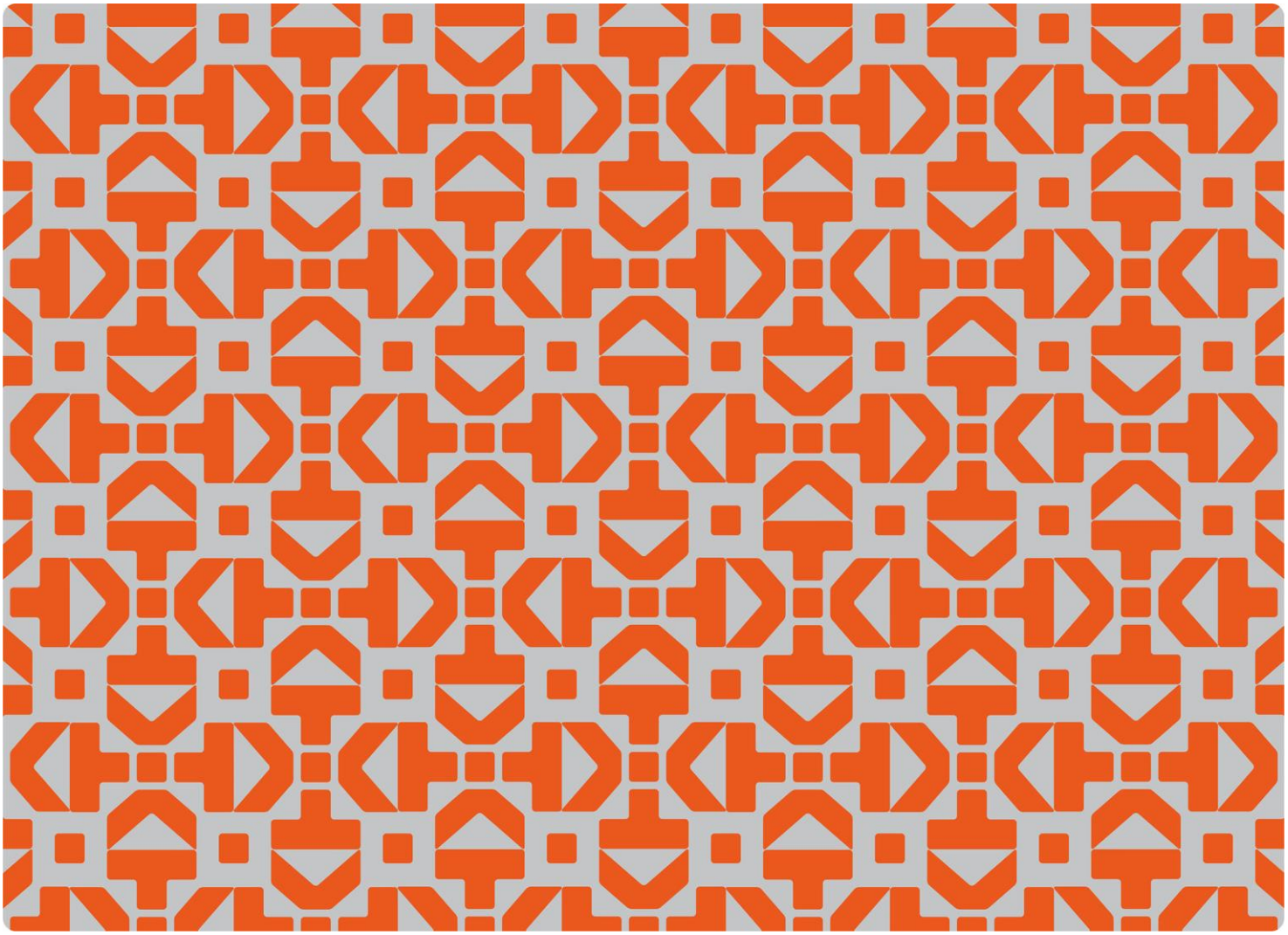
Direktoratet for høyere utdanning og kompetanse

Forskningsrådet

Report no 01/2023

Guidelines and Tools for Responsible International Knowledge Cooperation



Editors:
Kristine Offerdal (HK-dir) and Christina I. M. Abildgaard (NFR)

Editors: Margrete Søvik and Hege Toje

Authors:
Siri Lader Bruhn
Magnus Løken Bain
Thomas Hansteen
Karine Kålsås
Ingrid Radtke
Gunnhild Rønningen
Agnethe Sidselrud
Margrete Søvik
Berit Berg Tjørhom
Hege Toje
Torill Iversen Wanvik

ISSN: 2703-9102
Published: 03/23

Preface

In its allocation letter for 2022 from the Ministry of Education and Research (KD), the Directorate for Higher Education and Skills (HK-dir) and the Research Council of Norway were assigned the task of jointly developing national guidelines for responsible international cooperation.

The assignment was based on the revised Panorama Strategy (2021–2027). This strategy concerns how Norway can increase its cooperation on research, higher education and innovation with selected countries outside the EU/EEA area, based on a long-term perspective, by looking at the foreign, business and knowledge policy objectives in conjunction with each other. The Panorama countries have been selected because of their global and regional role. Together, they account for a large and vital part of global knowledge production. At the same time, some of these strategic partner countries have in recent years been designated high-risk countries in the public threat and risk assessments produced by the Norwegian Intelligence Service (NIS), the Police Security Service (PST) and the National Security Authority (NSM).

Accountability was added as a new principle for knowledge cooperation in the new Panorama Strategy (2021–2027), in addition to quality, relevance, reciprocity and a long-term perspective. Accountability is defined as: 'consideration for fundamental academic values and national interests, including security interests.'

The assignment to develop national guidelines for responsible international cooperation in the research and education sector is an extension of this principle. The nature of the work on the guidelines changed during 2022, with the outbreak of war in Ukraine, sanctions and increased attention to security considerations in general, including in the research and education sector. The national guidelines for responsible international cooperation are intended to help the sector to exercise accountability in a geopolitical context characterised by heightened tension.

A project group comprising participants from HK-dir and the Research Council of Norway was established in the new year 2022. HK-dir has managed and coordinated the project. The assignment from KD expressed the expectation that work on the guidelines should be carried out in dialogue with the environments and institutions it concerns. Three resource groups were established, comprising representatives from higher education and research institutions in Norway. The members of the resource groups have participated in discussions and provided input on draft texts. We have also held 50 meetings with authorities, knowledge institutions and interest groups in Norway and in Europe.
In March 2023, the research and education sector was invited to submit input on the 'Proposed Guidelines for Responsible International Cooperation'. We received a total of 25 submissions and have used them to further develop the current guidelines.

The work on developing guidelines for responsible international cooperation is complex, involving requirements and conflicting interests across different ministries, policy areas, legislation and international agreements. The report must be seen as a starting point for long-term efforts to develop resources for the research and education sector with a view to strengthening the planning and implementation of international cooperation.

Table of contents

Glossary

A **cyberattack** is an attempt to gain access to and control of an organisation's digital infrastructure.

Due diligence is an analysis of an organisation for the purpose of preparing for a transaction or collaboration. In the context of research and education cooperation, due diligence involves examining the partner's past activities, the sector in which it operates, a commercial and ethical assessment with regard to intentional management, and the legal and regulatory framework the partner is subject to.

Dual-use items are items that were originally designed for civilian purposes, but have important military applications. In the knowledge context, dual use refers to research that can be expected to generate knowledge or technology that can potentially be exploited for harmful purposes and that threatens public health or national security, even if the research has a different purpose.

Protective security is a term used in the Security Act. It covers both measures that reduce the likelihood of an event occurring and measures that limit the effects of such an event.

Protective security work is the planning, facilitation, implementation and oversight of protective measures targeting activities that present a threat to security and the consequences of such activities.

Freedom of research means the right to freely formulate research questions, select and develop theories, collect empirical material, design and use academic research methods, shine a critical light on accepted truths and generate new ideas. It includes the right to share and publish research results openly, also through training and teaching. Researchers have a right to express their opinions without risk of detrimental consequences for their work and careers or of being subjected to censorship or discrimination at the institution where they work. This includes the freedom to establish trade unions, academic organisations and academic forums.

Research ethics encompasses norms, principles, values and institutional arrangements that help constitute and regulate scientific activities. In Norway, the term 'research ethics' is broadly understood, for example as defined in national research ethics guidelines. This means that research ethics includes norms aimed at ensuring quality and reliability; norms that regulate the research environment; norms that concern the relationship between the researcher and individuals and groups that are part of, or are affected by, the research; and norms that relate to the use of research, and its consequences for society and the environment.

Research integrity is defined on the basis of the main principles of reliability, honesty, respect and accountability. Research integrity means that these principles are applied at all stages of the research process.

Hybrid/Compound threats. In Report No 9 to the Storting (2022-2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet. Så åpent som mulig, så sikkert som nødvendig* ('National control and digital resilience to safeguard national security. As open as possible, as secure as necessary' – in Norwegian only), these threats are described as 'strategies for competition and confrontation that fall below the threshold of direct armed conflict, which may combine diplomatic, informational, military, economic, financial, intelligence and legal methods to achieve strategic objectives. Hybrid threats can arise in security policy grey areas where their purpose is to sow discord and create destabilisation. A wide range of methods can be employed, combining open, covert and clandestine methods. The methods may target specific activities or situations, or they may be more long-term methods of creating doubt, undermining trust and thereby weakening our democratic values. Hybrid threats are inherently complex, and they represent a challenge to early warning, unified situational awareness and effective and coordinated action.'

Conflicts of interest and conflicts of commitment. A conflict of interest is a set of circumstances that creates a risk that professional judgements or actions may be influenced by other interests. A conflict of commitment is a situation in which an individual takes on an excessive workload, or conflicting tasks, from different clients. Both can have an impact on impartiality.

Knowledge security means preventing the unwanted transfer of sensitive knowledge and technology with negative consequences for national security and innovation capacity. The term covers activities aimed at influencing and disrupting activities on behalf of foreign state actors within higher education and research. Such activities can lead to censorship and impair academic freedom. Knowledge security also covers ethical issues related to cooperating with countries where fundamental rights are not respected.

Countries of concern refers to countries identified as high-risk countries in the annual national risk and threat assessments issued by NIS, PST and NSM.

National security is defined as state security and as a limited part of the social security area that is essential for a state's ability to safeguard national security interests.

National security interests are a country's sovereignty, territorial integrity and democratic system of government, as well as general political security interests related to (a) the activities, security and freedom of action of the highest state bodies, (b) defence, security and contingency preparedness, (c) relations with other states and international organisations, (d) economic stability and freedom of action, and (e) fundamental societal functions and the basic security of the population.

