VRIJE
UNIVERSITEIT
AMSTERDAM

VU Amsterdam Knowledge Security Framework

Prepared by the Advisory Group on Knowledge Security

Introduction

The practice of science would be impossible without international collaboration, and Dutch knowledge institutions enjoy a good reputation worldwide for their commitment to academic freedom, integrity and transparency.

But besides opportunities, international collaboration also entails risks. Global power shifts are taking place in which geopolitics, security and economics are interwoven, with countries viewing knowledge and innovation as sources of power. To ensure that international collaborations take place as securely as possible, VU Amsterdam has developed a knowledge security policy in accordance with the applicable legislation. Recently, there has been a growing awareness of the fact that collaborations are not always desirable, even if they do not violate any laws or regulations. This is also addressed in the policy.

The present document marks a major step towards a more comprehensive approach to knowledge security at VU Amsterdam. The Knowledge Security Framework is based on the National Knowledge Security Guidelines. It serves as a support tool for discussions on knowledge security and can help inform decisions on whether or not to enter into or continue a collaboration with an individual, institution, funder or client. The framework's questions must be answered before starting or renewing any collaboration. By systematically examining the various aspects of a collaboration and assessing the security risks involved, a well-founded, well-documented and replicable decision can be made. Strategic considerations may play a role as well. The framework was created with the various academic disciplines practised at VU Amsterdam in mind. Besides knowledge security, ethical considerations are also important when it comes to collaborations. That is why VU Amsterdam is currently working on policy in this area too. As this becomes more concrete, we will strive to align it with the knowledge security policy, while also considering other perspectives and interests. The Knowledge Security Framework can be used to complement existing partnership processes within the faculties.

The faculties, Executive Board and the Knowledge Security programme were involved in the choices that were made regarding the framework's process, decision-making and support. These choices are explained in Section 2.2. The framework has been adopted by the Executive Board and takes effect from 1 September 2023. It applies to every person, faculty, service department and institution associated with VU Amsterdam. This means that the framework's questions, listed in Section 2.2, will need to be answered before a collaboration can be entered into or renewed.

VU Amsterdam's Advisory Group on Knowledge Security was set up by the Executive Board to develop policy and provide advice. It reports directly to the Rector Magnificus. This document offers a first set of guidelines for the practical implementation of the knowledge security policy developed by the advisory group. Section 1 briefly describes what knowledge security is, and Section 2 details how VU Amsterdam currently promotes knowledge security. Section 3 sets out the steps that must be taken to ensure that the envisaged knowledge security process outlined in Section 2 becomes standing practice, listing the topics and developments that will require attention from the faculties and service departments in the coming period. The aim is to achieve integrated processes and more detailed policies, for example by developing a portal that brings together all the relevant information and collaboration checklists in one place. For now, information on knowledge security is available on vu.nl. This framework will be updated as circumstances demand.

1. Knowledge security

Good-quality higher education and science cannot exist without international cooperation and talented academics from all over the world. Knowledge security is about recognising relevant risks to ensure that these kinds of international collaborations can take place as safely as possible, with due regard for the core values academic freedom and scientific integrity.

Knowledge security is based around three facets. First, the goal is to prevent the undesirable transfer of sensitive[1] knowledge and technology. Transfer is undesirable if it affects national security, such as in cases where research results can be used for military applications. Naturally, VU Amsterdam strives to comply with all national legislation in this area. Second, knowledge security is about protecting education and research from state actors seeking to exert covert influence, as such interference could be harmful to academic freedom and social safety. Finally, knowledge security also concerns ethical issues that could arise over the course of collaborations with countries that do not respect fundamental human rights. With regard to the latter two aspects, the risks and opportunities associated with a collaboration should be assessed on a case-by-case basis. The aim is to foster a culture in which VU Amsterdam employees discuss the desirability of collaborations and the prevention of unwanted use of the university's research, knowledge and technology.

