

**ask &
apply**



Suomen Akatemia
Finlands Akademi
Research Council of Finland

Research Security

Katrine Mahlamäki 30.9.2025



**Internationalization is not an option for
Finland but a necessity.**

At the Research Council of Finland, we
have an important task to connect our top
experts with international networks.

Together, we can make Finland an
attractive country for science.

At the same time, we must recognize the
risks posed to us by the global operating
environment.



Paula Eerola

President, RCF

Context

- Openness, academic freedom and international cooperation are essential for excellent research.
- But increasing geopolitical tensions, hybrid threats, risks of misuse of research and technology, and influence by third countries create vulnerabilities.
- Our aim is to support researchers in addressing those risks while preserving values such as openness, ethics, and autonomy.

Key definitions

- Research security: Anticipating and managing risks from
 - the transfer of critical knowledge or technology that may affect EU or national security;
 - malign influence (e.g., disinformation, self-censorship);
 - ethical or integrity violations undermining EU values.
- Critical knowledge and technology:
 - Emerging or disruptive technologies and domains important for economic competitiveness, social welfare and security;
 - dual-use potential included.
- Risk appraisal: evaluation of several risk-factors (organisation, partner country, domain, etc.) to determine risk level.

Principles for Responsible Internationalisation

- Academic freedom and institutional autonomy
- Openness + security — “as open as possible, as closed as necessary”
- Proportionality: measures should avoid undue burden
- Safeguard economic and national security, values and integrity; avoid protectionism or political misuse of research
- Self-governance by research institutions; policies should be country-agnostic and avoid discrimination or stigmatisation.

Division of responsibilities

- Research funding organisations:
 - Integrate research security into application process (risk profiling, due diligence)
- Research performing organisations:
 - Internal risk management, due diligence, protecting sensitive infrastructure and data; build cybersecurity and culture of security.
 - Transparent disclosure of funding sources and affiliations; avoid conflicts of interest and foreign dependencies.

We must balance freedom, responsibility, and risk management

Academic freedom is upheld

- All research topics remain permitted.

We share a common responsibility

- The researcher, their host organization, and we as the funder are jointly responsible, but the main responsibility lies with the researcher's own organization.

Our task is to identify and manage risks

- Funding may be withdrawn if risk identification and management fail.



The role of Research Council of Finland in strengthening research security

We will incorporate risk assessment related to security threats into the funding process.

Going forward, we will consider research security in:

- - our funding process
- - funding terms and conditions
- - our own international cooperation.

Our actions are based on information provided by the applicants and their host institutions.



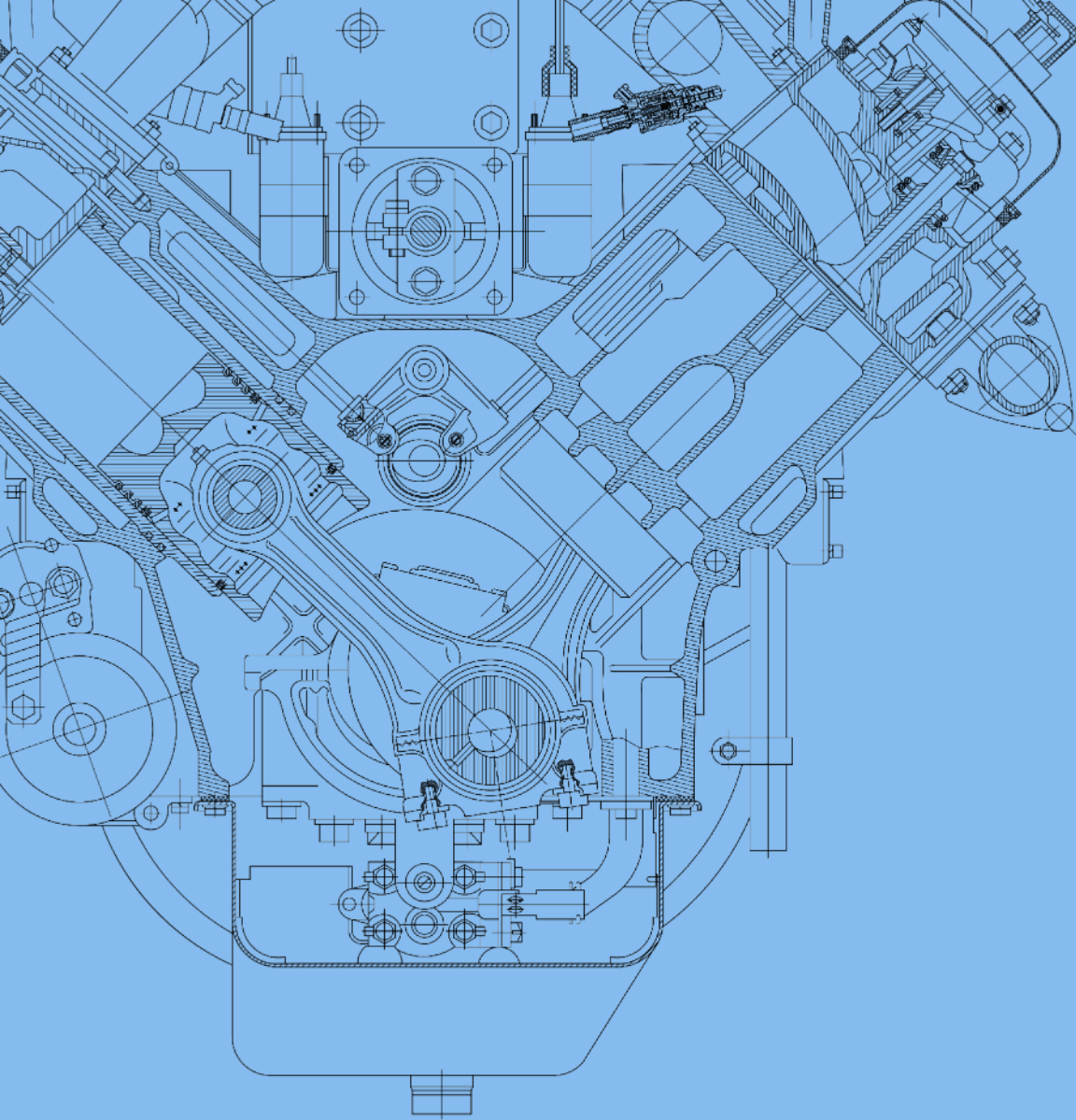
International cooperation is vital for Finland

