

Name of principal investigator:	
Application/project number:	
Date:	

Research security assessment and risk management plan

Identifying and evaluating the risks related to research security and presenting an adequate risk management plan are prerequisites for the granting of funding. An insufficient risk assessment or risk management plan may lead to an application being inadmissible or rejected.

For funded projects, the appendix must be refilled and submitted to the RCF in accordance with the standard terms for funding, if changes during the project change the previous assessment of research security in the project. Failure to notify the changes may result in suspension of payment and recovery of funds.

Before completing this appendix, please read the instructions on the RCF website: [Research security](#) and [self-assessment of research security](#). If you need help filling in the appendix, please primarily contact the support services at your own organisation.

The appendix has two parts:

- A) Research security self-assessment: Answer all questions 1–4.
- B) Description of risk factors and risk management plan: Explain your answer to the questions under section A. For the risks identified, please answer questions 1–3.

Save the appendix in PDF format. Do not print to PDF as this makes it more difficult to process the appendix. Name the appendix as follows: **research security_application/project number_year_yoursurname.pdf**.

A) Research security self-assessment

1. Are there any collaborators (individuals or organisations) involved in the project that cause security risks? Based on your background analysis, is there any reason to suspect, for example, cooperation with or ties to (significant funding, affiliations) the armed forces or governments of non-EU countries in a way that would jeopardise research security?	☐ Yes ☐ No
2. Does the project fall within the critical technology sector? - See Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States (PDF). - Answer “Yes” if critical technologies are being developed or utilised in the project or if critical technologies are mentioned in the application, regardless of whether you believe this poses risks to research security. - Answer “Yes” if the project represents fundamental research in these areas, and describe it in section B.	☐ Yes ☐ No
3. Do the results and outputs of the project have dual-use potential, or does the project use equipment with dual-use potential?	☐ Yes ☐ No

• Dual use means suitability for military purposes in addition to normal civilian use. See, for example, the EU Commission recommendation on research involving dual-use items. • Answer “Yes” if the results of your project can be used for military purposes, regardless of whether, in your view, this poses risks to research security. • Answer “Yes” if the data you collect or use has dual-use potential. • Answer “Yes” if the project represents fundamental research in these areas, and describe it in section B.	
4. Are there any other identifiable risks related to research security in the project? For example, risks related to the following aspects: • limiting academic freedom (e.g. self-censorship, politically sensitive topics) or influencing politics through research (e.g. spreading disinformation) • using research results and outputs in a way that restricts fundamental rights (e.g. for purposes prohibited by the EU regulation on artificial intelligence) or contrary to EU values • the undesirable transfer of data belonging to special categories of personal data (e.g. health data, political opinion) or sensitive data (e.g. critical infrastructure, security of supply, genetic data) in a way that jeopardises research security.	☐ Yes ☐ No

B) Description of risk factors and risk management plan

Explain your “No” answer to the questions in section A. Briefly justify your position if you consider that there are no risks concerning research security, especially if critical technologies or dual-use technologies are mentioned in the application or if the project involved collaborators from countries where the government seeks to influence research and the subject is politically sensitive.

Please answer questions 1–3 for the risks you have identified.

- 1) Describe the risks you have identified for the security of the research.
- 2) Assess the effects of the risks (how significant the consequences of the risk materialising would be) and their probability (how likely the risk is to materialise).
- 3) Present a risk management plan describing the risk management measures (how risks are prevented, reduced or managed) and how the risks are monitored (the risks and the circumstances affecting them are not permanent, i.e., how possible changes are monitored).