VU Amsterdam recognises the possible risks associated with international collaborations and seeks to apply a balanced approach in limiting these to prevent any undesired consequences. With this in mind, a framework has been drawn up for identifying the risks and opportunities associated with collaborations that also provides scope to assess collaborations on a case-by-case basis. Our aim is to prevent stigmatisation and discrimination, and to avoid the implementation of strict rules that would make it impossible to collaborate with certain countries, despite there being no legal reasons for not doing so. Also, the competitive position of VU Amsterdam is taken into account. Implementing this framework will not always be easy, and we will undoubtedly face a number of obstacles along the way. The assessment process for collaborations was designed to be clear, flexible and easy to apply. Supporting researchers and departments to quickly find out whether a collaboration might be feasible and, if it turns out that this is not the case, why the collaboration would be ill-advised. Knowledge security is not a static concept: changing geopolitical relations can affect how existing and prospective collaborations are viewed. Higher education institutions are currently under pressure from both the government and society at large to be more vigilant when it comes to knowledge security, which may lead to further developments moving forward.

[1] See question 4 in the framework for more information.

2. Implementation of knowledge security at VU Amsterdam

Knowledge security policy has an impact on the entire university and is therefore a shared responsibility within the university. International collaborations often start informally, between academics.

Sometimes these collaborations grow into something bigger, drawing in more colleagues, departments and even institutions, thereby acquiring a formal character. VU Amsterdam's knowledge security framework was designed to be accessible and easy to use, offering guidelines for identifying and responding to potential risks to the university's research, teaching and operations. Staff can use the framework to assess the desirability of a study or collaboration with regard to potential unethical consequences and national security threats.

2.1 VU Amsterdam Knowledge Security Framework

UNL members are working closely together to further develop tools to help researchers and other relevant staff, such as contract managers and knowledge security advisors, when entering into, navigating or evaluating international collaborations. These tools include guidelines for every phase of a collaboration: due diligence and selection (Phase 1), the negotiations (Phase 2), the collaboration itself (Phase 3) and the evaluation (Phase 4). They are available here.
The questions and areas of focus with regard to knowledge security have been translated into seven steps. Where appropriate, faculties may add additional questions and information for internal use, for example from a research code of ethics. Although the framework focuses mainly on research, it also provides steps for the service departments and faculties, for example for hiring support staff.

Legal framework – Is it legally permissible?

1. Is the person, company, organisation or country you want to collaborate with on the EU or UN sanctions list?

Collaborating with persons, companies, organisations or countries that appear on the EU or UN sanctions list is illegal. Specific technologies may also be subject to sanctions against certain countries. Screen people's CVs for any affiliations (direct or indirect) to organisations that appear on the EU or UN sanctions list (see EU Sanctions Map). If the person in question has been associated with a sanctioned organisation in the past four years, you should discuss this with your HR adviser and/or your manager.

2. Does the research fall under the Dual-Use Regulation?

If your research involves dual-use products, software or technology, it can only go ahead if Customs' Central Import and Export Office (CDIU) issues a licence.
The following questions are relevant in this context:

a. Dual-use?

- Does you research involve (knowledge about) products, software or technology that **could** be used for military purposes? This includes (knowledge about) products, software and technology that could be used for the design, development, production or use of nuclear, chemical or biological weapons or their delivery systems.
- If the answer is yes, go to question 2b.
- If the answer is no, the Dual-Use Regulation does not apply, go to question 3.

Please note: Annex 1 to the Dual-use Regulation provides **a non-exhaustive** list of dual-use goods (products, software or technology).

b. Fundamental scientific research?

- Does your study involve *fundamental* scientific research?
- Fundamental scientific research is experimental or theoretical work aimed primarily at gaining new knowledge about the fundamental principles of phenomena or observable facts, and is **not** intended to serve a specific practical aim or purpose.
- If the answer is yes, you do not require a licence, go to question 3.
- If the answer is no, go to question 2c.

Please note: the higher the Technology Readiness Level (TRL), the less likely it is that the study qualifies as fundamental scientific research.

c. Publicly accessible?

- Is the (knowledge about) products, software or technology publicly accessible?
- Publicly accessible means that the products, software or technology are available to anyone, with no restrictions on further dissemination.
- If the answer is yes, you do not require a licence, go to question 3.
- If the answers is no, it is highly likely that a licence is required. Contact Institutional and Legal Affairs (BJZ) at kennisveiligheid@vu.nl.

Please note: products, software and technology are not considered publicly accessible if the knowledge involved will be made available after the research has been concluded. The fact that your research results will *eventually* be published is **not** relevant in this context.

If you have any questions or doubts, contact Institutional and Legal Affairs at kennisveiligheid@vu.nl.

