Toolkit

Knowledge security

Introduction

Knowledge Security Guidelines
How do NWO institutes identify the risks surrounding knowledge security?

Undesirable knowledge transfer

Dual use en exportcontrole

Cybersecurity

Interference

Covert influence

An open and socially safe culture

Ethics/integrity

Academic core values

Moral deliberation

Social safety
Do you feel free to initiate a conversation?

I am starting a new project or are involved in an ongoing project with possible knowledge security risks
Possible steps to address any concerns

Knowledge security in popular media
Reading and viewing tips for more insight

About this toolkit

This toolkit has been developed for those employees at the NWO institutes who support or conduct scientific research. It contains information and tools about knowledge security: who is it important for, and what does it cover? What are your options should you encounter difficulties, and where can you find further information? What guidelines does NWO-I apply? You can use this toolkit wherever necessary and use it as a reference, depending on what is most relevant to your work.

What is knowledge security?

The knowledge security policy is based on the National Security Strategy. The approach to knowledge security in the knowledge sector is described in the National Knowledge Security Guidelines. It is a direct response to the shifting geopolitical landscape, in which research and innovation are playing an increasingly significant role in how state actors acquire and consolidate their power. The international and open character of science is thus put under pressure. The knowledge security policy has been developed to protect the Dutch national security and to safeguard science itself from external influence. The Dutch knowledge institutes develop and implement their knowledge security policies based on the National Knowledge Security Guidelines.

The definition of knowledge security can be divided into three main categories:

1. Undesirable knowledge transfer: the transfer of knowledge and technologies as a result of which the national security (and sometimes the competitive strength) of the Netherlands can be threatened.
2. Interference: (covert) influencing of academic education and research by or from within other states; as a result of this, academic freedom and the safety of students and researchers can be put under pressure.
3. Ethics/intergrity: ethical issues that can play a role in the collaboration with institutes and researchers in countries where governments do not respect human rights, or fail to do so sufficiently.

National Security Strategy

In the National Security Strategy, the Ministry of Defence periodically describes threats to the national security of the Netherlands. The current strategy covers the period from 2023 to 2029. As part of this strategy, a line of action has been developed that focuses on: *'Increasing the resilience of the economy and protecting science*': The Netherlands must actively pursue a knowledge security policy in order to prevent specialist knowledge from falling into the hands of state actors that could pose a threat to Dutch security. To boost the economy's resilience, this line of action also focuses on reducing the risks of strategic dependencies, for example in terms of technological knowledge.

National Knowledge Security Guidelines

The approach to knowledge security by knowledge institutes is described in the National Knowledge Security Guidelines ('Guidelines'). The Guidelines provide insight into the context of knowledge security and provide tools to help implement the knowledge security policies. The Guidelines were drawn up by the following umbrella organisations: Universities of the Netherlands (UNL), the Netherlands Association of Universities of Applied Sciences (VH), the Netherlands Federation of University Medical Centres (NFU), the Dutch Organisation for Scientific Research (NWO), the applied research institutes (TO2), the Royal Netherlands Academy of Arts and Sciences (KNAW), and the Ministry of Education, Culture and Science. While it is not a binding document, its joint creation has led to the expectation that knowledge institutes will adopt the Guidelines for the implementation of their policies.

Uniform risk indicators

In 2025, a national working group developed a set of indicators for Risk Assessment for International Collaborations involving Knowledge Security. This set of indicators provide knowledge institutes with tools for assessing the risk profile of international collaborations. The document serves as an Appendix to the National Knowledge Security Guidelines. As indicated by the document itself: a risk identified on the basis of these indicators does not mean that collaboration is inadmissible. However, an accumulation of risks may indicate that cooperation is inappropriate in the context of knowledge security.

