Guidelines for international research and innovation cooperation

Committee on guidelines for international research and innovation cooperation

May 2022

Published by The Ministry of Higher Education and Science on behalf of the Committee on guidelines for international research and innovation cooperation
Børsgade 4
POB 21351015 København K
Phone: +45 3392 9700
ufm@ufm.dk
www.ufm.dk

This publication can be downloaded at ufm.dk/publikationer

Guidelines for international research and innovation cooperation

Committee on guidelines for international research and innovation cooperation

Contents

Foreword 6

Summary 10

Identify and protect your vital research 13

Know the value and potential of your research 13
Protect your knowledge and results 14
Familiarize yourself with export control rules and the Investment Screening Act 16

Get to know your cooperative partners 18

Check out who you are cooperating with 18
Ask yourself why you are collaborating with them 19
Define what you are working with them on 21

Protect your institution, staff and students 23

Be aware of a potential threat 23
Focus on security procedures and systems 24
Protect your employees and students 25

About the committee 28

Foreword

Why is there a need for these guidelines?

Research and innovation are international by nature, and international cooperation is of particular interest to a small, open economy such as that of Denmark. Strong and open bonds forged through international research and innovation provide access to highly specialized research facilities abroad and to the latest knowledge - as well as helping to attract talented researchers to Denmark.

However, the fact is that Danish higher education and research institutions have found that navigating international cooperation in the field of research and innovation has become more complex over the past decade, and that such cooperation is open to serious ethical, economic and security risks. These risks include breaches of the principles of research integrity and responsible research practices, censorship and the restriction of academic freedom, the loss of military or commercial knowledge and the unethical use of technology, including usage in violation of human rights.

The danger of foreign interference is real, and both Danish and foreign intelligence services stress that alien states, to a greater extent than even before, are unlawfully attempting to acquire knowledge, technology and products that are vital to Danish competitiveness, or that may pose a security threat. To complicate matters further, the geopolitical context and the nature of possible threats are constantly changing.

Denmark is not alone in facing these challenges. There is a broad consensus in the EU that international research and innovation cooperation must be placed on a much more strategic footing; we must focus more on our *own interests*, while insisting on *reciprocity* and *transparency*.

Countries that might pose serious risks

International research and innovation cooperation is an integral and important part of modern research practice and comes in all shapes and sizes at different levels. For example, cooperation with international partners may take the form of joint research projects, strategic partnerships, *memoranda of understanding,* actual company contracts, joint publications and institutional visits or exchanges.

International cooperation calls for special caution if the partner's home country is characterized as 'not like-minded', which in this context means a country that violates internationally recognized norms and principles, such as the UN human rights charter, the rule of law, academic freedom and the independence of the individual/institution from the state. In this context, listings in the *Academic Freedom Index, Freedom in the World* or the *World Justice Project Rule of Law Index* may be useful in terms of risk assessment. An aggravating circumstance in not like-minded countries are those cases in which civilian research is not separated from military research (military-civil fusion), because Danish institutions may inadvertently contribute to supporting the military capacity of potentially hostile powers.

It is in the interests of Denmark to maintain and enforce global standards for science. Such a global system is dependent on countries exchanging knowledge and on researchers feeling connected to each other by working within the same criteria and values. Danish institutions are encouraged to promote international standards for good scientific practice, such as *The European Code of Conduct for Research Integrity* and *the Bonn Declaration on Freedom of Scientific Research,* for example, by including references to these standards in international cooperation agreements.

For the above reasons, the Committee on guidelines for international research and innovation cooperation has prepared a number of guidelines for Danish educational and research institutions.

What is the purpose of these guidelines?

These guidelines must help Danish institutions achieve a balanced approach to international cooperation on research and innovation, aiming to reduce ethical, financial and security risks and to protect their own long-term interests within such cooperation.

There is a twofold purpose: To increase staff awareness of the risks possibly posed by international cooperation and to assist institutional management in building up structures and procedures that may help staff navigate international cooperative relations and to make wise choices.

Who are the guidelines for?

The guidelines are intended for the management teams of Danish educational and research institutions. Full implementation of the guidelines will require the involvement of both management and staff, but it is the responsibility of institutional management to make staff aware of the risks that may be involved in international cooperation, and to design structures and procedures that may help them navigate such cooperation.

