VRIJE UNIVERSITEIT AMSTERDAM

FACULTEIT DER BÈTAWETENSCHAPPEN

Knowledge Security

Faculty procedure and summary of VU Knowledge Security Framework for international collaboration

About this document

URL	Knowledge Security
status	Faculty procedure
version	2
authors	Esther van de Hengel, Maaike Verbree, Kirsty Brachel
date	3 November 2023
distribution	Faculty of Science

Vastgestelde versies

#	Date	Auteur(s)	Changes
1	20220706	Esther van den Hengel, Maaike Verbree	
2	FB-besluit 20231103	Kirsty Brachel, Maaike Verbree, Esther van den Hengel	Connection to VU Framework Knowledge Security

Index

Background

The purpose of knowledge security is to ensure that international collaboration can take place securely. It is about knowing and recognising the security risks associated with international collaboration, with the aim of enabling such collaboration between scholars to take place as securely as possible. It is based on the core values of academic freedom and scientific integrity.

Knowledge security policy has three aims:

1. First, it is about preventing the undesirable transfer of sensitive knowledge and technology. Any such transfer is undesirable if it affects national security.
2. Knowledge security is also about the covert influences on education and research by other states. Such interference forms a danger to academic freedom and security in society.
3. Finally, knowledge security concerns ethical issues that could arise in the collaborative partnerships with countries that do not respect fundamental rights or, in the case of VU Amsterdam, institutions that do not share our academic values.

The VU Knowledge Security Framework came into force on 1 September 2023. This framework ensures that international cooperation can take place in a safe manner. It supports the consideration of whether or not to enter into a collaboration with a person, institution, funder or client. This means that when entering into international cooperation and/or relationships for research, education and business operations, everyone must always answer the questions in this framework before a collaboration can be entered into.

A key focus is to increase awareness of knowledge security among all VU employees. This faculty procedure on knowledge security aims to contribute to this.

Faculty procedure

For staff of the Faculty of Science (BETA), the following process steps guide the legal review and risk assessment of knowledge security when engaging in international cooperation:

1. If an employee wishes to enter into or renew an international cooperation, the 6 questions of the Knowledge Security Framework must be answered beforehand.
    a. If it involves recruiting a new employee[1] or providing hospitality, the HR adviser should be informed. The HR adviser[2] has an advisory and signaling role in relation to Knowledge Security and can advise an employee to complete the Knowledge Security Framework questions. For hiring new employees, a fact sheet has been prepared for you to consult.
    b. If a cooperation agreement is involved, consult the factsheet 'Keep direction and avoid dependency' (Houd regie en voorkom afhankelijkheid) and contact legal@vu.nl if necessary to make proper contract arrangements.

   When co-authoring manuscripts, alertness is required if the corresponding author is from a high-risk country (see section 4 Knowledge Security Framework).
2. If one or more of the questions of the Knowledge Security Framework are answered with 'yes', or if there are doubts about answering the questions, additional questions should be answered. The comprehensive questionnaire can be found here and in Appendix 2 of the Vrije Universiteit Amsterdam Knowledge

[1] These are both employees with academic and support job profiles.
[2] For an overview of HR-advisors and department managers for each department see here.

Security Framework. Completing this comprehensive questionnaire helps to speed up the advisory and decision-making process.

3. Send the completed comprehensive questionnaire to the faculty Knowledge Security Contacts (Esther van de Hengel and Maaike Verbree) and inform the department's MT via the department manager[3].
4. The Knowledge Security Contacts will decide - based on the completed questionnaire - whether the cooperation can go ahead. If uncertainty remains, they will ask the employee concerned for more information. Before making a decision, they may request a recommendation from the VU University Amsterdam Knowledge Security Advisory Group. The VU Amsterdam Knowledge Security Advisory Group has online consultation hours every Thursday.
5. Only the Knowledge Security Advisory Group may, if necessary, contact the National Contact point Knowledge Security (Landelijk Loket Kennisveiligheid) for additional advice.
6. The Knowledge Security contact persons will decide, based on the completed comprehensive questionnaire and, if necessary, on the advice of the VU Knowledge Security Advisory Group, whether the cooperation can go ahead. In some cases, it will be necessary to have one or more discussions. The contact persons can substantiated deviate from the advice by the Knowledge Security Advisory Group or “Landelijk Loket Kennisveiligheid”. If necessary, decision-making is discussed with the Faculty Board.
7. If international cooperation can go ahead, check the following next steps:
    a. When appointing a **new employee**, the HR adviser should be involved;
    b. When drafting a **contract**, contact Legal@vu.nl;
    c. When receiving **foreign national delegations/visits**, recommendations from the factsheet are followed;
    d. When making an international travel, the following points of attention are important.

If you currently have an international collaboration and doubt whether it is permitted, contact the department's MT[3] and the Managing Director immediately.

If you have already contacted the VU Knowledge Security Advisory Group yourself, also inform the faculty Knowledge Security contacts and the department MT of the case.

