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, and/or the knowledge security contact person to formulate a well-informed response to your request for advice.

|  |  |
| --- | --- |
| **Question about collaboration** | **Answer1)** |
| **Contact person** |  |
| **Your supervisor** |  |
| **Name of collaboration or project title** |  |
| **When will the collaboration end? (Month and year)** |  |
| **Faculty of the VU** |  |
| **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 explanation2 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](https://unitracker.aspi.org.au/). 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. |  |
| **Will 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**

|  |
| --- |
|  |

1) Some information about the collaboration may have already been filled in. You can adjust this where necessary.

2) For more information on key technologies, emerging technologies and crown jewels, see Appendix 1 of the Knowledge Security Framework VU. TNO’s full report on recalibrating key technologies, published in 2023, is available [here](https://www.nwo.nl/en/key-enabling-technologies).