Sensitive technologies

The knowledge security policy often refers to sensitive technologies. The National Contact Point for Knowledge Security (Loket Kennisveiligheid) describes this term as follows:

- **Dual-use items:** knowledge, goods, technology, or software that could serve both civilian and military purposes.
- **Crown jewels:** the knowledge domains within which the Netherlands or institutions in the Netherlands hold a unique position. Consider, for example, an area for which an institute is internationally recognised.
- **Knowledge areas where expertise is essential to critical national processes:** consider, for example, the internet, transportation and gas production.
- These are knowledge areas in which the Netherlands is heavily dependent due to a lack of viable alternatives of its own.

While there is no complete list of technologies considered sensitive by the government, there are various lists associated with legislation that contain dual-use or sensitive technologies. Some of these lists are:

- The EU Dual-Use Directive (2021/821 – Annex 1). This extensive list covers those technologies that fall under the EU export control regime because they are dual-use items.
- List of sensitive technologies appended to the Vifo Act. This is a Dutch list accompanying the Investments, Mergers and Acquisitions Security Screening Act (*Wet veiligheidstoets investeringen, fusies en overnames*; Vifo Act), as of 2023. This law requires a government assessment of risks to national security in cases where new investors or owners become involved in, for example, companies.
- Draft list of sensitive technologies forming part of the Knowledge Security Screening Bill. The Knowledge Security Screening Bill was published in April 2025 for the purpose of an online consultation process. This was accompanied by a draft list of sensitive technologies to which the screening, which has been proposed but has not yet been enacted into law, would apply.

If you are not sure as to whether or not you work with sensitive technologies, please contact the **knowledge security contact person** at your institution.

Where can I turn to?

- Knowledge security contact person: all institutes have a knowledge security contact person. Check within your own institute or with the knowledge security coordinator to find out who this is
- NWO-I knowledge security coordinator: via strategy@nwo-i.nl

- Contact Point for Knowledge Security: this contact point is a central hub bringing together all the Dutch government's expertise on knowledge security, which can be consulted in complex cases. You can present a question to the Contact Point for Knowledge Security via the NWO-I knowledge security coordinator

- Knowledge base for knowledge security: there is a knowledge base available on NWO-I's website with some relevant reports for more background information

Undesirable knowledge transfer

Undesirable knowledge transfer can take different forms:

- This may involve the transfer of knowledge that has an impact on *national security,* for example because a hostile state uses the knowledge to enhance weapons or other military means.
- Also, *economic impact* can play a role in some cases, for example, if the transfer of knowledge affects the economic competitiveness of the Netherlands and Dutch businesses.
- Partly overlapping with this, it may concern the transfer of *knowledge that contravenes the law,* for instance, through violations of export control legislation or sanctions.
- Sometimes, undesirable knowledge transfer involves transfer of knowledge that *has a negative impact on human rights.* As an example, a state might use stolen technological knowledge to conduct surveillance on a specific population group. Or, consider a scenario in which information about the abuses of a particular government falls into the hands of that same government, potentially putting the source of this information at risk.

Dual use and export control

Sometimes, scientific research leads to a discovery or a new technology that can also be applied in a military setting, hence the term dual use. Examples include radar technology, rocket technology or software that encrypts files. Given the fact that these technologies can thus also be used by state actors or armies against civilians, there are stricter regulations in place with regard to the export of these technologies to other countries and sharing them with these countries, also referred to as export controls. These regulations are often enforced by customs. In the Netherlands, this task is carried out by the Central Import and Export Office (CDIU).

For certain countries, there are particularly strict rules or sanctions in place on the export of dual-use goods or technologies. The Netherlands adheres at least to the sanctions that apply to the entire EU. You can find a list of countries subject to EU sanctions at: *sanctions map*. Below is an overview of the main sanctions relevant to NWO-I:

Countries with an EU dual-use restriction and/or a telecommunications restriction:

- Belarus (dual use/telecommunications)
- Iran (dual use)
- Myanmar/Burma (dual use/ telecommunications)
- North Korea (dual use)
- Russia (dual use)
- Syria (telecommunications)
- Venezuela (telecommunications)

Cyber security

There are many parallels between knowledge security policy and cyber security measures. In both cases, amongst other things, the aim is to prevent information from falling into the wrong hands. Cyber security prevents knowledge from being stolen via digital channels. It also prevents espionage within the organisation's networks. Adequate cyber security is therefore a prerequisite for knowledge security.