- International engagement enhances the quality of research and generates new scientific questions, and research fields.
- Our funding instruments are designed to enable international cooperation in its various forms.
- In addition, the Research Council of Finland supports and funds international collaboration with its international partners at the European, Nordic, and global levels.

Legal requirement

The amendment of the Act on the Research Council of Finland

- When carrying out the tasks, the Research Council of Finland shall ensure that **research security** and the **risks related to research projects, research collaboration, and the exploitation of research results** are appropriately taken into account.
- In safeguarding research security, a researcher's right to choose their research topic and methods may not be restricted.



Research
security in our
funding process

Procedure

- Applicants are required to conduct a research security assessment as part of the application.
 - A self-assessment and, if necessary, a risk management plan must be submitted as a mandatory attachment to the application.
 - The site of research confirms that security risks and their management have been adequately addressed in the application.
- A sufficient security assessment and, if applicable, a risk management plan are prerequisites for funding approval.
 - An inadequate plan may result in the application not being processed.
 - The decision-maker determines, on a case-by-case basis, what constitutes an acceptable level of risk.
- Changes during the project, such as new collaborators, must be assessed
 - If risks related to research security arise, they must be notified to the Research Council of Finland.
 - Failure to notify the RCF of changes may lead to suspension of payments or recovery of funds.

It's new to all of us!

- In Winter Call 2026, we will ask for clarifications if your security assessment or risk management plan are not sufficient – your application will not be disqualified because of this
 - However, failing to respond to our request may result in your application not being processed or funding denied

Self assessment and risk management plan

A) Research security self-assessment:

- Each applicant must fill in this section.
- Answer all questions 1–4.
- Please note that answering “Yes” does not prevent you from receiving funding!

B) Risk management plan:

- Applicant must fill in this section, if the answer to one or more questions in section A is “Yes”.
- Answer all questions 1–3

1. Collaborator

- Researchers must be familiar with their international collaborators and the risks involved in the cooperation. Are there any collaborators (individuals or organisations) involved in the project that increase security risks?
 - Based on your background check, is there reason to suspect, for example, cooperation with the armed forces or governments of countries outside the EU in a manner that jeopardises research security?
- Please note that cooperation is not possible if sanctions are imposed on the collaborator.

2. Critical technologies

- Does the project presented in the application fall within the area of critical technology?
 - See Critical technology areas for the EU's economic security.
- Please note that the RCF may fund research in the area of critical technology if the risks involved have been adequately taken into account.

3. Dual use

- Do the results of the project presented in the application have dual-use potential, or does the project use equipment with dual-use potential?
 - Dual use means suitability for military purposes in addition to normal civilian use.
 - See, for example, EU Commission recommendation on research involving dual-use items.
 - Please note that the RCF may fund research with dual-use potential if the risks involved have been adequately taken into account.

4. Other risks

- Are there any other identifiable risks related to research security in the application? For example, risk related to the following aspects:
 - restricting academic freedom, or political influence
 - using research results in a way that restricts fundamental rights
 - sensitive personal data or large datasets
 - respect for the rule of law or the protection of human rights in the collaborator country.

Risk management plan

If you answered “Yes” to one or more of the questions in section A, provide answers to the three points below for each risk identified in your self-assessment.