Knowledge Security Framework

When entering into new international collaborations, such as the appointment of a new employee, collaboration with an institution or contracts with a client or funder in the field of research, education or business operations, the 6 questions below are leading:

To go through the 6 questions, you can also consult the Flowchart Knowledge Security. Below is a summary of the VU Amsterdam Knowledge Security Framework with more detailed explanatory notes on the flowchart:

Legal Framework: Is it legally permissible?

1. **Is the person, company, organisation or country you want to collaborate with on the**

[3] For an overview of HR-advisors and department managers for each department see here.

EU or UN sanctions list?
Collaborating with persons, companies, organisations or countries that appear on the EU or UN sanctions list is illegal.

- Any partnerships with Iran and North Korea should always be checked through the EU sanctionlist. Country information can also be found on the following government website: Countries and regions (rvo.nl).
- See here for instruction on how to perform the sanction list check.
- As for China, there are no formal restrictions on cooperation with scientists, but this may apply to certain institutes and persons who have been associated with them (recently <4 years) (see also question 3).
- Special stipulations apply to Russia/Belarus.
- For hiring new employees, a fact sheet has been prepared with points of attention. This applies to all employees, both with an academic and support job profile, guest appointments and temporary appointments (PhD candidates and postdocs). Involve the HR adviser in this process. They can also provide assistance if required.

2. **Does the research fall under the Dual-Use Regulation?**
    - These are (knowledge of) products, software or technology (see Annex 1 of the Dual-use Regulation) that can have both civilian and military uses.
    - Considerations here are 1) the degree of fundamental scientific research based on the Technology Readiness Level (TRL) and 2) the public accessibility of the (knowledge about) the products, software or technology before the start of the research.
    - For dual-use of research in Life Sciences (e.g. high-risk pathogens), please refer to the specific fact sheet on biosecurity for more information.
    - Turn to page 7 of the VU Amsterdam Knowledge Security Framework for more information.

Risk management: What are the risks?

3. **Is the partner associated with a foreign military organisation outside the EU (over the past 4 years)?**
   Collaboration with foreign military organizations outside the EU is highly undesirable. The same applies to institutions with ties to foreign militaries outside the EU. Screen people's CVs to see if they have any relevant affiliations (indirect or otherwise).
   For China, research institutes with strong ties to the Chinese military should be avoided (especially the so-called 'Seven Sons'). For these institutes, the 'ASPI list' can be consulted (ASPI unitracker). This list contains information not only about the institutes, but also about specific labs within them.
   Keep in mind that an institute itself may be at medium risk, but a specific laboratory within it may be at (very) high risk. The following principles apply to the risk levels:
    - Very high risk – collaborations are highly undesirable
    - High risk – avoid dual-use research, keep your distance from defence-related research departments, avoid sensitive research areas
    - Medium risk – keep your distance from defencerelated research departments, avoid sensitive research areas
    - Low risk – avoid sensitive research areas
4. **Does the collaboration involve sensitive research?**
    - An overview with key enabling technologies can be find here.
    - If digital products are involved, also consult the factsheet 'Grapperhaus criteria for tenders'
    - Cooperation on sensitive research is undesirable with high-risk countries. Risk can be determined by a combination of the following sources of information:

    - Countries scoring low (<0.4) on the Academic Freedom Index
    - Countries with an increased risk profile according to the EU-sanction list and AIVD threat assessment (Dreigingsbeeld statelijke actoren)
5. **Does the research involve any practices or issues that could potentially be ethically questionable?**
   Examples include the risk of violating human rights or academic values, the misuse of knowledge, the safety of researchers and respondents (for instance if the research might cause them to be pressured or coerced), unintended knowledge transfer, and harm to people, animals or the environment. If a country has a score of 0.4 or less on the Academic Freedom Index, the collaboration should be discussed with the Managing Director.
6. **Is the collaboration, or are incoming employees, funded solely by the partner (unilateral external financing)?**
   VU Amsterdam is cautious when it comes to appointing researchers from countries with a score below 0.4 on the Academic Freedom Index. The following restrictions apply:
   - No scholarship PhD students who come to the university for less than two years and who are supervised from their home country
   - No research involving dual-use items or sensitive research areas
   - No researchers from a partner who falls under the preconditions for Very High Risk of question 3

   Scholarship students selected by the university to do doctoral research on a subject proposed by the university – and who intend to graduate at the VU – may be appointed.

For detailed explanatory notes on the above questions go to pages 7 and 8 VU Knowledge Security Framework.

Additional information

Contacts

- Faculty board:
    - Esther van den Hengel: e.i.v.vanden.hengel@vu.nl
    - Maaike Verbree: m.verbree@vu.nl.
- VU Knowledge Security Advisory Group: kennisveiligheid@vu.nl
- Managementteam (MT) departments[4]
- HR advisor departments[4]
- Legal services VU: legal@vu.nl.

Links

- Knowledge security for VU employees
- Knowledge Security Framework VU
- National contact point Knowledge Security (Landelijk Loket Kennisveiligheid)
- National Knowledge Security guidelines (Nationale leidraad kennisveiligheid)
- An overview of key enabling technologies can be find here

[4] For an overview of HR-advisors and department managers for each department see here.

- Flowchart Knowledge Security with 6 basic questions.
- The comprehensive questionnaire can be found here.