The Committee expects the management teams of Danish institutions to make use of these guidelines when assessing which international collaborative relationships might make a positive contribution to their research, and spotting those they should keep a careful eye on, or avoid altogether.

The guidelines are also relevant for other actors in the field of research and innovation, including the Danish government-approved Research and Technology Organizations (GTS institutes), Danish regions and companies heavily involved in research.

These guidelines have been prepared by the Committee on guidelines for international research and innovation cooperation.

Useful links

A pamphlet issued by the Ministry of Higher Education and Science and the Danish Security and Intelligence Service: 'Is your research at risk?'

Guidelines issued by the Danish Security and Intelligence Service and the Danish Defence Intelligence Service: 'Assessment of the espionage threat to Denmark' and 'Intelligence outlook 2021'.

The Danish Defence Intelligence Service Centre for Cyber Security: 'The threat of cyber espionage against Danish research and universities'.

The Danish Business Authority on export control and investment screening.

EU list of dual-use items and staff working document for educational and research institutions on to tackling R&I foreign interference.

The EU network EU-KNOC's overview of guidelines from other countries .

Summary

Below is a summary of the specific actions expected to be taken by institutions as a follow-up to the work of the Committee.

Identify and protect your vital research

Know the value and potential of your research

- Institutions should make an overall assessment of the research areas, data, equipment and results that are strategically important to the institution and therefore vulnerable.
- Institutions assess whether these research areas, equipment, data and results are adequately protected, paying special attention to the collaborative relationships entered into in this field.

Protect your knowledge and results

- Institutions should draw up standard agreements for international cooperation, in which the conditions for IPR, the scope of knowledge sharing and the matter of ownership are clearly formulated, and support their staff in enforcing these conditions during and after the project.
- Institutions should heighten their awareness of the relevant terms of the cooperation agreement, and continually monitor the need for further action to protect research.

Familiarize yourself with export control rules and the Investment Screening Act

- Institutions should take the initiative to prepare institution-specific guidelines and/or run workshops or courses about regulations and their implementation, adapted to the specific needs of their institution.
- Institutions should consider establishing working groups or appointing resource persons in specific areas, such as dual-use.

Get to know your cooperative partners

Check out who you are collaborating with

- Institutions should establish procedures for doing complete background checks on international partners, where relevant, and share with each other information about potentially problematic partners.
- Institutions should adopt a critical attitude towards unfamiliar partners and ensure that their staff know how to report any suspicions to the management.

Ask yourself why you are working with them

- Institutions should prepare a questionnaire guide for researchers that can be used to assess the relevance of entering into a particular case of international cooperation.
- Institutions should carefully consider whether the likelihood of added value is greatest with a particular partner under consideration, and whether the cooperation envisaged is based on compatible interests and ensures equality.

Define what you are working with them on

- By default, institutions should consider including positive lists in international cooperation agreements, specifying which technologies, data, equipment, results, etc., they will share or provide access to. Negative lists may also be considered.

Protect your institution, staff and students

Be aware of a potential threat

- Institutions should make staff and students more aware of threats and risks, and advise them on risk avoidance by holding courses, preparing guidelines, arranging briefings, etc., perhaps adapted to the particular department.
- Institutions should do their best to create a culture of awareness throughout the entire organization, including

encouraging employees to participate in the institution's initiatives in this area.

Focus on security procedures and systems

- Institutions should clearly identify chains of command within the organization, establishing clear channels of communication and procedures for handling security.
- Institutions should ensure that staff and students know the standards of correct digital behaviour, show caution when travelling and staying abroad, especially in countries that are not like-minded, and report suspicious communications or behaviour to the management.

Protect your staff and students

- Institutions should review their internal rules for subsidiary employment and shield their employees and students from access to knowledge and critical research areas, etc, that are not necessary for their studies or work, and which foreign states could have an interest in acquiring, accessing or influencing.
- Institutions should have clear procedures for the onboarding of new employees, including a knowledge of current regulations and codes of behaviour, and ensure the constant scrutiny by management of the relevance of staff employment, especially in the case of foreigners.
- Institutions should raise the awareness of staff and students concerning human interaction and financial practices that may lead to foreign interference, and encourage the reporting of such events.