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). If in the past four years the person in question has been associated with an institution with ties to a foreign military organization outside the EU (other than as a BSc or MSc student), the collaboration cannot go ahead. The ASPI Uni Tracker offers a list of universities and their ties to the Chinese military. Collaborations with universities labelled as *Military* or *National defence* are highly undesirable. The guidelines per risk rating are listed below. Deviations are only allowed with approval from the authorised signatory (managing director of the faculty or director of service department).

- **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 defence-related research departments, avoid sensitive research areas
- **Low risk** – avoid sensitive research areas

4. Does the collaboration involve sensitive research?

This concerns key technologies[2] and Emerging Technologies[3]: these are technologies regarded by the Dutch government as having military, economic and geopolitical strategic value. Collaborations with high-risk countries[4] involving these technologies are generally undesirable.

Does the collaboration involve a sensitive knowledge area and a partner from a country with an elevated risk profile (these are countries on the EU sanctions list; see the threat assessment)? No two situations are the same, and you are advised to involve the Advisory Group on Knowledge Security, via kennisveiligheid@vu.nl. In some cases, collaboration may not be possible, even with a sound contract. This is the case if the residual risks are not acceptable to the relevant risk owner (the service department, faculty or Executive Board).

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[5], the collaboration should be discussed with the authorised signatory (managing director of the faculty or director of service department), who may choose to appoint a contact person to process reports related to knowledge security issues.

6. Is the collaboration, or are incoming employees, funded solely by the partner (unilateral external financing)?

Carry out due diligence (see vu.nl). Also, ask yourself what possible reasons the partner may have for financing the research or the individuals involved, and what possible risks this one-sided funding entails. This includes self-funded researchers. 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.

[2] Key technologies: the government is expected to produce an assessment framework for these. An overview of key technologies is provided in Appendix 1.

[3] Emerging technologies: a VU Amsterdam webpage on this topic will be launched in 2023.

[4] High-risk countries: countries with a low score on the Academic Freedom Index and/or Rule of Law Index, supplemented where necessary with information from the threat assessment drawn up by the General Intelligence and Security Service (AIVD).

[5] In the future, this may be extended to include ethical considerations. To answer this question, faculties can use any relevant information, including information that is being used in the assessment by the faculty's ethics committee.

No obstacle – The collaboration can go ahead

7. There are no obstacles to collaboration
Before starting an international collaboration, it is still advisable to take a look at the Partnering Tools. These offer tips for every phase of a collaboration: introductions, contracts, implementation and evaluation. The due diligence page on vu.nl can also be useful.

2.2 Explanation of the framework

The VU Amsterdam Knowledge Security Framework, as set out above, offers employees better insight and understanding of the possible security risks involved in an intended collaboration. It focuses on collaborations involving contracts between VU Amsterdam and another institution, funder or client, as well as on situations where individuals enter into a relationship with VU Amsterdam (hospitality, external PhD students, joining a graduate school). The basic checklist above should be completed for all prospective collaborations. If the answer to every question is no, no further action is required.

The framework's first two questions are related to legislation. If the answer to the first question is 'yes', the collaboration cannot go ahead. If the second question is answered 'yes', an export licence may be required. For further details, please contact kennisveiligheid@vu.nl.

Questions 3 to 6 focus on collaborations that do not violate any laws, but may still require further investigation for knowledge security reasons. If any of these questions are answered 'yes', the collaboration could involve certain risks. If this is the case, or if there are ambiguities, the employee in question must inform their direct manager and the manager with decision-making authority (director of operations or director of service department). The supervisor with decision-making authority can appoint a contact person for knowledge security issues to process these reports; the faculties and service departments are free to design this process themselves. After the supervisor with decision-making authority or the knowledge security contact person has been informed, they will discuss the initial risk assessment with the employee. This is followed by a risk management procedure using a more comprehensive questionnaire (see Appendix 2), aimed at identifying and assessing risks. The completed questionnaire will be kept on file for future reference. The probability of any unintended effects, the magnitude of the potential impact and risk-mitigation measures are also considered, as are any opportunities the collaboration might offer VU Amsterdam.

If a faculty or service department has a knowledge security contact person, they issue a substantiated advice to the supervisor with decision-making authority (managing director of the faculty or director of service department). This supervisor then decides whether the collaboration can go ahead, observing the limits set out in the procuration scheme (adopted in January 2021), or they ask the Executive Board to take a decision. If the collaboration does go ahead, the faculty or service department continues to monitor relevant risks.

