- ➔ **Knowledge institutions always investigate affiliations during at least the past five years. If the circumstances justify it, affiliations during the past ten years may be investigated in some cases.**

Assessing an organisation or affiliation results in an initial risk estimation, which is considered together with the specific details of the research, project or collaboration (see the following section). The combination of affiliations and expertise or areas of interest of the entity and the sensitivity of the research or technology may lead to a collaboration being labelled as high-risk at this stage, particularly if the state actor with which the organisation is affiliated represents a threat.

3. Discipline and research type

Sensitive knowledge and technology

Collaborations that involve specific knowledge and technology may create increased risks to national security, as they may lead to undesirable end use (such as particular military applications) or the emergence of high-risk strategic dependencies (in which knowledge or technology are used as instruments of power). In such cases, sensitive knowledge and technology are involved. Examples include artificial intelligence, quantum research, biotechnology and rocket technology.

The Ministry of Education, Culture and Science is developing legislation to introduce a screening obligation, which includes a more specific list of sensitive technologies. Institutions can access this list by visiting the public internet consultation (in Dutch). This list is authoritative from the perspective of preventing undesirable knowledge and technology transfer. While the bill covers the screening of individuals, this list may also be used in the context of international collaborations with organisations. It may be subject to change during the passage of the legislation.

- ➔ **Does the research involve or use sensitive technology that is not already publicly accessible?**
- ➔ **Is the objective of the research to develop, study or produce applications in the military, police, intelligence or security domain?**
- ➔ **Does the research have a broad area of application in vital infrastructure or vital processes?**

The National Coordinator for Security and Counterterrorism (NCTV) has published a description of vital infrastructure and processes.

The degree of sensitivity of a technology may be lower in the case of fundamental research, although there may still be risks, for example if a specific high-risk application is intended, or in the event of a collaboration with an external funder.

4. Dependency and influencing

To assess the risks of international collaborations, knowledge institutions also pay attention to foreign interference and sources of funding.

Foreign interference

State actors may attempt to influence research and education. They may wish to change the way the actor is seen and understood internationally. State actors may also wish to monitor and control their citizens, for example by ensuring that they do not express dissident or negative statements about their country of origin. Scientific experts can be used by state actors to serve as credible mouthpieces, particularly if these experts express views that align with the interests of the state. Finally, interference may also be aimed at undesirable knowledge transfer.

To achieve this, a state actor deploys (financial) resources either as an incentive (reward) or as a means of applying pressure (threat). Scientists or students may also be financially dependent. The resulting pressure may lead to self-censorship, with individuals or groups sometimes unwilling to openly express critical views. Academics may also be discouraged from publishing research results if these do not align with the wishes of the state actor. This may adversely affect the social safety of the scientist or student. As such, it is crucial for researchers and students to be able to talk about their experiences or identified knowledge security risks in a safe environment without suffering consequences.

To assess the risks of foreign interference, knowledge institutions assess the source and potential objective of funding when entering into collaborations. They ask at least the following questions:

- ➔ **Is/are the collaboration or incoming (guest) staff members (principally) funded with external funding from a single source?**
- ➔ **What are the reasons for the partner to fund the research, the collaboration or the individuals involved?**
- ➔ **What is the origin of the funding?**
- ➔ **Is the collaboration (partly) funded by a foreign (government) provider with links to a state actor that represents a threat or that is known to misuse research?**

Grant programmes

Collaborations may involve foreign grant programmes. Some state actors fund international grant programmes with the objective of interfering or obtaining access to sensitive knowledge. For many Dutch institutions, financial contributions make it attractive to recruit scientific talent without incurring high costs. State actors are aware of this and are actively working to create such dependencies. The knowledge institutions pay attention to this. As regards grant programmes funded by organisations in high-risk countries, the knowledge institutions ask the following questions:

- ➔ **Is the grant awarded for a period of less than two years for a subject set by, and with guidance from, the home country?**
- ➔ **Will the grant recipients study or work with sensitive technology that is not already publicly accessible?**
- ➔ **Do the grant recipients come from a university with military links or from a country that represents a threat?**

5. Ethics and integrity

Unethical practices

Before knowledge institutions assess the ethical aspects of collaborations with foreign parties, it is important that researchers ensure that their own work complies with the Netherlands Code of Conduct for Research Integrity and that the knowledge institutions comply with their duties of care with regard to ethical standards and procedures.

Some research types may result in human rights violations, misuse of knowledge or unsafe situations for researchers and respondents, for example if data come into the hands of other state actors or if research data about marginalised groups reach a repressive government. This may result in reprisals directed at these researchers and respondents. To limit these knowledge

security risks, it is important to pay attention to signs of such undesirable practices and to ensure that the collaboration partner recognises and complies with academic values.