Risk can be seen as the sum of values/assets that the institution must protect, the external threat landscape and the institution's vulnerabilities. A risk assessment is made on the basis of a valuation, a threat assessment and a vulnerability assessment.

Public security is society's ability to protect itself against and deal with events that threaten fundamental values and functions, and endanger life and health. Such events may have natural causes or be the result of technical faults or human errors, or of deliberate actions.

State security is the safeguarding of the state's existence, sovereignty, territorial integrity and political freedom of action. State security has traditionally been linked to the defence of the state's territory against armed attacks, but it can also be challenged by the application of various forms of pressure against Norwegian authorities and societal actors.

A **vulnerability assessment** describes how vulnerable the values/assets are in light of identified threats, and it forms the basis for preventive and mitigating measures.

A **threat** is an external actor or external circumstances that can adversely affect the institution's own activities and values/assets by, among other things, exploiting its internal vulnerabilities.

Foreign interference occurs when activities that are coercive, clandestine, deceptive or corrupting, and are contrary to national sovereignty, values and interests, are carried out by, or on behalf of, a foreign party. This includes, e.g., researchers concealing military connections or connections with foreign states or companies, and cyberattacks.

Foreign influence takes place in an open and transparent manner. All countries influence other countries by means of different methods, e.g. through cultural exchanges or cultural events or language courses abroad.

On the one hand, '**values'** refers to norms and principles, such as academic freedom. However, the term 'values' or 'assets' is also used in the context of valuation and risk analysis. Here, the terms refer to anything that is worthy of protection and can be threatened, such as life and health, information, material assets and reputation.

A **valuation** is an analysis aimed at identifying what information, objects and other assets (e.g. life and health, reputation, etc.) are so important that they need to be shielded or protected. A valuation forms the basis for identifying threats that are relevant to the institution's activities in terms of how threat actors can affect the institution's values/assets.

Summary

These Guidelines and Tools for Responsible International Knowledge Cooperation are intended to be a resource the research and education sector can use to strengthen its valuations and risk assessments, vulnerability analyses and security procedures when engaging in international cooperation in a challenging world. The purpose of the guidelines is to ensure that academic values and research ethics standards, as well as national interests, are safeguarded, with the emphasis on foreign intelligence and interference, digital security and illegal knowledge transfer. A wide range of representatives of the research and education sector and authorities in Norway and abroad have been consulted when developing these guidelines.

Increased attention to institutional vulnerability and security threats may entail a risk that security considerations overshadow the need for international cooperation in the research and education sector. It is important to emphasise that international knowledge cooperation is part of our national preparedness. Openness and sharing are important prerequisites for good research and teaching, but some knowledge cannot be shared indiscriminately. The planning and evaluation of international cooperation must take account of both the strategic need for academic cooperation and possible security risks.

The target group for these guidelines consists of universities and university colleges, as well as the institute sector and other institutions that engage in international cooperation on research, innovation and higher education. Many of the recommendations will also be relevant for the regional health authorities and Norwegian businesses, in particular the chapters on export control, research partnerships and agreements on education and research cooperation.

The guidelines draw on national advice and national and European guidelines. They propose assessments and procedures based on what we know so far about the challenges and vulnerabilities in the Norwegian research and education sector. The guidelines provide an overview of legislation and guidelines that the Norwegian sector must comply with, and highlight key assessments and procedures for academic environments and for institutions' management and administration.

The guidelines are also a toolbox consisting of reports, guides, checklists and templates.
It is the institutions themselves that must find answers to the challenges and vulnerabilities that are pointed out, based on the distinctive characteristics of their own institution and its existing systems and the forms/scope of international cooperation it engages in. The work on securing Norwegian knowledge institutions will require a systematic focus and resources. However, this work is important to protect academic freedom, research integrity and institutional freedom of action in the long term.

Key advice for institutions' management and administration

- Carry out a systematic valuation and a risk and vulnerability analysis to identify specific security challenges and pressure on academic freedom and research ethics at the institution.
- Differentiate access to valuable information and infrastructure.
- Adopt procedures for background checks in connection with appointments to areas with a high security risk.
- Create a list of international cooperation agreements and research cooperation at the institution, and identify collaborations with countries where academic freedom is under threat, countries of concern based on national risk and threat assessments (NIS ,PST, and NSM), and countries covered by the national sanctions regulations.
- Introduce procedures that identify cooperation that could fall within the scope of the Export Control Regulations and offer help to the academic environments to carry out assessments when entering into international cooperation, recruiting staff and inviting visiting researchers.

- Build competence and awareness of academic values, security risks and research ethics dilemmas throughout the knowledge institution.
- Establish a contact point in the organisation with clearly assigned responsibility for research ethics challenges, and for reporting pressure from external actors or security breaches. Contact the relevant authorities for advice on difficult assessments.
- Establish dedicated forums for sharing experiences and discussing complex issues.

Key advice for academic environments

- Keep informed about countries, political contexts, partner institutions and academic environments when entering into knowledge cooperation especially as regards security challenges, laws and regulations, and possible challenges relating to academic values and ethics.
- Clarify expectations with partners as regards academic freedom and research ethics in the planning process and endeavour to create equitable partnerships with regard to funding, interests, etc.
- Carry out risk assessments relating to academic freedom, research ethics and export control based on information about the country context, and plan preventive measures.
- When cooperating with challenging countries, define the strategic framework for the cooperation and set out your expectations of compliance with academic freedom and research ethics principles etc. in the agreements entered into. Discuss in advance which breaches will lead to the agreement having to be terminated and how the cooperation agreements should provide for such termination and how it will be handled in practice.
- Seek advice from support services at the institution and/or from the relevant authorities when making difficult assessments.

The guidelines and tools for responsible international knowledge cooperation presented in this report should be regarded as the start of a long-term effort. If they are to be useful, the guidelines must be adopted and put into practice. The guidelines should also be adjusted and further developed in cooperation between the research and education sector and the authorities in order to address new challenges and needs. Knowledge security is about preventing the illegal transfer of sensitive knowledge and technology with negative consequences for national security and innovation capacity. This is a complex area. Conflicting considerations and needs must be weighed against each other. The goal is to achieve proportionality in security thinking, so that the need for broad international knowledge cooperation and fundamental values such as academic freedom, openness and sharing are safeguarded.

1 Introduction

1.1 Background and remit

The Directorate for Higher Education and Skills (HK-dir) and the Research Council of Norway have been commissioned by the Ministry of Education and Research (KD) to prepare guidelines for responsible international cooperation.
The purpose is to help to build knowledge about the opportunities and challenges international knowledge cooperation presents. The target group consists of universities and university colleges, as well as the institute sector and other institutions that engage in international cooperation on research, innovation and higher education. The guidelines will also be relevant for regional health authorities and Norwegian companies. Since institutions include companies, foundations and administrative bodies owned or controlled by different ministries, we do not go into detail about security management in the institute sector.

The backdrop is a changing security policy situation and increased rivalry between the world powers, where knowledge and technology development are central. Report No 9 to the Storting (2022-2023) National control and digital resilience to safeguard national security. As open as possible, as secure as necessary (in Norwegian only) points to a complex threat landscape. The term compound, or hybrid, threats refers to actions by state and non-state actors that aim to sow discord and create destabilisation, undermine trust, and weaken political systems. Strategies can be long term, both open and covert, and include various methods, such as economic, political, civilian, military, and information and intelligence methods.

The Norwegian research and education sector is internationally oriented, and it manages and develops knowledge at a high level. Internationalisation is a desired policy and a prerequisite if Norwegian academic environments are to be able to keep up with international knowledge development. Cooperation with academic environments in other countries is an integral part of research and higher education. At the same time, however, it makes the sector vulnerable. National risk and threat assessments have for several years pointed to the research and education sector as a target for foreign intelligence and influence. Known examples include digital attacks, student placements and irregular use of laboratory facilities among visiting researchers. Financial ties and dependencies can also lead to different forms of pressure.

Many countries, as well as international organisations including the EU and the OECD, have recently published guidelines for responsible international cooperation. The international work carried out in this area, especially in the EU, is also an important part of the context of the work on the Norwegian guidelines. The OECD (Integrity and Security in the Global Research Ecosystem) believes that academic freedom and cooperation must be recognised as fundamental principles of the global research system and that security should be an integral part of national and institutional frameworks for research ethics. The report states that safeguarding national security interests must be balanced against openness and cooperation in research, and that the assessments must be proportional.

In the Norwegian context, the principle of accountability in international cooperation was introduced in the new Panorama Strategy (2021–2027) for knowledge cooperation with priority countries outside Europe (USA, Canada, Brazil, India, South Africa, Russia, China, Japan and Korea). The importance of striking a good balance between openness and caution is also highlighted in the new Long-Term Plan for Research and Higher Education (2023–2032).

The assignment from KD states that the safeguarding of national security interests must be balanced against continued openness in Norwegian research and higher education. The sector must be equipped to deal with complex challenges, while maintaining and strengthening international cooperation. KD also emphasises safeguarding academic freedom and research ethics standards. Open research and sharing are important research policy objectives.

The guidelines are intended to be a resource in the work on planning international knowledge cooperation, so that the different considerations can be taken into account and balanced in the best possible way. The guidelines will not be used in the management of the sector, but will be a practical tool for institutions and academic environments. It will still be the institutions and the academic environments themselves that decide who they wish to collaborate with, based on their own plans and priorities, provided that they act in accordance with the applicable regulatory framework.

The assignment from KD also states that the guidelines must be relevant regardless of country and discipline. Many issues are the same regardless of the countries involved. Today, collaborative constellations, value chains, ownership and digital platforms are also clearly multinational. It can be difficult to identify ties and national origins. Nonetheless, particular challenges will arise in relation to certain countries. A key piece of advice in the report is therefore to build knowledge about partner countries and partner institutions. Challenges will also vary between disciplines, and sometimes also from project to project in the same field. The general advice in the report is to identify one's own interests, values/assets and vulnerabilities, and to be aware of what needs to be guaranteed when entering into an agreement on an individual cooperation project.

Some of the measures proposed in the report are voluntary and must be assessed on the basis of institutional needs, the nature of the specific cooperation and the specific national and international context in which they are carried out. Other measures are required by laws and regulations. This applies to a number of security systems and procedures in the individual organisations, export control regulations and relations with countries subject to Norwegian sanctions.

Proportionality is an important principle. Measures must be proportional to the risk situation in each case. Risk can be reduced, but not eliminated. It is very important to prevent security management systems imposing unnecessary restrictions on cooperation and knowledge exchange. The research front is international. Countries with which Norway does not cooperate on security policy-related matters, such as China, are at the forefront in several areas. National security and preparedness also depend on international access to knowledge. Furthermore, it is important to be aware that, unless handled in a good and nuanced way, increased attention to security and international threats can have unfortunate consequences in the form of more limited opportunities to exercise free speech, distrust and stigmatisation of groups and individuals.