If there are doubts, the managing director, the service department director or the Executive Board can ask the Advisory Group on Knowledge Security for advice before making a final decision. The Advisory Group on Knowledge Security is informed in a timely manner by the party asking for advice if the final decision differs from its recommendation.

If necessary, the Advisory Group on Knowledge Security can seek advice from the National Contact Point for Knowledge Security and use this to inform own recommendation. Bear in mind that this process may take some time, given that the National Contact Point takes an average of 15 working days to issue a recommendation.

In case of a potential knowledge security incident, the researcher concerned informs the director of operations, who then informs the advisory group. If required, the advisory group can help the researcher investigate the incident and decide on an appropriate response. The advisory group must always be consulted before a conclusion is reached and follow-up measures are taken.

3. Follow-up steps

The introduction of the framework is expected to lead to questions from employees, faculties and service departments. As the framework is applied in cases of research on sensitive subjects, we will gain useful experience with the framework. If needed this will lead to amendments of the framework.
VU Amsterdam is taking the necessary action to ensure that the situation envisaged in Section 2 actually materialises.

Risk management: VU Amsterdam is promoting a culture that supports the dialogue on knowledge security. A risk-management process is also being drawn up. And the desirability will be explored of integrating knowledge security into the planning and control cycles between the faculties and service departments and the Executive Board, and between the Executive Board and the Supervisory Board. In addition, a decision needs to be made on how to store the supplementary questionnaires for future reference, to learn from them or in case of an incident.

Linking structures and appointing contact persons at the faculties/service departments: setting up a consultation structure between the Advisory Group on Knowledge Security and the risk management steering group, and appointing knowledge security contact persons at the faculties and service departments. This can also be the director of operations or service department director.
For questions, please contact kennisveiligheid@vu.nl.

Provision of information, awareness and training: many VU Amsterdam employees may be familiar with knowledge security, but do not know what it means exactly or what impact it will have on their work. That is why the university is making sure that its policies on knowledge security are easy to find on its website. The university will also launch a campaign to raise awareness on the subject and offer training courses to employees.

Harmonisation with other VU policies and the line organisation: various aspects of knowledge security are relevant to the work and responsibilities of the line organisation. These aspects are also set out in the government's National Knowledge Security Guidelines. Discussions will be held with those involved on how knowledge security can become a part of their work and which aspects will be handled by new positions and structures. There will be discussions with the ethics committees, HR staff, IT, the International Office and IXA-GO.

Appendix 1: Overview of key technologies

The overview of the key technologies can be found on the knowledge security page on vu.nl under 'VU Knowledge Security Framework'. Due to national developments, this list will be subject to change and the current list can be consulted online.

Before assessing whether a key technology is involved, it is advisable to always consult the most up-to-date list on vu.nl. For more background information, see the NWO Key Technologies page.

Appendix 2: comprehensive knowledge security questionnaire

Before filling in the questionnaire below, please indicate which of the framework's six questions you answered yes to or had doubts about.

Question	Answer
1. Is the person, company, organisation or country you want to collaborate with on the EU or UN sanctions list?	
2. Does the research fall under the Dual-Use Regulation?	
3. Has the partner ever been associated with a foreign military organization outside the EU?	
4. Does the collaboration involve sensitive research?	
5. Does the research involve any practices or issues that could potentially be ethically questionable?	
6. Is the collaboration, or are incoming employees, funded solely by the partner?	

The table below lists a number of additional questions about your research and/or collaboration. These questions should be answered if you answered yes to one or more questions in the VU Amsterdam Knowledge Security Framework, or if you have doubts about any of the questions. Answering these additional questions will help us, the VU Advisory Group on Knowledge Security, formulate a well-informed response to your request for advice.

Question about collaboration	Answer[6]
Contact person	
Your supervisor	
Name of collaboration or project title	
When will the collaboration end? (Month and year)	
VU Amsterdam faculty	
Department	
What is your research area?	