What can you do with regard to cyber security and knowledge security? Follow guidelines concerning online security and be aware of online threats. Regularly change your passwords, making sure to use strong and unique passwords. In other words, do not re-use passwords for different accounts. You could use a password manager for support. Also, be aware of phishing attempts and vishing attempts, i.e. voice phishing, which is often done via the telephone. And when you go on a trip, only take work-related information with you that you actually need. Depending on your destination, it may be wise to bring a laptop and telephone that are wiped clean from information. Check this with your IT department.

Where can I turn to?

- NWO-I knowledge security coordinator: via strategy@nwo-i.nl
- Information Security Officers or the Chief Information Security Officer: your institute's ISO and the CISO of the NWO-I Office deal with cyber security. They are available to receive reports and can answer your questions
- Legal Affairs: NWO-I has a Legal Affairs Department that may be able to offer you assistance and guidance. Legal Affairs can be reached via juridisch-i@nwo.nl

Interference

Interference involves the covert influencing of academic education and research by or from other states; as a result of this, academic freedom and the safety of students and researchers can be put under pressure.

- Consider a situation in which a professor is asked not to include certain information in their lectures, otherwise there will be consequences for their career or research funding.
- Or a scientist who is conducting research into human rights violations by the government of their country of origin, and subsequently receives threats directed at them and/or their family, forcing them to withhold or alter information in the research, or even to abandon the research altogether.

Covert influence

The effects of covert influencing could have a major impact on individual employees. Employees of an institute may feel compelled to spy for a state actor due to enormous pressure on them or their family. Or, employees may feel forced to pass on knowledge or information which may result in undesirable knowledge transfer. It may also lead to employees no longer daring to speak out in debates, for example. If scientists no longer feel free to engage in academic debate, this constitutes a violation of their academic freedom, an important core academic value.

An open and socially safe culture

Creating and maintaining an open, socially safe culture is an important prerequisite for a successful knowledge security policy. Having an open, socially safe culture at institutes may help you feel more comfortable reporting covert influence or attempted covert influence to, for example, a confidential advisor or the institute's management team. This, in turn, makes it possible to take protective measures, and the means to jointly discuss the options of further action.

Where can I turn to?

- NWO-I knowledge security coordinator: via strategy@nwo-i.nl
- The knowledge security contact person at your institute
- The knowledge security advisory team: the knowledge security contact person can help you present a difficult case to the advisory team. They can support you in finding a possible solution
- Confidential advisor: Do you recognise or are you experiencing covert influencing? Please know you can always discuss this with a confidential advisor at your institute, or with an external confidential advisor. The individuals involved differ across institutions
- NWO-I Confidential advisor for research integrity: Some case studies on research integrity are possibly being violated. In those cases, you may also contact the confidential advisors for research integrity

Ethics/integrity

This component of knowledge security involves issues that may arise in collaborations with researchers based in countries in which governments fail to respect human rights, or fail to do so sufficiently. See the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union.

- Moreover, this may involve countries where Dutch principles of research integrity are not being upheld. For more information please read the Netherlands Code of Conduct for Research Integrity.
- For example, a state might use stolen technological knowledge to conduct surveillance on a specific population group.
- Or, consider a situation in which a foreign research partner contributes DNA data, of which there is no certainty that these have been collected in an ethical manner.

Academic core values

The Netherlands applies academic core values, such as open science, research integrity and academic freedom. In a collaboration, a partner may violate or seek to restrict these academic core values, for example by influencing research questions or by not being transparent about the data underlying an analysis. Make sure you protect the academic core values. Pay extra attention to countries with governments that fail or fail to sufficiently respect human rights and those countries with poor academic freedom.