The key to good international cooperation lies in good planning. The purpose of the cooperation project and the conditions for its success must be well thought out. Assessments of risk factors must be based on knowledge and be carried out both at an early stage and as the cooperation progresses. This applies in particular to assessments of what should be shared in individual projects. The necessary systems and division of responsibility for risk management must be in place. Cooperation and information exchange are particularly important, at the individual institution, across the sector and between institutions and the authorities. Dialogue between institutions and the authorities is also important to ensure that the framework conditions for security management in the research and development sector do not unnecessarily restrict international cooperation and the international flow of knowledge on which research depends.

1.2 Knowledge base

The proposed Norwegian guidelines presented in this report are strongly inspired by international resources and guidelines. The EU, which Norwegian research and educational institutions are linked to through the European Education and Research Area, is a particularly important source of inspiration. Security management systems should be as harmonised as possible with the rest of Europe in order to facilitate cooperation through the Horizon Europe and Erasmus+ programmes. The EU report Tackling Foreign Interference (2022) has been an important reference document.

At the same time, the work on responsible international cooperation must be adapted to the Norwegian context. The challenges in Norway are different from those faced by many other countries. Educational and research institutions in countries such as the United States, the United Kingdom and Australia have engaged in large-scale recruitment of international staff and, not least, students, who are an important source of income. Many institutions have also established campuses in other countries. In the international context, Norwegian higher education and research institutions are small. They enjoy great autonomy and have a distinctly flat organisational structure compared to many international institutions. A high degree of freedom brings great responsibility for the individual institution, researcher and teacher, which can feel challenging. On the other hand, a relatively small sector and short lines of communication between institutions and the authorities can facilitate dialogue and information sharing. Several Norwegian institutions have recently developed their own resources and guidelines for responsible international cooperation. Some resources that are openly available are shared in this report. It is important to facilitate more sharing of experience and information in future.

As part of this project, a call for tenders was issued for a survey study of the challenges Norwegian research and higher education environments face through international contact points and communication channels, and how they are handled. The Norwegian Institute of International Affairs (NUPI) was awarded the assignment.

The results are published in the report Utfordrende kunnskapssamarbeid: Etiske og sikkerhetsrelaterte utfordringer som forskere og kunnskapsinstitusjoner møter i internasjonalt samarbeid (2022) ('Challenging Knowledge Cooperation: Ethical and Security-related Challenges faced by Researchers and Knowledge Institutions in International Cooperation' – in Norwegian only). The study covers all scholarly disciplines and most of the accredited higher education institutions and research institutes that receive basic public funding in Norway. Questionnaires were distributed to three sample groups: 200 researchers who receive project funding from the grant schemes INTPART and UTFORSK, the central management of 30 accredited universities and university colleges in Norway, and research institutes that received basic public funding from the Research Council in 2022. In addition, interviews were conducted with focus groups and individuals taken from academic and administrative staff at various academic environments and at different levels.

The general findings in NUPI's study suggest that researchers and knowledge institutions in Norway do not experience unmanageable ethical and security-related challenges in connection with international cooperation. Their experience varies, however. While the data do not provide a basis for drawing conclusions about the extent of the challenges faced by the different disciplines, some types of challenges are more common in certain disciplines. Many respondents are used to handling different types of risk and are satisfied with the way things are done. At the same time, many find that the challenges are becoming more numerous and more demanding to handle.

More knowledge is needed about the challenges the research and education sector encounters in international cooperation and communication. The picture is varied, and it will be useful to have more insight into the situation in the different disciplines. Students' experiences should also be mapped. The NUPI study indicates that this is an area the institutions do not know enough about, which several informants express concern about.

1.3 Structure of the report

The report is divided into different thematic sections. Each section begins with a brief outline of the relevant topics, including legislation and policy where applicable. Recommended assessments and procedures are then presented. Where appropriate, the guidelines are structured according to different user groups. Parts of the guidelines are aimed at the institutions' management and administration (e.g. the HR department, research administration department, international office, IT

section), while others are intended as resources that can be used by researchers and lecturers planning to establish or further develop international cooperation projects.

At the beginning, there is a glossary of key terms. The terms 'values' and 'assets' are clarified initially, as they are frequently used in the report. 'Values' refers to norms and principles, such as academic freedom. Both 'values' and 'assets' are used for anything that is worthy of protection and can be threatened. In the Council for Public Security and Preparedness in the Research and Education Sector's guide to risk and vulnerability analyses for the sector (Veileder i risiko- og sårbarhetsanalyser for kunnskapssektoren – in Norwegian only) values/assets such as life and health, information, material assets and reputation are emphasised. The final part of the report is devoted to the central government level, where an overview of the various government bodies and their responsibilities is provided.

Much of the work on the guidelines has consisted of creating an overview of laws and regulations, policy guidelines, existing reports, resources and guidelines in various areas, and presenting them together. Links to various sources are provided in the text. There is also a complete list of resources and reports at the end, organised by topic. Many relevant regulations, guidelines, guides and policies are under review, and these guidelines will have to be updated as the framework conditions change.

2 Academic values and responsibilities

2.1 Academic freedom

Section 1-5 of the Act relating to Universities and University Colleges regulates academic freedom and responsibility at Norwegian universities and university colleges. The Act stipulates that the institutions must promote and safeguard academic freedom and ensure transparency about the results of research and development work. The rights include freedom to choose the topic of the research, methods and the method of publication, and independent academic responsibility for the content of the teaching within the institutionally established framework. The obligations include respecting the norms and ethics of science.

The institute sector and the business sector are not covered by the Act relating to Universities and University Colleges. Academic freedom in these sectors is somewhat more limited through the employer's and client's managerial prerogative. Here, it is primarily the Act on the Organisation of Research Ethics (Research Ethics Act) (in Norwegian only) that regulates the framework for research activity, including a duty to comply with recognised research ethics norms. The guidelines for basic funding of research institutes also state that the institutes must ensure that the principle of academic freedom applies to all publicly funded research.

Academic freedom enjoys strong legal protection in Norway, but it is not absolute. Legally, it may be limited by, for example, the Health Research Act , the Biotechnology Act, the Research Ethics Act, (https://lovdata.no/dokument/NL/lov/2017-04-28-23) the Government Employees Act (in Norwegian only), the Equality and Anti-Discrimination Act, the Working Environment Act, (https://lovdata.no/dokument/NLE/lov/2018-06-01-24) and the Act relating to Control of the Export of Strategic Goods, Services, Technology, etc.

The protection of academic freedom also has a strong standing in Norwegian politics. Several recent official reports and white papers devote a great deal of attention to this topic. As part of the work on the Long-term plan for research and higher education, a committee chaired by Anine Kierulf was established to look into the conditions for academic freedom of expression in Norway. The report, Academic freedom of expression. A good culture of free speech must be built from the bottom up, every single day (Official Norwegian Report (NOU) 2022: 2), refers to restrictions on academic freedom in several countries, including allied countries, and to challenges arising from cooperation with authoritarian states. One of the key dilemmas pointed out by the Kierulf Committee is the fact that international cooperation can both protect and challenge academic freedom. It can protect individual researchers from other countries against interference by the authorities, but it can also mean that researchers and students from Norwegian institutions are subjected to pressure and restrictions by actors and authorities in other countries. It can be added here that researchers in some countries may find that international cooperation makes their relationship with their own authorities more challenging. The Government will follow-up the Kierulf Committee's report by promoting academic freedom through international cooperation in accordance with the long-term plan.

A draft new university and university colleges act is scheduled for presentation in 2023. The draft bill will, among other things, be based on the Aune Committee's report Ny lov om universiteter og høyskoler (NOU 2020: 3 ('New Act relating to universities and university colleges' – in Norwegian only). (https://www.regjeringen.no/no/dokumenter/nou-2020-3/id2690294/) The Committee points out that questions concerning academic freedom may arise in connection with cooperation on education and research. It refers to commissioned research, but also international cooperation projects. The Committee emphasises that the requirement to promote and safeguard academic freedom applies 'also when cooperating with others, both authorities and private actors at home and abroad' (p. 135).

Academic freedom is also high on the agenda of international organisations. The Magna Charta Universitatum, which was signed by European university rectors on the occasion of the 900th anniversary of the University of Bologna in 1988, describes academic freedom and institutional

autonomy as the foundation of the university as an institution. The charter marked the start of the Bologna Process, which Norway joined in 1999. The Rome Ministerial Communiqué, signed in 2020 by ministers responsible for higher education within the Bologna Process, also refers to the principles enshrined in the Magna Charta Universitatum. In the same year, Norway endorsed the Bonn Declaration on Freedom of Scientific Research, adopted at the Ministerial Conference on the European Research Area (ERA). It includes a common definition of academic freedom.

Pressures on academic freedom are not limited to international contexts, cf. the Kierulf Committee's report. The Committee also describes how academic freedom in close partner countries is under pressure in new and serious ways. However, the ability to perceive and handle pressure may vary depending on what information is available about the country in question and the contextual understanding. It is also important to be aware that, in practice, what academic freedom is understood to entail may be politically and culturally conditioned.

The NUPI study Challenging Knowledge Cooperation (in Norwegian only) includes examples of how academic values and norms can come under pressure in international cooperation. This can be due to differences in research ethics principles between countries, partners with roles and ties that weaken confidence in their independence, or pressure to adapt statements and presentations of research findings and teaching activities. The examples given relate to issues such as gender and sexuality, ethnic minorities, territorial borders and geographical definitions. Researchers and institutions have experienced that international colleagues are reluctant to participate in certain academic activities, such as courses and guest lectures, due to political restrictions in their home country.

Another challenge many of the respondents are concerned about is that an excessive focus on security can lead to discrimination and to suspicion being cast on employees and students, as well as to unnecessary restrictions on international cooperation. Openness, inclusion and cooperation are academic values that must be safeguarded, but that can also come under pressure as a result of risk prevention measures. It is important to be aware of this.

Challenges and dilemmas related to academic values and norms in international cooperation projects are also described in international reports and guidelines. Some countries have recruited many international students, and the institutions are financially dependent on them. This can put them in a vulnerable situation. The situation is different in Norway. Examples from other countries can nevertheless be a useful starting point for reflection and discussion. Among other things, the report Managing Risks in Internationalisation: Security Related Issues (Universities UK, 2020) discusses difficult situations that can arise if international students (and visiting researchers) are under surveillance and possibly subject to laws in their home country that also restrict their freedom during stays abroad. Some institutions in the UK have put measures in place to protect such persons, for example by introducing the Chatham House Rule in seminars and allowing student assignments to be submitted anonymously. The report recommends making separate assessments for digital platforms where recording is possible. The Australian Government's Department of Education has published cases involving academic freedom in international interaction arenas.