What is the name of the institution or organisation you want to collaborate with? If the collaboration only involves one or several individuals, please indicate which institutions or organisations they work for. Please also mention the countries in which the institutions or organisations are located so that we can carry out a sanctions check.	
Describe the subject of the collaboration in three lines	
How would VU Amsterdam benefit from the collaboration? (Is there something unique the university stands to gain?)	
How would the researcher and research group benefit from the collaboration?	
Does the collaboration involve any sensitive research areas? Give a brief description of the research and describe the extent to which the department's key technologies, emerging technologies and crown jewels (see explanation[2] at the bottom of this table) play a role in the research, and how they are used.	
Could the research results or data be used for other (unethical) purposes? Consider questions such as: (1) Could the research results cause harm to humans, animals or the environment (possibly after modification or enhancement)? (2) Could the research results lead to a violation of human rights? (3) What could happen if the research results or data ended up in the wrong hands?	
Who are your prospective partners and what kind of collaboration are you planning to engage in? E.g. project exchange students/academic staff, knowledge network, joint research, etc. Describe the type of collaboration agreement.	
Is the partner associated with a foreign military outside the EU? Do we consider the partner institution trustworthy? Is it involved in the development of technology that could potentially be used for human rights violations or military applications? For Chinese institutions, see: ASPI Uni Tracker. This is a list of Chinese universities and their ties to the Chinese military. It offers information not just about these institutions, but also about specific labs. Bear in mind that medium-risk institutions may have specific labs with a high risk rating.	
Are there sufficient sources available to determine whether the potential partner researcher or institution should raise any red flags? E.g. with regard to human rights, research or affiliation with a military government.	
Does the collaboration present any ethical or moral dilemmas? If so, please give a brief description. Examples include violations of human rights or academic values, the misuse of knowledge, the safety of researchers (for instance if the research might cause them to be pressured or coerced) and unintended knowledge transfer (diversion).	

Is the collaboration, or are incoming employees, funded solely by the partner? This includes self-funded researchers. Also, ask yourself what possible reasons the partner may have for financing the research or the individuals involved, and what possible risks this one-sided funding entails.	
Would the research partner have access to VU Amsterdam's digital or physical research environment? If so, will any restrictions be in place?	
If the research will be conducted at VU lab facilities, briefly describe the type of lab and the techniques you are planning to use. Indicate whether researchers will have access to other studies or set-ups in the lab, and whether these are (or could be) sensitive.	
What other risks are associated with the collaboration?	
What measures have been taken to mitigate these? E.g. limiting access to certain buildings, departments, online environments or information.	
Is there anything else you would like to mention that has not yet been addressed in the questionnaire? List any other relevant issues here.	
Why do the benefits of this collaboration outweigh the risks? Consider: (1) How the collaboration would benefit VU Amsterdam. (2) The risks involved. (3) The consequences of ending the collaboration, both internally (research, teaching, etc.) and externally (relationships with partners, reputation, dissolution of contract, etc.).	