Identify and protect your vital research

Know the value and potential of your research

It is important that institutions:

- *prepare an overall assessment of which research areas, data, equipment and results are strategically important to the institution, and therefore vulnerable.*
- *assess whether these areas, equipment, data and results are adequately protected, and pay extra attention to the collaborative relationships that are entered into this connection.*

It is important that those of you who are on the management team of a research institution have an overview of which research results or areas are strategically important for your institution. For example, it may be that your institution possesses data that is unique and in global demand, or that your research is close to a breakthrough in some field. This is all about identifying particularly valuable and vulnerable areas of research - assets that others might want to seize.

In these areas, it is not only necessary to protect research through patenting and enforcing copyrights, but also by carefully considering who to collaborate internationally with and how to do so. There are in fact numerous cases of foreign researchers unjustifiably trying to gain access to unique data, trade secrets or military know-how, to the detriment of Danish interests.

In our view, foreign state actors are trying to acquire knowledge and illegally steal technology to a greater extent than ever before. In some cases this is for military or un-ethical use, sometimes involving the violation of human rights, in other cases to strengthen their own research capacity and competitiveness at the expense of the Danish.

In practice, it may be difficult to assess what specific research fields or actual research results can potentially be (mis)used for. And the closer

research is to real basic research, the harder it gets. However, even though some particular research is in its early stages, it may still be valuable and worthy of protection. Since the researcher alone can best assess and classify knowledge in a specific field of research, the researcher has a shared responsibility to help management assess the value and potential of their research.

Experience shows that the most vulnerable areas for losing commercial or military know-how are found within the natural sciences, the health sciences and the technical sciences (see also section 1.3.). However, there may also be risks within the social sciences and the humanities, for example, restrictions on academic freedom, censorship and pressure on, or the rewriting of, research results. It is therefore important always to take the actual research as a starting point.

Protect your knowledge and results

It is important that institutions:

- *draw up standard agreements for international cooperation, in which the conditions for IPR, the scope of knowledge sharing and the matter of ownership are clearly formulated, and support their staff in enforcing these conditions during and after the project.*
- *heighten their awareness of the relevant terms of the cooperation agreement, and continually monitor the need for further action to protect research.*

It is not always the case that you and your international partners have the same reasons for cooperating.

While your interest may be academic or research-related, your international partner may be interested in:

- research leading to a future commercial or patentable result;
- sensitive data or personally identifiable information such as genetic information or commercial test data;
- a potential military application of the research;
- a potential basis for international strategic policy negotiations or decisions;
- using laboratory equipment within a sensitive research area that the partner would not otherwise have access to.

So, when you start up an international cooperative venture, you should decide from the outset how you want to handle and protect the knowledge you bring with you, what you are willing to share and who is to own the results you help to generate. Your level of risk management must increase to match the level of technology development and money involved, and the number of staff exchanges entailed by the collaborative venture.

If you do not adopt a clear position on this, you run the risk of not being able to:

- apply your knowledge and test your ideas in a safe way;
- prove your ownership;
- benefit from a possible commercialization of the results;
- prevent or deter unwanted use of your knowledge and results.

Specifically, the above points should be included in your cooperation agreement with the international partner. This can be done, for example, by making a list of the scientific studies, methods, materials, etc. that you bring into the collaboration, while at the same time examining what the position is on these matters in terms of intellectual property rights (IPR), such as patents, licensing agreements and copyright.

It may also be appropriate in cooperation agreements to include a reference to common academic values, such as *The European Code of Conduct for Research Integrity* and *the Bonn Declaration on Freedom of Scientific Research.* This is not only relevant for IPR. Prior to entering into a cooperation agreement on a joint research project, you may need to enter into a separate non-disclosure agreement (NDA) to discourage your international partner from misusing or disclosing key information.

A good cooperation agreement can never fully protect you against theft, espionage and abuse, but it sends a clear signal to international partners that you are aware of your rights and ready to enforce them. It can help prevent and deter attempts at unwanted transfer and/or use of your knowledge and results.

To facilitate the work and standardize your institutional approach to these matters, you should provide a standard contract that your staff can use as a starting point. Not all forms of cooperation require a cooperation agreement to be drawn up, and the scope of agreements

varies according to the type and formality of the cooperation. This is best assessed by you.