Institutions should ask at least the following questions:

- ➔ **Is there a risk that the freedoms of the researcher(s) may be threatened?**
- ➔ **Are countries with serious restrictions on academic freedom involved with the collaboration?**
- ➔ **Can the research results and/or data be used for purposes that conflict with the protection of human rights?**

One way of identifying such signs is by performing due diligence. For example, it is possible to investigate whether there are negative reports in reliable or independent media. Such sources can provide information about the reputation of a business partner. There may be news reports of human rights violations or recent bribery and corruption scandals. Institutions can also purchase tools for due diligence investigations. These tools check for evidence such as criminal offences, negative media coverage, sanctions lists, state-owned companies and state-financed companies. Due diligence can also be performed during the research to trace potential unethical applications.

Assessing and weighing up ethical questions in the context of international collaborations can be a difficult and sensitive process that involves careful considerations. As such, knowledge institutions have their own criteria and specific process steps for doing so, so that the considerations are transparent.

Sources

Knowledge institutions consult various sources to assess the risks associated with entering into international collaborations. These sources refer to various risk indicators and are not equally suitable for all collaboration types. This summary lists sources that the government and the institutions consider to be reliable and useful.

General

Staff members and executive boards can consult advisory teams, committees and/or officers about knowledge security risks. Consultations are always held if major risks are suspected.

The National Contact Point for Knowledge Security provides information and advice in response to questions about risks and measures to be undertaken in relation to international collaboration in higher education and science.

- National Contact Point for Knowledge Security

Statutory frameworks

The government provides the following sources to help determine whether, and under which conditions, a collaboration is legally permissible:

- Central government - International sanctions (in Dutch)
    - Sanctions schemes - current situation as of 20 March 2025 | Regulation | Rijksoverheid.nl (in Dutch)
- EU Sanctions Map
- United Nations Security Council Consolidated List
- Exemption from Knowledge Embargo
    - 2017 sanctions regulation covering North Korea (in Dutch)
    - 2012 sanctions regulation covering Iran (in Dutch)
    - 2014 sanctions regulation concerning the territorial integrity of Ukraine (in Dutch)
- EU dual-use regulation

Affiliations and organisation type

The Dutch intelligence and security services publish threat assessments. These identify China, Iran, North Korea and Russia as countries with offensive (cyber) programmes directed against the Netherlands and western interests. These countries represent a threat to all international collaborations. There is a major risk of undesirable knowledge and technology transfer, particularly with sensitive technological research.

- National Coordinator for Security and Counterterrorism - Threats from State Actors (in Dutch)
    - State Actor Threat Assessment 2025
    - Hybrid and Military Threat Assessment (in Dutch)
    - Phenomenon Analysis 'Across the Border' (in Dutch)

Institutions also use various online tools to perform risk assessments. The following tools are useful for investigating military links and affiliations with state actors in various countries:

- ASPI Defence University Tracker
- Named Research Organizations
- CSET

Discipline, research type and funding

The Ministry of Education, Culture and Science is developing legislation to introduce a screening obligation, which includes a specific list of sensitive technologies. Institutions consult this list as a minimum when assessing sensitive knowledge and technology.

- Knowledge security screening bill: Annex 2 to the bill and section III of the explanatory memorandum (in Dutch)

In the past, institutions used the list of key technologies published by the Dutch Research Council (NWO). This list is still usable, but is broader than the list in the bill.

- Key enabling technologies | NWO

The risks of foreign interference, clandestine influence and ethical issues are greater in the case of collaborations that involve countries with limited academic freedom. These sources can be used as an initial indication of whether there are risks associated with a collaboration. Knowledge institutions pay particular attention when working with countries with a score of 0.4 or less in the Academic Freedom Index, or a score of 5 or less in the Democracy Index.

- Academic Freedom Index
- Democracy Index
- Freedom in the World
- World Justice Project Rule of Law

Ethics and integrity

When entering into international collaborations, the institutions follow the five principles set out in the Netherlands Code of Conduct for Research Integrity.

- Netherlands Code of Conduct for Research Integrity

Contact details

National Contact Point for Knowledge Security

Telephone: +31 88 042 42 42
Email: info@loketkennisveiligheid.nl
Website: english.loketkennisveiligheid.nl

Export control - Central Import and Export Office (CDIU)

Telephone: +31 88 151 21 22
Website: https://www.douane.nl/en/themes/safety-health-economy-and-environment-vgem/cdiu/
Application form for request for classification: www.douane.nl/kennisbank/documenten/aanvraag-indelingsverzoek/ (in Dutch)