

This guideline describes **when** the issue of knowledge security (possibly) plays a role and **how** and **who** within the FBMS faculty applies the [Knowledge Security Framework VU](#). In addition, it briefly explains (1) what knowledge security is; (2) how FBMS deals with knowledge security/what is considered desirable; (3) how (process-wise) knowledge security is safeguarded; (4) what conditions need to be met to continue doing this; and (5) which documentation can be consulted.

1. What is knowledge security?

Knowledge security is about the **recognition and knowledge of security risks surrounding international collaboration** with the aim of ensuring that desired international scientific collaboration takes place as safely as possible. The protection of knowledge is a core task of the national government which has drawn up the [National Guide to Knowledge Security](#). This guide helps us as a knowledge institution weigh opportunities and (security) risks against each other and has three goals. It aims to:

1. Prevent unwanted transfer of sensitive knowledge and technology;
2. Prevent covert influencing of education and research by state actors;
3. Form a good picture of ethical issues that may play a role in cooperation with countries and/or institutions that do not share our academic values.

The [Knowledge Security Framework VU](#) describes **what steps are needed** when entering into, extending or evaluating an international collaboration from VU. In some instances, it is necessary to ask critical questions about the background of a partner organisation or client, so that the collaboration can (continue to) take place safely. The application of the framework requires customisation to prevent stigmatisation and/or discrimination.

2. What is the desired culture within FBMS regarding knowledge security?

Within FBMS we frequently collaborate internationally. We do this based on the VU-wide core values of **academic freedom** and **scientific integrity**, as well as our faculty ambition to be able to conduct high-quality interdisciplinary research. Sometimes there are risks associated with an international collaboration that we ideally recognise before the start or continuation of a collaboration. The three facets which guide knowledge security are described in “What is knowledge security?”, but (security) risks rarely present themselves in such a simple way. Therefore, it is important that discussions about the desirability of collaboration and the prevention of undesirable use of research, knowledge or technology are also discussed within the research team, section and/or department before entering into a collaboration or accepting an assignment. The faculty board expects FBMS-employees to:

- Be broadly familiar with the Knowledge Security Framework VU;
- View knowledge security as a shared responsibility that also belongs to the individual employee;
- Use the flowchart included in the framework (see the following paragraph);
- Investigate the background of the foreign partner organisation or client (due diligence);
- Contact the knowledge security contact person within the FBMS if they have questions or doubts (see next paragraph).

3. How do we deal with knowledge security within FBMS?

FBMS follows the [Knowledge Security Framework VU](#) and has a **faculty contact person for knowledge security**: Ravenna Aarnoutse, head of REPS. She is the **first point of contact** for knowledge security and provides support in answering questions about the framework. The framework centers around six questions (the same questions can be found in the [Flowchart Knowledge Security VU](#)) that provide the employee with insight into the possible knowledge security risks of a proposed collaboration. An explanation of the questions can be found in the framework itself (in section 2.2.), the flowchart does not offer this explanation. The questions are focused on the collaborations where a contract is concluded between the VU and an institution, financier, client or where an individual enters into a relationship with the VU (including those in hospitality or external PhD candidates). In addition to the contact person for knowledge security within the faculty, there are two other important 'gatekeepers' where it concerns knowledge security, namely the dean and the director of operations. Ideally, department heads adopt the same critical attitude when a collaboration or contract is being discussed with them.

4. How does scientific collaboration proceed safely?

In principle, the questionnaire should be completed for each international collaboration project and **ideally, the questionnaire should be discussed with the contact person for knowledge security**, even when it is believed that all questions can be answered 'no'. If one of the questions is answered 'yes', this means that there may be a risk which must be addressed. If this is the case, the employee should inform their own supervisor, the director of operations (Martin van Aken) and the contact person for knowledge security (Ravenna Aarnoutse). The latter will discuss the risk assessment with the employee and go through a **risk management process** using an [extensive questionnaire](#). This discussion focuses on the identification and assessment of risks, possible unintended effects (and their impact), as well as measures which can be taken to reduce risks and the opportunities that the collaboration offers the faculty and the VU. The contact person for knowledge security will then prepare a **substantiated advice**, if necessary test this with the Knowledge Security Advisory Group¹, and present this to the director of operations. The latter will bring the decision to be taken in accordance with the limits set in the [proxy arrangement](#) to the Faculty Board where decision-making about the collaboration can take place. The workflow described here is shown in Figure 1.

5. Information available for making the right choices

- [Hiring new employees](#)
- [Academic Freedom Index²](#)
- [Special provisions Russia and Belarus](#)
- [Dual-use Regulation](#)
- [Keep control and avoid dependency](#)
- [International travel](#)
- [Receiving foreign delegations](#)

¹ The Knowledge Security Advisory Group is the central contact point where faculties and services can go with questions about knowledge security. It can seek advice from the [National Knowledge Security Desk](#) and use this advice in the advice to the person seeking advice.

² Consult when there is a risk of violating human rights or academic values. With a country score of 0.4 or lower or the AFI, the proposed collaboration must be discussed with the knowledge security contact person.

- [EU Sanctions List](#) and [search in sanctions list](#)
- [Key technologies](#)
- [Knowledge security for VU employees](#)
- [NWO Key Technologies](#)
- [NWO Sleuteltechnologieën](#)

Figure 1 (Flowchart application knowledge security framework within FBMS)