Proposed assessments and procedures for the institutions' management and administration

- Has the institution, through dedicated strategies, plans and regulations, undertaken to safeguard and promote academic freedom?
- Does the institution take responsibility for building knowledge and awareness of academic freedom among its staff, students and visitors, e.g. in the form of courses/seminars?
- Does the institution have systems in place for detecting violations of and threats to academic freedom, and procedures for dealing with such issues?

- When entering into international cooperation agreements (see also the separate chapter on cooperation agreements):
    - Is there a risk that any of the sources of funding can lead to unfortunate ties?
    - Is there a risk that non-academic actors in other countries will have influence over research and teaching that exceeds what is desirable or acceptable?
    - Consider clarifying in the text of the agreement what the parties mean by academic freedom in the specific cooperation project.
    - Consider whether to clarify the framework conditions for academic freedom in the text of the agreement.
    - Does the institution have procedures in place for when and how cooperation can be terminated if violations of academic freedom and other key values are identified?

Proposed assessments and procedures for the academic environments

- Discuss with partners what academic freedom means in the specific project.
- Do you have sufficient knowledge of the framework conditions for academic freedom in the partners' home country?
- Could restrictions on academic freedom on the part of the partner have an impact on the cooperation?
- Should the framework conditions for academic freedom be set out in the text of the agreement? Examples include provisions on the conditions for the publication of findings. See also chapter 6 on agreements in the field of research and education.
- Be aware that financial ties or other types of ties can affect academic freedom.
- Ensure transparency about financial or other types of ties that can influence your research work.

2.2 Research ethics

Research ethics and ensuring that the research is carried out in accordance with recognised research ethics norms are a prerequisite for good and responsible research and for trust in the research. Research ethics training is a statutory duty. Many of the questions and challenges addressed in this report touch on research ethics. The OECD report Integrity and Security in the Global Research Ecosystem (2022), stresses that research integrity, security and international research cooperation are closely linked.

Research ethics can be defined as values, norms, and institutional arrangements that help constitute and regulate scientific activities. Research integrity and trust in research depends on the research community being committed to such standards, and other actors in the research system must also recognise and comply with ethical and legal framework conditions for research. The Act on the Organisation of Research Ethics (Research Ethics Act) regulates the organisation of research ethics work in Norway. The purpose of the Act is to ensure that all public and private research is conducted in accordance with recognised research ethics norms (Section 1). The Act stipulates that the research institutions are responsible for teaching research ethics and for dealing with cases involving possible breaches of research ethics norms (Sections 5 and 6). A new Research Ethics Act was adopted in 2017 in order, among other things, to further specify institutional responsibilities in relation to research ethics.

The Act requires institutions to:

- ensure that the research at the institution is conducted in accordance with recognised research ethics norms
- provide training in research ethics for candidates and employees

- ensure that everyone who participates in the research is familiar with research ethics norms
- consider all cases of possible breaches of research ethical norms, called misconduct cases in the Act
- have guidelines on how such cases should be treated
- appoint a committee to consider misconduct cases
- report possible serious violations to the National Commission for the Investigation of Research Misconduct

In Norway, recognised research ethics norms are defined in national research ethics guidelines. The research environments themselves define the content of research ethics. The National Research Ethics Committees are independent committees broadly composed of researchers and lay people. The committees prepare national research ethics guidelines and guides for different subject areas. The committees are preparing a guide to the institutions' research ethics work, which will be completed in 2023. The National Research Ethics Committees has also written general research ethics guidelines as an introduction to research ethics principles and norms across disciplines. The guidelines include the following principles:

- **Respect:** Persons participating in research, as informants or otherwise, shall be treated with respect.
- **Good consequences:** Researchers shall seek to ensure that their activities have good consequences and that any adverse consequences are within the limits of acceptability.
- **Fairness:** All research projects shall be designed and implemented fairly.
- **Integrity:** Researchers shall comply with recognised norms and behave responsibly, openly and honestly towards their colleagues and the public.

A joint European framework has also been developed, ALLEA's European Code of Conduct for Research Integrity, which is incorporated in Horizon 2020, the EU Framework Programme for Research and Innovation (Article 35 Ethics and Research Integrity). A new revised version will be completed in 2023. The European Code of Conduct for Research Integrity complements the Norwegian legislation and the research ethics guidelines in different disciplines. The National Research Ethics Committees have translated them into Norwegian on behalf of KD.

As the subject areas are different, and the regulation of research ethics varies between different areas and different countries, challenges may arise related to interdisciplinarity and international cooperation.

The need to ensure the integrity of research through a common understanding among the research environments at the global level led to the launch of the World Conference on Research Integrity. The Montreal Statement from 2013 contains 20 principles on which research cooperation should be based. The statement's main message is that partners must take collective responsibility for the credibility of the overall research collaboration.

Proposed assessments and procedures for the institutions' management and administration

- Consider whether information about research ethics guidelines, systems and procedures for research integrity and ethics is readily available on the institution's website.
- Consider whether it is necessary to provide more training in research ethics guidelines during the course of education and internally within the organisation.
- Consider whether the institution has established satisfactory mechanisms for dealing with suspected breaches of research ethics norms.
- Consider whether satisfactory procedures have been established for clarifying partiality/conflicts of interest in connection with the execution of research, funding, peer reviews, evaluations and cooperation.

- Consider whether the procedures for the publication and dissemination of research are sufficiently specified, for example in relation to guidelines for authorship and procedures for handling any disputes.
- Consider whether there is a need to establish discussion forums for reflection on ethical dilemmas and conflicts of interest.

Proposed assessments and procedures for the academic environments

- Carry out an ethical assessment of the research project with reference to relevant guidelines and regulations.
- Consider research ethics issues before entering into international cooperation. Perceptions and legislation may differ between countries.
- Consider whether everyone who carries out or participates in the research is familiar with recognised research ethics norms.
- Consider the health, safety and the environment implications for society, employees and others associated with or affected by the research.
- Consider the potential harm and risk that may result from the research.

2.3 Open research and sharing

In open research, the research processes are characterised by openness and knowledge sharing, so that knowledge is made available across academic environments, sectors and national borders. This is based on fundamental research ethics norms, and is important to ensure a high quality of research and society's confidence in the research and research results. In principle, the concept of open science encompasses the entire research process from start-up via funding and implementation of the research through data management, analysis, scholarly publication, scientific synthesis and communication activities.

In the Long-Term Plan for Research and Higher Education (Report No 5 to the Storting (2022–2023), Chapter *8 Open research and the value of data*, the Government states that more openness and data sharing in research are required in order to realise the objectives of the long-term plan,. The Research Council has developed a Policy for open access to research data (2017), and a Policy for Open Science, and it has published the report How should we share research data? Report and recommendations relating to licensing and making research data available (2021). Useful background information on open research can be found on the website openscience.no/en.

The international FAIR principles have been formulated as guidelines for the reuse of research data. FAIR is an acronym for Findable, Accessible, Interoperable and Reusable. It is possible to limit the sharing of data during a project, and yet remain true to the FAIR principles, which largely concern further use of the data after the project is completed.

The nature of various disciplines and subject areas means that researchers and research institutions have different traditions and potential to move towards open science. In certain fields, the sharing of data, results, methods, models and source code is an important prerequisite for further advancement of research. In other fields and areas, openness requirements may be incompatible with concerns about data protection, confidentiality, national security interests or trade secrets (see 3.3 on export control of knowledge transfer and international sanctions).

Many find that inadequate infrastructure for secure sharing can also be a problem, and there is no 'one size fits all' solution to this, because research data are different in nature, and are subject to different limitations, some of them under different legislative regimes.

Through the Long-Term Plan for Research and Higher Education 2023-2032, the Government has given HK-dir, Sikt and the Research Council the assignment of helping the research institutions to prepare a strategy for Norwegian scientific publication after 2024 and a plan for achieving the

objectives of this strategy. A draft strategy will be distributed for consultation during the period 15 June–15 September 2023.

Opening the research process to greater participation and involvement of different societal actors raises important questions about representativeness, the ability to exert influence and individual considerations. Whereas certain groups may have a political agenda and the potential to exert influence over research processes and results, other groups or individuals may be vulnerable and in need of protection. In interactions with other societal actors, it is important that researchers adopt a role that encourages different types of skills and expertise to supplement each other, based on established standards for quality assurance, data protection, non-discrimination and research ethics.

Proposed assessments and procedures for the institutions' management and administration

- Consider whether guidance and training in data management are required and whether it has been ensured that practices are in accordance with the legislation and applicable codes of conduct. Are systems and infrastructure available?
- Consider how the institution can support the academic environments in their work on open publishing and data management.

Proposed assessments and procedures for the academic environments

- Consider how different aspects of openness can be addressed in the best possible way in accordance with the regulatory framework in situations where other weighty considerations apply, such as national security interests, data protection, legal issues and/or competition considerations.

3 Security management at the institution

The work on responsible international knowledge cooperation should be linked to the institutions' security management structures and form part of their overall risk management work. The institutions must comply with several security management measures set out in laws, regulations and instructions. In this chapter, we begin by looking at the overarching requirements related to security management. We then consider information security and export control in more detail.

3.1 Overarching security management requirements

The Act relating to national security (Security Act) applies to all governmental, county and municipal administrative bodies. Subcontractors, public or private, may also be subject to the Act. The Act applies to all of KD's subordinate undertakings (designation for a legal person/organisation that produces goods/services). The Act requires undertakings to conduct regular risk assessments. The assessment shall form the basis for the implementation of protective security measures required to ensure an appropriate level of security. Responsibility for protective security work rests with the head of an undertaking. It is a requirement that roles and responsibilities at lower levels of the organisation are clearly defined, and that the necessary systems and principles for security management are in place. The Act also requires the undertakings' employees to have a sufficient understanding of and expertise in security. The National Security Authority or authorities with sector responsibility that have been assigned supervisory powers will supervise undertakings that fall within the scope of the Act. Undertakings may be instructed to implement measures.

Since KD's subordinate undertakings are subject to the Security Act, they are also subject to the Regulations relating to the protective security work of undertakings (the Security of Undertakings Regulations). Among other things, the regulations stipulate requirements concerning the handling and protection of sensitive information and critical national objects and infrastructure, a national warning system for digital infrastructure, security requirements in connection with procurements (including requirements that apply to foreign suppliers and procedures for visits from abroad in connection with classified procurements) and personnel security (including the authorisation of persons holding foreign citizenship). The regulations require the necessary resources to be made available for the protective security work (Section 7). The regulations further stipulate that security measures shall not be more invasive than necessary to manage a relevant risk (Section 15).