When collaborating with foreign research institutions, you should also be aware that individual institutions and countries may have different rules concerning the ownership of research results. Be sure to clarify this before starting the cooperative venture. Does the institution or the individual researcher own the results? Who is allowed to access the results afterwards and to what extent?

Familiarize yourself with export control rules and the Investment Screening Act

It is important that institutions:

- take the initiative to prepare institution-specific guidelines and/or run workshops or courses about regulations and their implementation, adapted to the specific needs of their institution.
- *consider establishing working groups or appointing resource persons in specific areas, such as dual-use*.

Military or unethical uses of technology and research results are key risk areas in international cooperation. On the other hand, these are highly regulated risk areas, and it is therefore important that you familiarize yourself in particular with the export control rules and the Investment Screening Act.

The export control regime calls for controls on exports and technical assistance in connection with a number of items and technologies that can be used for both civil and military purposes (dual-use). For example, the rules require authorization for exports of dual-use items and technologies outside the EU, but also within the EU for certain particularly critical products.

Export controls also include a prohibition on providing technical assistance related to dual-use items, if there is a risk that they could be used for weapons of mass destruction. Technical assistance may, for example, take the form of lectures, training or consultancy, so that knowledge and academic activities may therefore be subject to export controls.

Joint ventures for research and development connected with the defence sector, IT security, critical technology, or critical infrastructure are covered by the Investment Screening Act. This means that agreements in the areas mentioned between a foreign investor and Danish research institutions require authorization from the Danish Business Authority.

According to the Investment Screening Act, critical technology includes:

- artificial intelligence and machine learning for autonomous vehicles, the imitation of humans, the analysis of positioning data and biometric identification;
- advanced industrial robot technology designed for production robots or use in the healthcare sector, as well as advanced drone technology;
- semiconductors for use in integrated circuits, including technologies that support their production;
- cyber and information security protection technologies concerning the availability, integrity or confidentiality of IT systems, as well as defence against cyber attacks.
- space technology for launching satellites, persons and other payloads, and the supporting communications technology;
- technologies related to industrial energy storage, energy conversion and energy transport;
- quantum technology in connection with quantum computers, quantum sensors, quantum cryptography and quantum communication;
- nuclear technology, excluding products for use in the healthcare sector;
- nanotechnology , including advanced graphene materials;
- biotechnology in synthetic biology; and,
- 3D printing for the manufacture of components for industrial use.

As there may be difficulties when implementing the export control regime and the Investment Screening Act in the field of research, you will need to address the issue specifically. This can be done, for example, by providing guidelines and checklists and by organising workshops or training courses. You should also consider setting up a dual-use working group or appointing resource persons in specific subject areas.

Get to know your cooperative partners

Check out who you are cooperating with

It is important that institutions:

- establish procedures for doing complete background checks on international partners, where relevant, and share with other Danish institutions information about potentially problematic partners.
- adopt a critical attitude towards unfamiliar partners and ensure that their staff know how to report any suspicions to the management.

For the same reason that companies use due diligence investigations in connection with business transfers and mergers, you should only enter into cooperation with international partners on an informed basis. This will help you to identify and reduce potential risks in connection with the proposed collaboration.

Such background checks provide a necessary tool for you to assess the scope of the proposed cooperative venture (is there anything you cannot collaborate with the international partner on?), and whether it will add sufficient value to your research (are you going to get enough out of the cooperation?).

Foreign interference can be difficult to discern in international cooperation, so it is vitally important to find out who you might be indirectly cooperating with. This means investigating who controls all or part of your international partner. For example, if there is a risk that your partner has close relations with the military, or political parties of a foreign state, you should be extremely cautious and tread extremely carefully when initiating any cooperation.

In order to utilize the knowledge already built up in Denmark in a particular area, we recommend that you contact other Danish research institutions (or perhaps the Innovation Centres Denmark) to enquire about their experiences with a specific partner. In exceptional cases, it may be necessary to contact the intelligence services, who will be happy to assist with further advice. Each institution should appoint a contact person or unit to manage contact with relevant services.

Simple cooperation, such as attending conferences and joint conference publications, requires a different approach to risk assessment than more complex cooperation, such as cooperative ventures and actual partnerships.