Moral deliberation

Considerations involving knowledge security can be complex and may lead to ethical dilemmas. Do you share certain sensitive data (assuming there are no legal restrictions) or not? Should you enter into a partnership with an organisation or individual from a country with a high-risk profile? Would you terminate a collaboration if you had concerns about knowledge security or not? In-house guidelines provide tools for such deliberations, but they are not always conclusive.

Moral deliberation is a structured approach to analysing a case and reaching a carefully considered decision. NWO-I offers institutes support in dealing with dilemmas by offering moral deliberation workshops.

Where can I turn to?

- NWO-I knowledge security coordinator: via strategy@nwo-i.nl
- Request for a moral deliberation workshop for your institute via strategy@nwo-i.nl
- Consult with your institute's management team for guidelines or standards

Social safety

Having an open, socially safe culture is an important prerequisite for a successful knowledge security policy. In an open safety culture, individuals feel free to initiate a conversation and report any identified risks to safety and knowledge security. Social safety is also key in protecting the academic values: if these are under pressure or if they are being violated, individuals should feel no hesitation in speaking up about this. Furthermore, social safety is important as geopolitical relations play a role in the knowledge security policy. We want everyone, regardless of nationality or background, to feel welcome and safe within our organisation.

Uncomfortable situations

The Dutch knowledge security policy may lead to uncomfortable situations in your everyday work. For example:

1. Employees who suspect there to be a knowledge security risk during a collaboration and who do not know who to turn to or how to address this.
2. Employees who suspect that their cooperation partner is violating academic core values.
3. Employees who suspect that their colleagues may have been put under pressure by their government.
4. Employees who feel discriminated against or stigmatised by the knowledge security policy.

Language makes a difference

Given that knowledge security is a complex subject whereby geopolitical relationships play a role, it is essential to engage in conversations about knowledge security in a nuanced manner. For example, make a distinction between a state's actions and do not generalise entire groups of people with a certain nationality. This will help to prevent people from feeling stigmatised or discriminated against on the basis of their nationality or origin. It is furthermore important to realise that individuals from countries where the state exercises considerable influence over its diaspora may not always feel at liberty to speak openly in political discussions and may be reluctant to share personal information. Please bear this in mind when you engage in dialogue.

I am starting a new project or are involved in an ongoing project with possible knowledge security risks

New project

If you are planning to start a new project, please be advised to check whether this project falls under one of the sensitive technologies. Please contact the knowledge security contact person at your institution when in doubt about this.

At the very least, make use of the Knowledge Security Guidelines drawn up by NWO-I and which apply to all NWO institutes to identify any possible knowledge security risks. The knowledge security contact person can help you in going through the Guidelines.

If the Guidelines indicate that there are possible knowledge security risks, for example given the sensitive subject or if it concerns a collaboration with a country with a high-risk profile, the institute's management team will need to be informed about this. You can inform them together with the knowledge security contact person. In the event of a high risk to knowledge security, you will furthermore require approval for a collaboration from the Board of Governors of NWO-I.

Ongoing project

It may be that technologies are being developed during an ongoing project that may potentially also have dual-use properties, or that a current collaboration suddenly changes, for example, because a party from a country with a high-risk profile starts to contribute more funds and thus gains more control over the project. In that case, it is also well-worth going through the Guidlines again and it is often advisable to inform the institute's management team. This can be done together with or via the knowledge security contact person at your institute.

Where can I turn to?