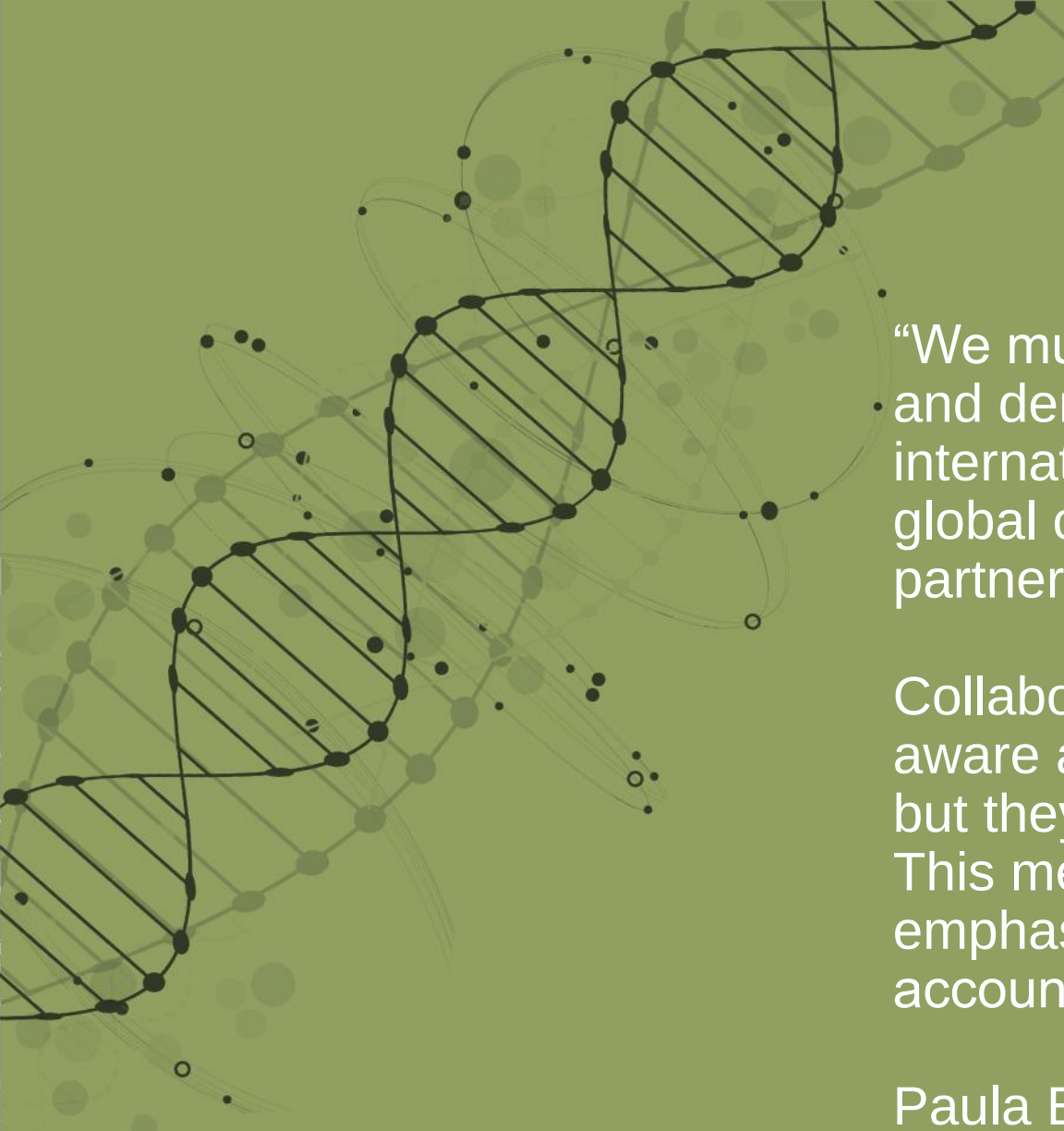
1. Briefly describe the risks involved (e.g. whether research linked to these categories involves the transfer of information within or outside the EU).
2. Assess the effects of the risks (how significant the consequences of the risk materializing would be) and their probability (how likely the risk is to materialize).
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., what kind of procedures are in place to monitor possible changes)



Need assistance?

Help needed!

- Contact the support services at your own organization
 - Your own organization knows the context of your research, the risk management practices at your organization etc.
- RCF can be contacted for general questions
 - We can't give guidance on the contents of your assessment, whether your assessment is sufficient, or whether a collaborator is risky etc.
 - Please use the questions and feedback form on our web page



“We must uphold our values, such as the rule of law and democracy, while also being able to engage in international research collaboration in order to address global challenges — even in cooperation with difficult partners.

Collaboration with challenging partners requires a risk-aware approach. Risks cannot be entirely eliminated, but they can be managed.

This means pursuing value-based cooperation that emphasizes transparency while also taking risks into account.”

Paula Eerola, president, RCF

**ask &
apply**