If you are entering into a multinational cooperative venture involving both European and non-European partners, we recommend you to ask the European partners who have arranged the contact with the non-European partners whether they have carried out the necessary background checks.

Not all non-European states demand the same measure of caution. International cooperation calls for special caution if the partner's home country violates internationally recognized norms and principles, such as the UN human rights charter, the rule of law, academic freedom and the independence of the individual/institution from the state. In this context, listings in the *Academic Freedom Index, Freedom in the World* or the *World Justice Project Rule of Law Index* may be useful in terms of risk assessment. An aggravating circumstance in not like-minded countries are those cases in which civilian research is not separated from military research (military-civil fusion).

Ask yourself why you are collaborating with them

It is important that institutions:

- *prepare a questionnaire guide for researchers that can be used to assess the relevance of entering into a particular international cooperative venture.*
- *carefully consider whether the likelihood of added value is greatest with the particular partner under scrutiny, and whether the cooperation envisaged is based on compatible interests and insures equality.*

You should only enter into major binding cooperative ventures with international partners when you can clearly see that collaboration is of benefit to you. Maybe you will gain access to knowledge you would not otherwise be able to acquire, or to equipment that would otherwise be too expensive to buy.

Always ask yourself whether this partner is the one most likely to provide added value for you. A good rule of thumb is to start small - small, exploratory activities involving low levels of technology development, such as a joint presentation at a conference, are less binding and risky than larger cooperative ventures.

You should not enter into cooperative ventures if the financial contribution of your international partner seems suspiciously generous, or is not proportionate to the work effort. Although it may be difficult to assess a partner's real motivation, you should also not enter into cooperation with international partners if you are in doubt about the partner's motivation. One danger signal is if someone is more interested in what you know in general, than in what you can contribute specifically to the cooperative venture - or if the agreement contains unusual requirements, or entails self-censorship.

International cooperation should be equally enriching for both parties. To achieve this, clear common objectives should be formulated and there should be transparency in terms of motivation and the allocation of resources. One-sided funding or resource allocation should be avoided. In this way, you can promote reciprocity in cooperation while maintaining a strong focus on your own interests.

You should also assess the risk that a partner might put pressure on such fundamental values as academic freedom, freedom of expression, research integrity and responsible research practices. In some countries, there are specific problems with fake peer reviews, the fabrication and falsification of data, or plagiarism – due to a combination of low salaries for researchers and high bonuses for publication. Finally, you should be aware that there have been examples of 'ethical dumping', when research projects that cannot be carried out in the EU for ethical reasons are exported for implementation to countries with very different standards.

As an indicative question guide, you could start with the following:

Question guide

- Who are we working with (directly and indirectly) and why?
- Is there equality in the collaborative venture?
- Who finances the collaborative venture in question, and how much influence is attached to it?
- Who has the legal rights to the research results?
- What potential risks may be associated with cooperation with researchers from the specific country and/or institution?
- Does the agreement impose direct and/or indirect restrictions on the freedom of research - is the text of the agreement clear or does it leave room for interpretation?
- What data is shared and who has the right to it?
- Does the partner have strong commercial interests in the collaborative venture? If so, what does this mean in terms of knowledge sharing?

Define what you are working with them on

It is important that institutions:

- *should, as a matter of course, consider including positive lists in international cooperation agreements, specifying what technologies, data, equipment, results, etc., they will share or provide access to. Negative lists may also be considered if this is deemed appropriate.*

To avoid giving the international partner unnecessary access to your knowledge and research results, you should make sure in the agreement to limit cooperation to specified areas. You could consider adding a positive list of those research areas, technology, equipment, or even buildings, that your international partner may have access to under the terms of the collaborative agreement. Negative lists (of areas or equipment to which access will not be granted) can also be considered, if appropriate.

Your starting point should be that cooperation should be as open as possible, and as closed as necessary. This approach, which is also adopted in EU projects, is important, but may seem unusual, since the starting point in the research world is to promote the principle of *open science*.

This is particularly important for those of you on the management team of a research institution, as the institution is usually the legal entity that signs the formal cooperation agreement. Therefore, if you have not defined what your institution will share and provide access to, you run the risk of your international partner demanding access to all the technology, data and equipment available at your institution, on the grounds that this is necessary to meet their obligations under the agreement.