Outcome of discussion

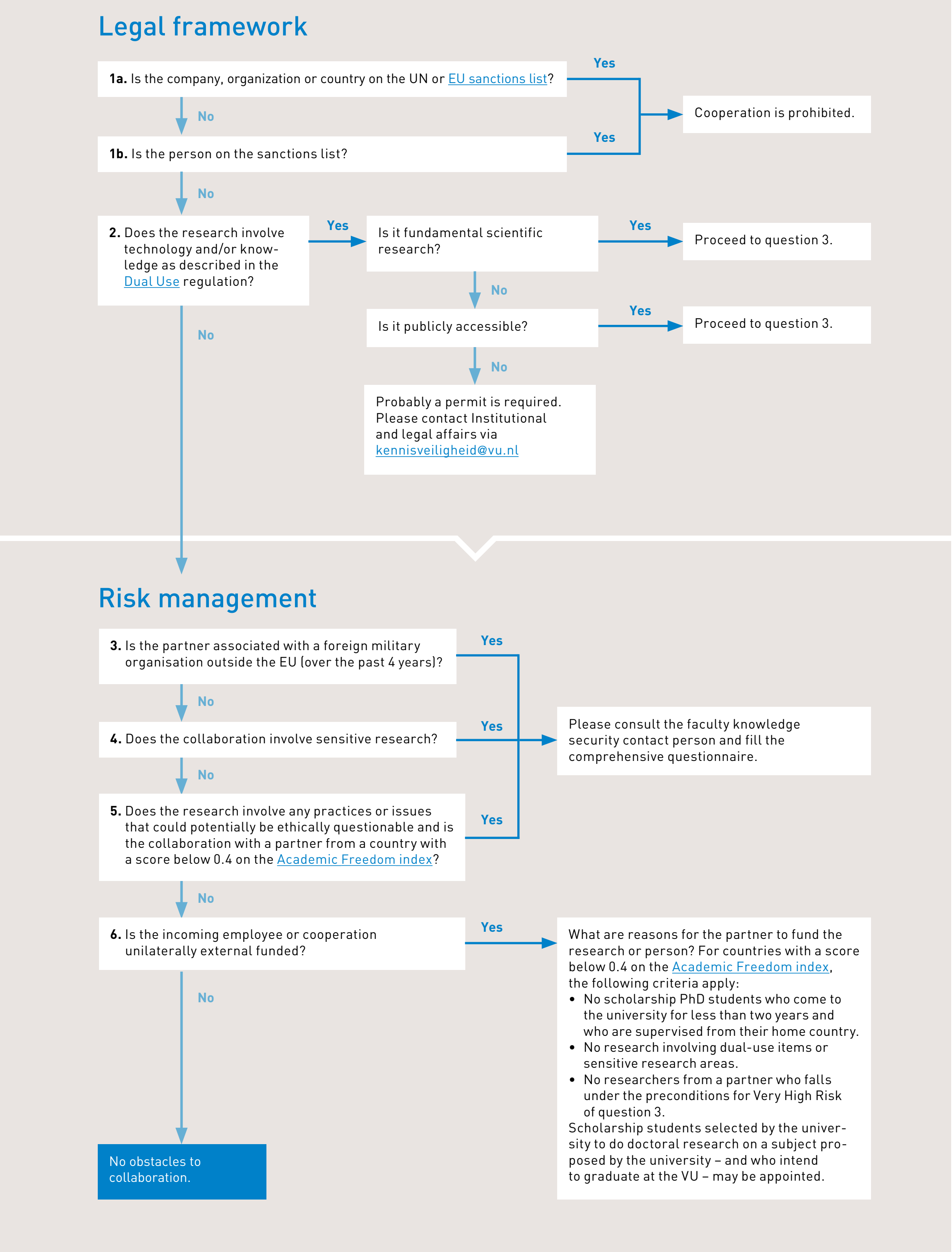
[6] Some information about the collaboration may have already been filled in. You can adjust this where necessary.

[7] For more information on key technologies, emerging technologies and crown jewels, see Appendix 1. TNO's full report on recalibrating key technologies, published in 2023, is available here.

Appendix 3

Is collaboration with and organization or individual permitted and desirable?

Please answer the questions below. **If all questions are answered with 'no', there are no obstacles to collaboration.** It is still advisable to check the Partnering Tools.



Legal framework

1a. Is the company, organization or country on the UN or EU sanctions list?

Yes → Cooperation is prohibited.

No

1b. Is the person on the sanctions list?

Yes → Cooperation is prohibited.

No

2. Does the research involve technology and/or knowledge as described in the Dual Use regulation?

Yes → Is it fundamental scientific research?

Yes → Proceed to question 3.

No → Is it publicly accessible?

Yes → Proceed to question 3.

No → Probably a permit is required. Please contact Institutional and legal affairs via kennisveiligheid@vu.nl

No

Risk management

3. Is the partner associated with a foreign military organisation outside the EU (over the past 4 years)?

Yes

No

4. Does the collaboration involve sensitive research?

Yes

No

5. Does the research involve any practices or issues that could potentially be ethically questionable and is the collaboration with a partner from a country with a score below 0.4 on the Academic Freedom index?

Yes → Please consult the faculty knowledge security contact person and fill the comprehensive questionnaire.

No

6. Is the incoming employee or cooperation unilaterally external funded?

Yes → What are reasons for the partner to fund the research or person? For countries with a score below 0.4 on the Academic Freedom index, the following criteria 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.

No

No obstacles to collaboration.

Colophon
The VU Knowledge Security Framework has been drawn up by the Knowledge Security Advisory Group. For more information about knowledge security and the VU policy for this, see the employee page on knowledge security.

You can contact the advisory group via kennisveiligheid@vu.nl. The faculties' contact persons for knowledge security are listed on the employee page knowledge security. These contact persons within your faculty are generally the first point of contact.

Design
Haagsblauw p.p. VU Designstudio

Photography
Peter Valckx

Version 1.0: 18 July 2023
2073402

VU

VRIJE
UNIVERSITEIT
AMSTERDAM