The Instructions for the Ministries' work on civil protection and emergency preparedness state that all ministries are responsible for security in their own sector. The instructions stipulate that the civil protection work should be managed at the lowest possible level. In practice, this means that KD's subordinate undertakings are responsible for the operational work on civil protection in their field.

KD's Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor (2021) ('Governing document for the work on security and emergency preparedness in the Ministry of Education and Research's sector' – in Norwegian only) describes the work done on security and emergency preparedness in the research and education sector. The security work carried out by KD's subordinate undertakings is subject to a number of requirements. For undertakings in KD's policy area that are subject to more limited control by KD (for example private undertakings), these requirements are formulated as strong recommendations.

All undertakings that are subordinate to KD are required to work systematically and comprehensively on security and emergency preparedness. It is the management's responsibility to provide framework conditions and structures for the work, but the governing document emphasises that a security culture must be developed that involves all employees, raises their awareness and makes everyone accountable. The work must be based on knowledge and experience. Among other things, this involves conducting regular risk and vulnerability analyses (RVA analyses). KD recommends that the undertakings, among other things, take account of the risk and threat assessments from NSM, PST and

NIS in their RVA analyses. The RVA analysis must be followed up by concrete measures set out in an action plan. The undertakings must develop emergency and contingency plans that are reviewed annually and revised as necessary, and they must organise emergency and contingency drills.

The Council for Public Security and Preparedness in the Research and Education Sector, appointed by KD in 2017, has produced a guide to risk and vulnerability analyses in the sector. The guide can be used as a reference work, especially by people who have roles and responsibilities related to the implementation of RVA analyses. The RVA analysis aims to identify and assess risks related to the institution's operations and values/assets, and identify relevant risk mitigation measures. The values/assets can be employees, students and visitors (life and health), information (e.g. personal data and research data), material assets (e.g. infrastructure and buildings), and reputation/credibility. It is part of the RVA analysis to assess the knowledge (data, information) that forms the basis for decisions made.

NSM has developed a guide to security management (in Norwegian only) and other guides, including a guide to valuation of information (in Norwegian only). The Norwegian Agency for Public and Financial Management (DFØ) also has a guide to risk management (in Norwegian only). The aim is to facilitate a shared understanding of what risk is and how it can be managed through measures at the institutional level.

Guidelines for responsible international cooperation developed in other countries, as well as the EU guidelines in the report Tackling R&I Foreign Interference (2022), emphasise the same measures as Norwegian requirements and guidelines relating to security management. It is about ensuring that the work is supported by the organisation's management, ensuring a clear division of roles and responsibilities, regularly updating security management systems and procedures, involving the entire organisation and building an understanding of and expertise in security at all levels. It is also emphasised that the measures must be proportional to the security risk.

It is neither possible nor desirable to endeavour to ensure that international academic cooperation is risk-free, but it is important to implement measures that reduce risk based on good insight into the risk landscape and one's own vulnerabilities. Laws and regulations stipulate overriding requirements for security management, but the individual institution itself must decide how to operationalise the overarching requirements and principles. NSM's guide to security management states that it is the undertakings that must define what constitutes an appropriate level of security for their own organisation. In its governing document for the work on security and emergency preparedness in the Ministry of Education and Research's sector (in Norwegian only), KD also emphasises that security management must be adapted to the different institutions in the sector: 'The design of the management system must be adapted to the values to be protected […] It must be dimensioned in relation to activities that present a threat to security. What constitutes the right design and dimensioning to maintain an appropriate level of security will vary from one institution to another.' (p.35). To succeed, it is also important to build a culture of safety, based on trust between management and employees. Employees must perceive it as safe to report situations that give cause for concern.

Proposed assessments and procedures for the institutions' management and administration

- Has the institution identified assets and infrastructure that may be at risk from international contacts and activities and that need to be protected?
- Has the institution developed systems and procedures to identify and manage different types of risks relating to international cooperation and activities?
- Has the institution considered security measures to reduce an identified risk?
- Does the institution have procedures for upgrading or reassessing the risk assessment?
- Are international cooperation and employee and student mobility covered by the RVA analyses?

- Are international activities covered by the organisation's emergency and contingency plans?
- Does the institution have an overview of partnerships, agreements, funding, experience from mobility stays and collaborative projects, data security, international recruitment of employees, students and visiting researchers?
- Are responsibilities and roles related to risk management in the international work clearly defined?
- Has the institution developed guidelines or other resources to promote accountability in international cooperation?
- Is systematic competence-building and awareness-raising work being carried out in relation to responsible international cooperation in different parts of the organisation, among students and academic and administrative staff?
- Is there a notification (whistleblowing) function in place? Do employees and students know where to turn to if they experience situations that give cause for concern?
- Make a list of countries that are categorised as 'countries of concern' in the annual risk and threat assessments from NIS ,PST, and NSM, register whether the institution cooperates with or is otherwise in contact with these countries, and what forms of cooperation are involved.

3.2 Information security

KD's Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning ('Policy on information security and data protection in higher education and research' – in Norwegian only) summarises the most important statutory requirements and national guidelines in the field of information security. The policy was prepared by HK-dir and adopted by KD in autumn 2020 in circular F-04-20. The policy gives higher education institutions a good overview of the applicable requirements, which are otherwise spread between several acts, regulations and national standards.

The policy, which is aimed at institutions subject to KD's governance model for information security and data protection, sets out the following requirements:

1. Introduce an information security management system.
2. Maintain an overview of information assets.
3. Conduct risk assessments and establish security measures.
4. Establish solutions for incident management, continuity and the closure of non-conformities.
5. Ensure control of service providers.
6. Ensure internal control of the processing of personal data.
7. Safeguard the rights of data subjects.
8. Appoint a data protection officer.
9. Carry out data protection impact assessments.
10. Ensure data protection by design and information security.
11. Provide training and competence-building.
12. Document the work on information security and data protection work.

HK-dir conducts an annual survey of the institutions' compliance with the requirements set out in the policy.

NSM has developed core principles for ICT security ('Grunnprinsipper for IKT-sikkerhet' – in Norwegian only) as a means of protecting information systems against unauthorised access, damage or misuse. These principles are relevant for all Norwegian enterprises. NSM points out that digitalisation creates both opportunities and risks, and that the core principles of ICT security will help institutions in their digitalisation work.
The main target group for NSM's core principles is IT management and middle management, since they are the crucial link between senior management and the implementation and operational level.

The report Informasjonssikkerhet og personvern i høyere utdanning: Risiko- og tilstandsvurdering ('Information security and data protection in higher education: Risk and status assessment' – in Norwegian only) is an annual report published by HK-dir that provides an overview of the current

threat landscape in the Norwegian research and education sector. More and more Norwegian enterprises in the public and private sectors have been exposed to intentional digital attacks and more and more serious digital security incidents are being registered. NSM points out that states or state-sponsored threat actors are behind several of the incidents. In their risk and threat assessment, the intelligence, surveillance and security services (NSM, PST and NIS) emphasise that the threat landscape in Norway has become more serious and point to several specific areas of research and development that may be particularly vulnerable to digital attacks and knowledge espionage.

The services point out that the greatest threats come from Russia, China and Iran. In the wake of Russia's invasion of Ukraine, both NSM and PST believe that the foreign intelligence threat from Russia has increased.
Informasjonssikkerhet og personvern i høyere utdanning og forskning (2022) ('Information security and data protection in higher education and research' – in Norwegian only) provides examples of confirmed or suspected cases of state-sponsored hacking in the university and university college sector in 2021: regular attempts to break into the institutions' computer networks ('brute-force attacks'), reconnaissance activities (threat actors mapping the institutions via the internet, e.g. system service messages and other publicly available information about information security work), exploitation of software vulnerabilities to gain access to account passwords, including administrator accounts, and to other computers connected to the same network. Researchers at Norwegian higher education institutions enjoy a high degree of autonomy, and individual researchers often engage in networks with national and international contacts in their field. In addition to organised cooperation, there is also informal exchange of knowledge and information. This provides possibilities, but can also compromise the institution's security.

It is necessary to strengthen digital security expertise at the departmental level, and the guidelines below are therefore aimed at both the management level and the individual employee. The guidelines are already part of established management systems for information security and data protection.

Selection of the digital platform for project cooperation

The institutions need a common digital platform to communicate and interact with partners at the start of and during a collaboration project. The digital platform is used for storing project documentation and to hold and document project meetings.

It can be challenging if the cooperating institutions use software that may be unknown to Norwegian participants and where it is unclear whether the solution meets the Norwegian legal requirements for information security and data protection.

Proposed assessments and procedures

- The institutions should include an overview of the digital platforms that will be used during the project period in the cooperation agreement signed prior to start-up of a project.
- The participating institution that functions as the project's data controller vis-à-vis the digital platform that the project will use should document the following:
    - Will the digital platform be used to process personal data? If yes, what types of personal data?
    - What is the purpose of the processing of personal data?
    - Is it necessary to have a solution for registering the consent of the data subject?
    - Has a privacy statement been prepared for the digital platform?
    - What security measures for accessibility, integrity and confidentiality are used for the digital platform? Has a risk assessment been carried out?

    - What is the data flow on the digital platform? Is it integrated with other digital platforms?
    - What cloud services are used on the digital platform?
    - Which legal entity is responsible for the technical operation of the digital platform? Is there a data processing agreement in place?
    - For how long are logs from the digital platform stored?

- Based on the documentation submitted, the institution participating in the project should implement a procedure to assess whether the digital platform should be used during the project period. The assessment should be carried out at a different level from the project group or research group in question.

Selection of digital platform for data collection in project cooperation

The institutions need a secure digital solution for data collection. Various digital solutions are used for collecting and storing data.

The choice of digital interaction platform is also relevant here. It is therefore recommended that the questions and assessments described above be used to carry out an assessment before a digital solution for data collection is used at the Norwegian institution participating in the project.

Proposed assessments and procedures

- The institutions should include an overview of the digital platforms that will be used during the project period in the cooperation agreement signed at the start of a project.

- The participating institution that has the role of data controller vis-à-vis the digital platform that the project will use should enclose documentation as described above.

- Based on the documentation submitted, the participating institution should implement a procedure to assess whether the digital solution for data storage should be used during the project period. The assessment should be carried out at a different level from the project group or research group in question.

Access to the institution's digital information assets for foreign researchers and visiting researchers

The institution's digital information assets should be safeguarded through organisational and technical measures. The Ministry of Education and Research and NSM point out that Norway and Norwegian research are increasingly under threat from foreign intelligence activities. It can be challenging for individual employees to have a sufficient overview and knowledge of the applicable security measures. This can lead to unauthorised access being granted to information that should be protected.