- The knowledge security contact person: for a new project or changes to an existing one, the knowledge security contact person is the first and easily accessible point of contact. It would be advisable to regularly consult with the knowledge security contact person
- NWO-I knowledge security coordinator: via strategy@nwo-i.nl
- Legal Affairs: The Legal Affairs Department can assist in drawing up agreements and cooperative agreements in which the principles of knowledge security can be observed. In case of any risks to knowledge security, it would be advisable to first have the Legal Affairs Department check the agreement. Legal Affairs can be contacted via juridisch-i@nwo.nl

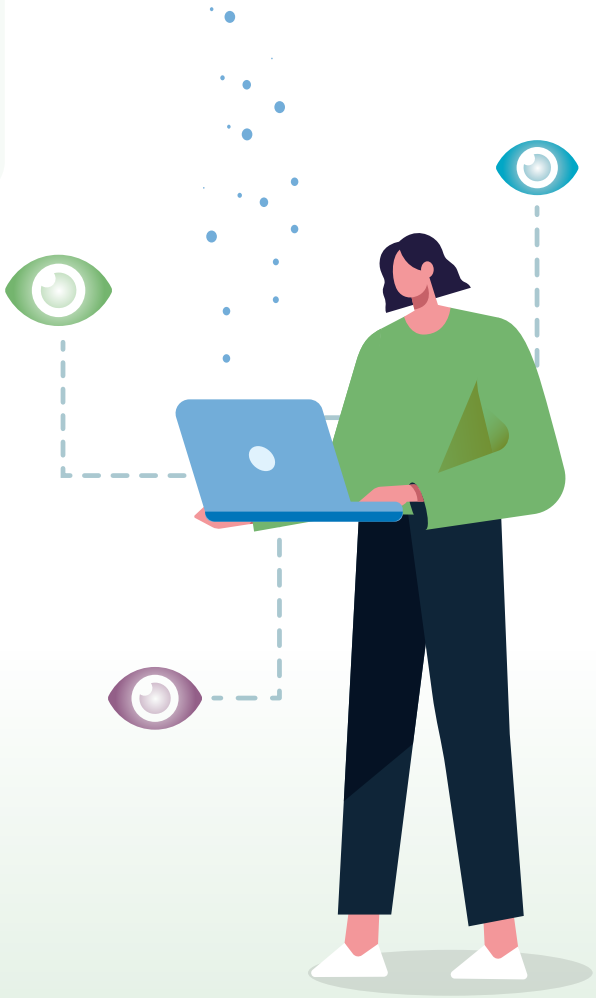
Knowledge Security Guidelines

The Knowledge Security Guidelines help gain insight into potential risks to knowledge security. Are you involved in international cooperation? Are you going abroad or is someone visiting your institute? Knowledge security may come into play in all those situations. The Knowledge Security Guidelines help identify any risks and give instructions on how to proceed from there.

There are five guidelines on knowledge security:

1. International cooperation
2. Work-related travel abroad
3. International visitors
4. Recruitment and selection
5. Appointment of guest researchers and scholarship students

Your institute's intranet contains the Guidelines. They are available for NWO-I office employees by sending an email to strategy@nwo-i.nl



Knowledge security in popular media

- **NPO 1 Podcast:** NPO1 (Argos) has made two podcasts that highlight the theme of knowledge security. The first series is '*De man en de maan*' (The man and the moon). It is about a Dutch astronomer who enters into a controversial collaboration with China. The sequence, '*Vriend of vijand*' (Friend or Foe), takes a closer look at the theme of knowledge security policy and the effects thereof. Both provide a very good impression of knowledge security in the Netherlands and internationally.
- **Huib Modderkolk:** This Dutch author has written two books on the changing world order and what this means for science, amongst other things:
  - **Het is oorlog maar niemand die het ziet** (It is war, but nobody sees it) (Publisher Podium, 2019. ISBN 9789057599804)
  - **Dit wil je écht niet weten** (You really do not want to know this) (Publisher Podium, 2024. ISBN 9789463812160)
- **Film**: historical movies can also provide a good representation of why there needs to be knowledge security policy. Consider, for example, films such as 'Oppenheimer' (2023) or 'Red Joan' (2018).