This also applies when inviting visiting researchers or hiring external lecturers. Specific authorisation procedures may need to be introduced, proactively designating what knowledge or equipment may be accessed.

Protect your institution, staff and students

Be aware of a potential threat

It is important that institutions:

- *make staff and students more aware of threats and risks, and advise them on risk avoidance by measures such as holding courses, preparing guidelines, arranging briefings, etc., perhaps adapted to the particular department.*
- *do their best to create a culture of awareness throughout the entire organization, including encouraging employees to participate in the institution's initiatives in this area.*

A number of specific incidents involving Danish institutions in recent years have made it clear that the threat posed by international research cooperation is real and complex. However, by no means all staff and students have experienced actual ethical or security risks themselves.

It is therefore important that you, as the management of a higher education and research institution, make your staff and (where appropriate) students aware of the threat, for example by providing specific examples of foreign interference and advising them on how to mitigate the risk. You should also consider whether there is a need to invite the PET (the Danish Security and Intelligence Service) to provide training or briefings on critical technologies and foreign interference.

As a senior management team, you have a responsibility of creating a culture of resilience and robustness in the face of potential threats to your institution by providing information, advice and practical guidance to staff and students on how to handle such situations.

Focus on security procedures and systems

It is important that institutions:

- *clearly identify chains of command within the organization, establishing clear channels of communication and procedures for handling security.*
- *ensure that staff and students know the standards of correct digital behaviour, show caution when traveling and staying abroad, especially in countries that are not like-minded, and report suspicious communications or behaviour to the management.*

Foreign countries use various methods to obtain information - whether legal, illegal or in the grey zone between the two. This can range from your research being the subject of special interest at international conferences and social media requests, to your institution being the target of a cyber attack or burglary.

It is your responsibility as a senior management team to implement measures such as a central security organisation, access control, IT, alarms and monitoring, etc., as well as clear procedures for who to go to as a staff member or student, if you experience anything worrying or suspicious.

It is also your responsibility to develop a security-conscious culture in the institution, in which staff and, where appropriate, students demonstrate good digital behaviour, exercise caution when travelling and staying abroad, particularly in countries that are not like-minded, and report suspicious inquiries or behaviour to the management.

Protect your employees and students

It is important that institutions:

- *review their internal rules for subsidiary employment and shield their employees and students from access to knowledge and critical research areas, etc, that are not necessary for their studies or work, and which foreign states could have an interest in acquiring, accessing or influencing;*
- *have clear procedures for the onboarding of new employees, including a knowledge of current regulations and codes of behaviour, and ensure the constant scrutiny by management of the relevance of staff employment, especially in the case of foreigners;*
- *raise the awareness of staff and students concerning human interaction and financial practices that may lead to foreign interference, and encourage the reporting of such events.*

As the management team at a research institution, you do not only have the responsibility of making your staff and students aware of potential threats. It is also your responsibility to actively protect them from foreign interference.

Examples of person-directed methods of foreign interference and espionage include: recruiting researchers and students abroad in order to steal knowledge; recruiting researchers and students to engage in espionage; and eliciting information from individuals through psychological manipulation, blackmail, threats and coercion and bribery.

You should be aware that the method used may be financially indirect and very difficult for the victim to grasp. It may, for example, involve scholarships, grants or foreign talent programmes, through which an employee or student is slowly drawn into an attachment, the consequences of which only become apparent over time.

It may therefore be necessary to review internal rules concerning secondary employment. Even if the rules are considered to be comprehensive and adequate, you should focus on whether your employees are sufficiently aware of what obligations the rules entail.

Participation in talent programmes, for example, is not necessarily problematic, and by maintaining an open and transparent dialogue about personal offers or external affiliations, you and your staff can assess whether there are grounds for concern.

At the same time, some foreign states have intelligence legislation that requires their citizens and companies, in a given situation, to cooperate with the security agencies of that state.

You should be aware that there may be a risk of foreign political party cells operating in Danish institutions with the aim of keeping foreign staff or students on the 'right ideological path'. This may compromise academic freedom, or lead to censorship of research topics or results, but may also result in the military or unethical use of research results, e.g. in violation of human rights.