Proposed assessments and procedures

- Regular asset mapping: The institutions in the Norwegian higher education sector map information assets and the necessary level of protection. This mapping is usually carried out by the central administrative departments. It is proposed that the administration assist with the implementation of corresponding asset mapping, for example at departmental level, to map the most important digital information assets (including where they are stored) before the start of an international cooperation project, or prior to welcoming a foreign visiting researcher.

- Institutions should ensure that current access management procedures are aligned with the mapping of assets. This is especially important when new partners join existing projects.
- The institutions should ensure that the applicable procedures for background checks when appointing researchers from countries that may pose a security risk, or foreign researchers in management positions, or positions that are authorised to make major financial decisions, are updated in line with the mapping of assets. In special cases, background checks are also required in connection with appointments regardless of country of origin. Factors such as the individual employee's financial obligations may constitute a security risk.

Exchange of personal data in connection with researcher and student mobility

Mobility is based on different types of cooperation in the form of, e.g., partnerships, research work and different mobility schemes.

The institutions need a common digital platform on which to exchange information about Norwegian students who are going on an exchange or foreign students coming to study at Norwegian educational institutions. In many cases, both the home institution and the host institution have access to the same Learning Management System (LMS), e.g. Canvas, which enables secure processing of personal data.

It can be a challenge if the institutions that are going to cooperate on a student exchange do not have access to the same system. In some cases, the institutions use email to send personal data about students, a solution that the Norwegian Data Protection Authority is critical view of as it will in most cases not comply with GDPR requirements.

All Norwegian universities, Universities Norway (UHR) and a number of university colleges collaborate on the management of the Scholars at Risk scheme. Norwegian universities and university colleges also cooperate on the Students at Risk scheme.
The main purpose of these schemes is to protect academics and students under threat, provide them with a safe haven and promote academic freedom. Educational institutions need a secure solution for the transfer of personal data in connection with the nomination, admission and reception of threatened researchers and students.

Proposed assessments and procedures

- Consider whether the exchange of personal data is sufficiently secured.
- Consider Sikt's web application, which can be used by Norwegian educational institutions to exchange personal data in a secure manner: Nomination - Felles studentsystem
- Consider the University of Oslo's online form service Nettskjema for the secure transfer of personal data.

3.3 Export control of knowledge transfer and international sanctions

Through international treaties, Norway has undertaken to prevent the proliferation of chemical and biological weapons, prevent the proliferation of goods and technology relevant to nuclear weapons, and control conventional weapons, military goods and sensitive high tech.

This is enshrined in the Act relating to Control of the Export of Strategic Goods, Services, Technology, etc. (https://lovdata.no/dokument/NLE/lov/1987-12-18-93) from 1987 and operationalised in Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester (eksportkontrollforskriften) ('Regulations relating to the export of defence materiel, dual-use items, technology and services (Export Control Regulations)' – in Norwegian only). The Ministry of Foreign Affairs (UD) is responsible for providing guidance on knowledge transfer and whether it will trigger a licensing requirement.

In addition, UD administers sanctions regulations that regulate Norway's obligations to implement sanctions adopted by the UN Security Council, as well as certain restrictive measures adopted by the EU. The regulations are based on Lov for gjennomføring av internasjonale sanksjoner ('Act relating to the implementation of international sanctions' – in Norwegian only). Such sanctions could affect international knowledge cooperation, for example as regards money transfers or the use of equipment.

Export control has two purposes:

- To ensure that exports of defence materiel from Norway are in line with Norway's security and defence policy.
- To ensure that exports of dual-purpose goods do not contribute to the proliferation of weapons of mass destruction (WMD – nuclear, chemical and biological weapons), as well as means of delivery for such weapons. Means of delivery can include underwater technology, advanced electronics and materials. 'Dual-use items' refers to items, software and technology that were originally designed for civilian purposes, but that can have important military applications.

In practice, the regulations mean that materiel, technology and knowledge with a military application must be approved by UD, which issues a licence or prior authorisation before such materiel and technology can be exported from Norway.

In recent years, threat assessments from PST and NIS have shown that some states are trying to acquire knowledge that can be used for military purposes, in violation of national security and defence policy interests. Such attempts can, for example, take place by placing and recruiting their own citizens in advanced educational and research environments. The fight for access to knowledge and research is at the heart of the geopolitical rivalry and the race to translate new technologies into military capabilities.

The Government has therefore decided to amend the Export Control Regulations in order to strengthen control of the transfer of knowledge that can be used in weapons of mass destruction, their means of delivery and conventional weapons.

The regulations are under revision, and UD distributed a draft version of the amended regulations for consultation on 28 March 2022. Nearly 40 consultation submissions were received. The regulatory amendment work has not been completed, and the guidelines below are therefore based on the existing regulations. The guidelines for responsible international cooperation in the field of export control will be updated once the Ministry of Foreign Affairs has completed its work. Until the amendments enter into force, the current legislation and practice apply. Updates will be published on UD's website.

In 2016, UD prepared separate export control guidelines for the research and education sector (in Norwegian only). Export control in the sector mainly concerns control of knowledge transfer and research cooperation, with pertaining mapping of equipment and technology that require a licence, as well as awareness of data security in relation to student and staff exchanges and

visiting lecturers. Research and educational institutions must comply with the export control rules, and the following measures are recommended in this connection:

- Obtain an overview of which knowledge areas are regulated by export control legislation.
- Obtain an overview of which international cooperation activities, educational levels and positions in the institution the export control regulations will apply to.
- Identify which equipment, lab facilities and information require additional protection in the form of access control, and develop security systems to safeguard these assets.
- Develop internal procedures that ensure control of knowledge transfer in all activities associated with the sensitive subject areas.

It is important to specify that knowledge transfer control does not apply to knowledge that is already openly available 'in the public domain'. Export control also makes an exception for basic research. The concept of basic research is defined in lists I and II as 'experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena […] not primarily directed towards a specific practical aim or objective.' In other words, basic research should not lead to the development of a product or have a practical industrial use, but can, for example, consist of the observation of phenomena in nature or similar. The definition of basic research used in the regulatory framework governing export control is negotiated in the multilateral export control regimes Norway participates in and is a definition we are obliged to comply with.

The opposite of basic research is 'applied research', which is primarily aimed at specific practical objectives, technological development or applications. Applied research can be covered by the definition of dual-use items or dual-use purposes. There are few Norwegian resources in dual-use technology beyond list II. It may be useful to examine the tool Stanford University has developed for export control. A similar resource is Germany's manual developed for academia in the export control field that can be used to methodically investigate whether the research field is subject to export control. Separate software has also been developed that is commercially available in Norway for searches in list II dual-use technology to make it easier to find out whether the research requires prior permission. Dual-use purposes in the Export Control Regulations are a demanding field since the areas of knowledge pertaining to dual-use potential have become more extensive. Claims that Russia removed computer chips from washing machines and refrigerators to repair its military equipment are an example of this. In addition, these areas that are changing in step with knowledge development and international negotiations in the export control field.

The current control system also has a limitation related to the level of education, and is mainly aimed at the doctoral degree level, and at master's degree level in certain disciplines that are covered by the regulations (3. Study programmes and particularly relevant disciplines).

In research cooperation, the export control rules apply to the sharing of information and research results with foreign institutions. For knowledge covered by the Export Control Regulations, information sharing at courses and conferences may trigger a licensing requirement or requirement for prior authorisation in accordance with the regulations. Based on estimates from Sweden and the United States, it is assumed that less than ten per cent of research projects should apply for an export licence, and that approximately two per cent of the projects will be problematic in terms of export control.

Norwegian universities have organised their efforts to comply with the Export Control Regulations in different ways. The Norwegian University of Science and Technology (NTNU) has developed its own resource pages for this work, with a dedicated contact point at the institution. The Norwegian University of Life Sciences (NMBU) has developed security procedures for entering into international cooperation which all employees must complete before the cooperation commences. These procedures are used to identify possible instances where the Export Control Regulations may apply. Security officers at the institution contact an expert for more detailed advice and information about

the application procedure for prior authorisation. The University of South-Eastern Norway has established a dedicated team that works on export control at the university.

As the knowledge transfer regulations are practised, the knowledge institutions are required to carry out a special assessment of doctoral research fellows and when choosing international partners, recruiting foreign researchers and inviting visiting researchers in the subject areas listed in the Guidelines for the control of knowledge transfer. In addition, these subject areas should be included in the institutions' valuation of assets and risk analyses with regard to access control and protection of critical infrastructure.

The lists of subject areas mentioned in the Guidelines for the control of knowledge transfer are not exhaustive. In addition, educational institutions must, on a general basis, be cautious when foreign students apply for admission to doctoral positions or master's degree programmes in other technology areas covered by the Ministry of Foreign Affairs' list of goods II and could thus pose a particular risk in terms of the proliferation of WMD or their means of delivery. In certain cases, the Ministry may trigger a licensing requirement and thus refuse the export of non-listed goods, technology or services (see the 'catch all' extended licensing requirement) (in Norwegian only).

Assessments must therefore be carried out when recruiting academic staff (including PhD students), receiving visiting researchers and admitting students to certain courses at master's degree level. The Directorate of Immigration (UDI) processes applications for work permits. The applications must be assessed in relation to matters affecting national security, which are set out in the Act relating to the admission of foreign nationals into the realm and their stay here (the Immigration Act) , Chapter 14 and Regulations relating to the admission of foreign nationals into the realm and their stay here (the Immigration Regulations) Chapter 19A. The case processing is described in GI-03/2023 – Instruks om behandling av saker som kan berøre grunnleggende nasjonale interesser eller utenrikspolitiske hensyn etter utlendingsloven kapittel 14, og saker etter eksportkontrollregelverket ('Instructions concerning the processing of cases that may affect fundamental national interests or foreign policy considerations under Chapter 14 of the Immigration Act and cases pursuant to the export control rules' – in Norwegian only). It also gives an indication of what information should be included in connection with a residence permit application.

The Council for Public Security and Preparedness in the Research and Education Sector has prepared a memo on export control (in Norwegian only) as a guide for the sector until new regulations are in place. Sikresiden.no has also created a separate e-learning course on export control.

Proposed assessments and procedures for the institutions' management and administration

- Incorporate export control as part of the institution's risk management. Consider assigning responsibility for export control to dedicated persons at the institution. However, it is important that the institution's security work is endorsed by the management.
- A valuation of the research areas forms the basis for which security measures must be introduced in order to comply with the regulations. The scope of values/assets covered by the Regulations should be used to dimension administrative support and control systems in this field.
- Map sensitive research areas, cooperation projects, interdisciplinary activities, master's and PhD programmes, laboratories and equipment.
    - Consider whether the academic environments covered by the Export Control Regulations are sufficiently familiar with them.
    - Ensure regular updates and familiarity with internal export control procedures in the relevant academic environments.
    - Consider the need for (enhanced) access control to laboratories and equipment.