In such situations, you can shield foreign staff at your institution from such intrusions by carefully considering how to limit knowledge sharing and access to particularly critical research areas, data or technologies, without compromising the work of the researcher concerned. In this way, the researcher's ability to share sensitive or critical knowledge with foreign services, either involuntarily or voluntarily, will be limited.

As management, you also need to focus on onboarding new and foreign staff into the organisational culture of your institution, including improving their knowledge of current rules and codes of behaviour, such as GDPR, dual-use, research integrity and research ethics.

You should consider whether it would be a good idea to have particularly close managerial contact with certain foreign employees - not least in order to be able to help them if the need arises. Make sure in such cases that the focus is on the welfare of your employees, so that any special attention is not perceived as discriminatory.

Finally, it is your responsibility to assess the need to develop country-specific guidelines or briefings before exchanges of researchers and students, especially in the case of not like-minded countries. You may consider consulting the PET in this regard. You should also consider whether, in specific cases, debriefings should be held when staff or

students return from abroad to check whether any potential risks have materialized and to identify any significant patterns.

About the committee

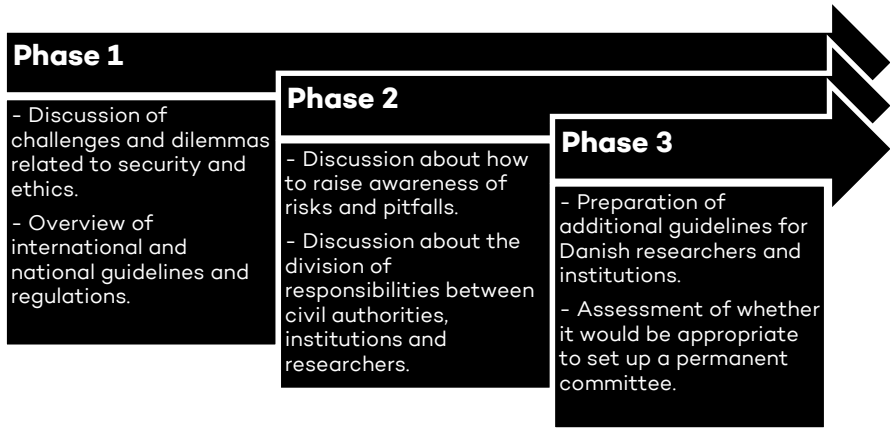
Committee on guidelines for international research and innovation cooperation (URIS)

URIS was set up in autumn 2020 to review existing policy for international research and innovation cooperation and to assess the need for possible supplementary measures. The aim was to support Danish research institutions through a balanced approach: promoting international research and innovation collaboration alongside an increased focus on potential risks.

As part of this task, URIS has addressed the following areas of risk:

- violation of the principles of research integrity and responsible research practices, including the responsible administration of research data and copyright protection;
- unethical uses of technology, including military use or use in violation of human rights;
- foreign interference and security breaches by foreign students and staff at Danish institutions, as well as Danish students on exchanges and staff traveling abroad; and,
- contributing to strengthening and developing research and innovation capacity in sensitive areas in countries that are not like-minded.

The Committee's work on these four areas of risk was divided into three phases:



Based on the above phases, eight committee meetings were held between September 2020 and January 2022. The URIS drew on international experience, as well as on relevant authorities and academic experts with an understanding of the issues.

The committee consisted of the following representatives from the universities, university colleges and foundations that fund academic research:

- Peter Kjær, Vice-Rector, Roskilde University
- Lene Pries-Heje, Head of Department, IT University
- Mogens Rysholt Poulsen, Dean, Aalborg University
- Nikolaj Malchow-Møller, Rector, Copenhagen Business School
- Kristian Pedersen, Dean, Aarhus University
- Rasmus Larsen, Vice-Rector, Technical University of Denmark
- David Dreyer Lassen, Vice-Rector, University of Copenhagen
- Henrik Bindslev, Dean, University of Southern Denmark
- Harald Mikkelsen, Chairman of the Strategic Research Initiative, Danish University Colleges (FIDP)
- Maja Horst, Chairman of the Board, Independent Research Fund Denmark
- Annemarie Munk Riis, Deputy Director, Innovation Fund Denmark
- Søren-Peter Olesen, Director, Danish National Research Foundation

The Ministry of Higher Education and Science chaired the committee and supplied the secretariat service.