    - Obtain an overview of equipment that requires a licence that is included on list II in the Export Control Regulations and sanctions and restrictive measures.
- The knowledge institution should have an overview of countries subject to sanctions that may entail restrictions on international knowledge cooperation. Note that prior authorisation must always be applied for in order for persons with Iranian nationality/connections to Iran to use the equipment/technology/knowledge listed in the annexes to the Iran Regulations.
- Consider introducing standardised background checks for employment in subject areas and positions covered by the Export Control Regulations (see also section 4.1 Recruitment and appointment).
- Consider whether positions with expanded authority, rights and access should be routinely authorised through a background check.
- If an educational or research institution is concerned that illegal knowledge transfer has taken or may take place, contact the Police Security Service for further dialogue and advice.

Proposed assessments and procedures for the academic environments

- Is your subject area on the list of knowledge areas covered by the Export Control Regulations?
- Does your research, teaching or international project cooperation depend on the use of a laboratory/technology/equipment/software that is on List II – dual-use technology?
- Can the knowledge developed through the collaboration have a potential military application (including delivery technology)?
- Is the country involved in the planned knowledge cooperation covered by the sanctions regulations? Consider possible implications for the cooperation.

To comply with the regulations that apply to sensitive knowledge and technology areas, UD must be contacted before knowledge transfer can take place with people from certain countries. In its assessments, UD treats each individual inquiry individually. UD should only be contacted once the institution has made its own assessment of whether the cooperation, considering the subject areas and nationality involved, falls within the scope of the provisions relating to export control of knowledge transfers. The assessments should be made in light of the partners involved and the project's research funding.

Applications for prior authorisation must be submitted via UD's electronic application portal e-lisens, using the form 'prior authorisation knowledge transfer'. The Ministry's Section for Export Control considers the applications. The e-lisens portal can also be used to submit general enquiries and questions related to export control.

4 Employees and students

4.1 Recruitment and appointment

Norway relies on international recruitment to meet its qualification needs in several disciplines. Including background checks in appointment procedures provides an opportunity to ensure that the information given in the application is correct. Background check procedures means that the institution must have carried out a valuation and a risk assessment to determine which positions, information, subject areas and infrastructure it is important to regulate access to. The legal basis for background checks is the employer's responsibility to appoint the right person to the position and the applicant's consent when applying for a position that requires specified qualifications, or the applicant's explicit consent to the collection of background information. What information an employer may collect will vary depending on the nature of the position, including the qualification requirements and other legal or contractual requirements that apply.

- The right to obtain additional information depends on the nature of the position and whether there are any restrictions in law, regulations or principles. There are restrictions on the right to obtain information about an applicant. They are set out, for example, in the Working Environment Act and the Equality and Anti-Discrimination Act, cf. *inter alia* the Working Environment Act Section 9-3 first paragraph and Section 13-4 first and third paragraphs, as well as the Equality and Anti-Discrimination Act Section 30 first paragraph. There are some exceptions in the individual provisions.
- The employer may not emphasise information that it is not possible to obtain pursuant to law, regulations or principles, even if such information has been provided with the job seeker's consent.

Background checks usually consist of four main parts: identity checks, verification of education and work experience, credit checks and business interests, as well as searches in open sources. The background check that is carried out should be appropriate to the position that is advertised. It is important that applicants are informed that a background check can be carried out, and what this means, and that written consent is obtained from the applicant before a background check is carried out. Some institutions choose to buy background check services, and OsloMet has developed its own resource page for accountability in recruiting and receiving visiting researchers (in Norwegian only).

If the position is in a discipline or subject area relevant to the Export Control Regulations for knowledge transfer, it is particularly important to consider security and to carry out a risk assessment when the position is advertised. The proposals below are based on the Veileder for sikkerhet i ansettelsesforhold ('Guidelines for security in employment relationships' – in Norwegian only), developed by PST, NSM, the police and the Norwegian Business and Industry Security Council. See also the Norwegian Data Protection Authority's resource page for background checks (in Norwegian only).

Internationally, useful tools and information have also been developed in connection with the recruitment and appointment of researchers: the Human Resources Strategy for Researchers (HRS4R) and the European Charter for Researchers and a Code of Conduct for the Recruitment of Researchers. The latter resource specifies general requirements for the researcher role and associated rights and obligations.

Proposed assessments and procedures for the institutions' management and administration

- Consider which positions/areas of responsibility at the institution require background checks.
- Develop a procedure for background checks at the institution to standardise procedures in accordance with regulations (e.g. for export control of knowledge transfer and the Equality and

Anti-Discrimination Act) and ensure that responsibility for background checks is assigned in the organisation.

- In the absence of the resources required for satisfactory background checks, in-depth discussions of academic issues can help to verify that the person has the background they claim to have. Bibliometrics can also be used, to analyse both people's and institutions' possible ties.

- Prior to employment, applicants for the position should be informed that the Export Control Regulations could affect their professional development and work. This applies in particular to disciplines covered by the Export Control Regulations for knowledge transfer. The institution may consider incorporating this reservation as a separate clause in the employment contract.

4.2 Protecting employees

Employees may have ties that, under certain circumstances, could put their academic work and values/assets under pressure. Citizenship is one example, but international networks, dependent relationships between parties and sources of funding are also examples of ties that could in certain situations make employees vulnerable. Temporary employment can also make people vulnerable to influence, which can put research integrity and academic freedom under pressure. Additional roles such as ownership interests in companies or board office can lead to conflicts of interest and conflicting pressures.

Focusing on risk and security at research and educational institutions could entail a risk of stigmatisation of foreign employees from countries that have been named as security threats against Norway. The emphasis on risks can in some cases go too far and result in arbitrary exclusion and discrimination of foreign employees and students at Norwegian institutions. If the institution has good security procedures in place to protect its most important institutional assets, it is easier to avoid suspicion being cast on international staff members. It is also important that the proportionality of risk management is discussed at the institutions and in the academic environments, and that possible discrimination against foreign employees and students is put on the agenda.

Foreign employees and students who are citizens of countries of concern that are known to pressure their citizens abroad into providing information may need follow-up from the institutions. They should be informed about the dangers and be told who they can contact at the institution if they are put under pressure and need help. Some research environments in the technology field carry out routine vulnerability interviews with employees after business trips to high-risk countries based on the person's background and/or field of work. For an overview of possible dangers and areas where insider threats can occur, see the resource pages at sikresiden.no.

New foreign employees often need help and support to navigate the Norwegian system. Some institutions have dedicated contact points that have been established to help these employees with practical challenges ranging from acquiring a bank card to how to apply for a kindergarten place. It is the institutions' responsibility to inform foreign employees about the laws and regulations that apply to the research and education sector in Norway and the institution's export control and security procedures.

Proposed assessments and procedures for the institutions' management and administration

- Consider whether to establish special procedures for informing new employees about the Export Control Regulations, research ethics and academic freedom, etc.

- Consider whether to develop special online resources for international cooperation that provide an overview of the institution's procedures and resources.
- Consider having one or more notification contact points that employees and students can contact if they are subjected to pressure from external actors or face ethical dilemmas in connection with international cooperation.
- Consider whether the obligations of the employment relationship and the consequences of violating the institution's guidelines are made sufficiently clear in employment contracts.
- Introduce measures that ensure that the employee knows the extent of the values/assets they are managing and understands the risks associated with the research field in connection with international cooperation.
- Consider whether to introduce vulnerability interviews with employees. Develop special procedures for such interviews. The procedures should describe the purpose of the vulnerability interviews, when and how they should be conducted, and which employees or groups of employees form the target group (see also NSM's personnel security guide – in Norwegian only).
- Consider whether it is necessary to strengthen the procedures for foreign travel for employees and students, especially to countries that do not have security cooperation with Norway (see also the travel advice at sikresiden.no).

4.3 Employees' responsibilities

Several international universities have developed a Code of Conduct to clarify the obligations of academic staff. Some universities have developed a similar code for their students. In that connection, the institutions have established a contact point that employees and students can contact if they are exposed to pressure or face difficult dilemmas. In Norway as well, a number of institutions have created their own frameworks for cooperation and for their employees. NTNU's code of ethics for employees is one such example. OsloMet – Oslo Metropolitan University has recently developed its own Code of Conduct for international cooperation (in Norwegian only).

It is crucial that employees are able to assess the risks associated with different situations and to reflect on their own ties and vulnerabilities. Such vulnerabilities may result in employees being pressured to act contrary to national security interests or the export control regulations. Academic staff should be trained to reflect on ethical dilemmas and difficult situations they may face as part of international cooperation. Researchers must also know who to contact at the institution if they experience pressure and threats, or if they suspect that colleagues and partners are acting unethically and putting research integrity at risk. It is important that such inquiries are not met with sanctions and punitive measures, but that staff are encouraged to report such matters based on the trust an employment relationship entails. Mistakes are made in all organisations, and it is therefore important that a culture is created where staff report when mistakes have been made or unethical behaviour is suspected, so that the institutions can limit the extent of the damage.

Proposed assessments and procedures for management and administration

- Consider creating an external activities register that maps employees' work for other institutions, offices and ownership interests to maintain an overview and create awareness of possible conflicts of interest and vulnerabilities. This register should be updated during the employment relationship. The register can reveal whether the researcher has secondary positions at international institutions in countries of concern or has ownership interests in companies that may represent a challenge with regard to their independence in certain research projects.

- Establish procedures in which the potential impact of additional roles on international cooperation on research and education is assessed and managed in the planning and implementation of cooperation projects.

Proposed assessments and procedures for the academic environments

- Consider whether your ties (additional roles, close relationships, funding, citizenship, etc.) could adversely affect your research activity, teaching activity, or create a loyalty conflict in your employment relationship. Seek advice from your immediate superior and take steps to reduce vulnerability to an acceptable level.
- If you find that your academic work is being put under undue pressure, contact your immediate superior, security officer or the institution's integrity committee.
- If any external actors ask you to share information that you are not sure you should share with outsiders, contact the security management at your institution and possibly PST.
- If you have experiences on trips abroad or in other situations that make you vulnerable to pressure, inform your immediate superior and/or the security officer at your institution for advice and support.
- If you suspect that any of your colleagues, visiting researchers or partners are acting unethically, contact your immediate superior, security officer or the integrity committee at your institution.

4.4 Inviting and safeguarding visiting researchers

The same advice applies as to hiring and safeguarding employees, insofar as appropriate. The duration of the stay and the need for access to physical infrastructure such as laboratories, equipment, data and other personnel, are factors that should be considered before simplifying procedures.

Visiting researchers are a source of vulnerability at Norwegian institutions because they are sometimes only subjected to a very simple background check before arriving. Visiting researchers from countries with which Norway has no security policy cooperation can be particularly vulnerable and may be subjected to pressure. Regulation of access can make both the institution and the visiting researcher less vulnerable. This advice also applies to guest lecturers, as far as appropriate. For longer stays, institutional cooperation agreements can also be entered into where security is a topic. It is important that employees who invite visiting researchers familiarise themselves with the institution's policies and report any worrying behaviour.

Proposed assessments and procedures for the institutions' management and administration

- Consider the need for an overview of visiting researchers at the institution.
- Consider access regulation for visiting researchers with regard to physical (areas at the institution such as labs and evening/night access) and digital access.

4.5 Employees abroad

If you have employees who work abroad, this introduces many new factors to the risk assessments, as well as new rules and regulations to comply with. If an undertaking has employees in another country, the employees in question may lose their membership of the Norwegian National Insurance scheme. The undertaking must comply with the laws and regulations of the country of work as regards tax, social security, sick leave, insurance, labour law, and registration and reporting obligations in the country. There may be issues related to work permits and visa requirements. Establishing a business abroad can also entail tax and reporting obligations for employers. It also has a bearing on employee follow-up and management. OsloMet has separate agreements between employees abroad and their immediate superiors to ensure the security of personal information and equipment.

It is important that institutions take responsibility as an employer for their employees abroad, including following up their obligations in relation to both the employee and the laws and regulations in the country of work. As the responsible employer, the institution should have good internal procedures and an overview of where the employees are at all times, so that they can quickly assist employees when needed. The institution should have clear contingency plans for employees who are abroad.

Employees who are travelling in countries with which Norway has no security policy cooperation should carefully consider what information and electronic equipment they take with them. Both computers and phones are vulnerable. It can be a good idea to carry an extra emergency phone, as more and more countries base both transport and payments on mobile phone solutions. If an employee is locked out of their phone, it can be difficult to carry out planned meetings and trips, show vaccination certificates, maintain contact with the employer, etc. Assessments and procedures related to students abroad may also be relevant for employees (see section 4.5 Students abroad).

4.6 Students abroad

The Norwegian authorities have ambitious goals for how many students should go on exchanges, also to priority countries outside Europe. Report No 7 to the Storting (2020-2021) En verden av muligheter – Internasjonal studentmobilitet i høyere utdanning ('A world of opportunities – International student mobility in higher education' – in Norwegian only) sets the goal that 50% of Norwegian students should go on an exchange at some point during their education. The white paper also emphasises the institutions' responsibility for their students' safety while they are abroad and the students' own responsibility when choosing their host institution. The institutions are responsible for informing and advising students about opportunities and restrictions before they leave, as well as for clarifying what the students themselves are responsible for.

Universities and university colleges' responsibility for students in general, including students on exchange stays abroad, is regulated through the Act relating to Universities and University Colleges and the Academic Supervision Regulations. According to the Security Act , state universities and university colleges are responsible for addressing information security, including during exchange stays. The institutions are required to have contingency plans that are up to date at all times, as described in Styringsdokument for arbeidet med sikkerhet og beredskap i Kunnskapsdepartementets sektor ('Governing document for the work on security and emergency preparedness in the Ministry of Education and Research's sector' – in Norwegian only).

According to the NUPI report Challenging Knowledge Cooperation (in Norwegian only), the institutions know little about students' experiences during their stays abroad. At the same time, some respondents in the study express concern for the students. The proposed assessments and procedures set out below are limited to students who travel under institutional agreements and/or within the framework of partnerships.

Proposed assessments and procedures for the institutions' management and administration

- Include students on stays abroad in contingency plans. Have any security challenges relating to gender, skin colour, sexual orientation and vulnerable minorities been considered in connection with stays abroad?
- Ensure data protection when transferring personal data to third countries (GDPR).
- Ensure that students can acquire sufficient information about the country and the contextual understanding needed for their stay abroad for their own safety and learning (before, during and after the stay). The safety of partners and fellow students must also be considered.

- Establish reporting procedures for incidents that challenge personal safety, information security or academic values.
    - Can procedures for submitting incident reports be incorporated into existing structures with regard to responsibility for follow-up and risk management (contract managers, people with academic responsibility etc.)?
    - How should notifications be systematised and followed up at the institutional level (responsibility, follow-up, privacy, etc.)?
- Clarify what contact points are available at the host institution abroad.
- Encourage students to register on UD's travel app, 'Reiseklar'.
- Encourage students to take out insurance and to consider making contact with and/or membership of the Association of Norwegian Students Abroad (ANSA).

4.7 Protecting students

Academic freedom must be ensured for all students and employees at Norwegian institutions, both in the context of international cooperation and otherwise. All students and employees must know what academic freedom entails. In its report Academic freedom of expression, the Kierulf Committee has included a proposal for a declaration of academic freedom of expression and ground rules for free speech for the research and education sector. Institutions should consider whether they have good systems in place to help students who find that their academic freedom is threatened or under pressure.

Proposed assessments and procedures for the institutions' management and administration

- Inform students about academic freedom, prerequisites for creating a good climate of expression and research ethics principles. Include students in relevant training programmes.
- Establish a clear contact point at the institution to which students can turn for help and support if they find themselves under pressure or surveillance.

5 Partnerships and agreements in the research and higher education field

5.1 Partnerships in the research field

By partnership is meant cooperation at the institutional level that extends beyond a single cooperation project. The information in this section, and especially information pertaining to agreements, can also be used to assess individual projects, and several of the assessments will be relevant to cooperation on both research and education, including with health trusts and companies.

Successful knowledge cooperation partnerships are often characterised by long-term cooperation and close and trusting communication between the partners. However, experience varies between institutions and between individual researchers, and there are few or no common Norwegian guidelines on how to ensure a good partnership over time. It will often depend on the persons involved, and a partnership between institutions should have the support of management and the academic staff.

Equitable partnerships have become increasingly important in the discussion about knowledge cooperation and cooperation between researchers and institutions. This is particularly relevant for cooperation between high-income countries and low- and middle-income countries (LMIC), where funding often goes through Norwegian education and research institutions that are responsible for the financial and administrative follow-up of a project. The starting point for cooperation with local partners in LMICs is therefore often based on an imbalance of power, where the project owner in Norway defines the parameters for the cooperation. It is important to be aware that an imbalance of power can also be to the disadvantage of the Norwegian academic environments, since Norway is a much smaller country than our priority partner countries, with fewer specialised academic environments and limited financial means at the institutions' disposal. In cases where the education and research activities are carried out in other countries, local knowledge and contact networks are also a source of influence.

To strengthen work on equitable partnerships, the UK Collaborative on Development Research (UKCDR) and ESSENCE on Health Research have developed a practical guide that research funders, research institutions and researchers can use in their work. Equitable partnerships are about recognising the partners' competence and giving them real opportunities for responsibility, development and competence-building, which will strengthen all partners in a project.

It is important to ensure a fair allocation of budgets, which should also cover administrative support and other indirect costs. Plans for mobility, data management, access, crediting and the dissemination of results, IPR management and data protection should be developed early and jointly to safeguard the rights of all partners and provide predictability for researchers who join a partnership after it has been established.

The European Commission applies the Global Code of Conduct for Research in Resource-Poor Settings (GCC) when funding research conducted in low-resource settings. The code of conduct promotes principles such as fairness, respect, care and honesty. This is also closely linked to research ethics considerations relating to cultural differences, risks of exploitation, involvement of vulnerable groups and local partnerships when conducting research in other countries. In Norway, the National Research Ethics Committees have developed research ethics guidelines that can be a good help for researchers planning research in low- and middle-income countries, but also in other countries.

Proposed assessments and procedures for the institutions' management and administration

- Both the short-term and long-term benefits of the partnership should be described.
- Consider whether to establish administrative support to allow academic staff to develop equitable partnerships in connection with:

    - The development of cooperation agreements
    - Preparing budgets and allocating costs
    - Measures to reduce risk, e.g. of financial dishonesty on the part of a partner, through prior due diligence and procedures for regular follow-up
    - Plans for responses to unforeseen incidents: termination of or adjustments to project plans
- Cooperate with administrative staff at the partner institution to achieve a mutual understanding of, e.g., the budget, accounting procedures, reporting, hiring and legislation.
- Check possible links and ties between the partner and the state, the intelligence service and military in the country in question, especially for countries with which Norway does not have security policy cooperation. This also applies to owners when the partner is a business, and to companies owned by the business.
- Carry out due diligence of the partner (mapping of activities, the sector in which the organisation operates, a commercial and ethical assessment of the institution's/enterprise's management and framework conditions):
    - Does the partner have a specific political, ideological or commercial agenda that should be taken into account?
    - Is the partner, including its employees or persons that serve on its governing bodies, linked to military activities or companies with an unclear profile?
    - What kind of relationship does the partner have with its own authorities, national or local?
    - What kind of decision-making structures does the partner have?
    - Check any previous relationships with foreign partners. Are there any issues or incidents that have caused problems?
    - Is the partner committed to following rules or norms for ethical conduct, transparency, openness, and academic freedom?
    - Is the partner in a sound financial situation, and does it have good and reliable operating systems?

- Be sure to collect enough information to be able to assess the risk to your own values and assets, security and reputation. This includes laws and regulations in partner countries for data sharing, personal data and intellectual property rights. Sometimes local laws and regulations will also be relevant.
- Do stays with the partner organisation entail any particular risks to researchers or students? Such risks can be related to nature, society or politics.
- Is a residence permit or visa required? What type of permit or visa is required? As regards mobility to Norway, see www.udi.no.
- Consider the distribution of risk in the project. This applies to all academic and administrative risks, not just risks associated with responsible international cooperation.
- Consider whether values such as academic freedom should be included in agreements, cf. chapter 2.

Proposed assessments and procedures for researchers and academic environments

- Start the planning as soon as possible so that you have as much time as possible to develop cooperation methods. Ensure a fair distribution of funds and institutional costs among the partner institutions. Ask for information about the partner organisations' own calculation models and cost estimates when you prepare the budget. All partners should be included from the start and be involved in the development of:
    - Research questions
    - Methods
    - Plan for the use of infrastructure and equipment, including digital infrastructure

    - Data management plans
    - Rules for crediting and authorship
    - Division of intellectual property rights
    - Networking activities
    - Plans for dissemination
- Involve users from an early stage to ensure relevance and benefits. This includes users in the countries where the research is carried out.
- Are there cultural differences that can lead to inaccurate wording of an agreement, or a lack of a shared understanding of measures that can be implemented in a given problematic situation?
- Are there differences in legislation, e.g. related to personal data, that must be taken into account?
- Consider the dual-use potential (see section 3.3 on export control).
- Identify opportunities for commercial exploitation of the results.
- Determine whether strategies are needed in relation to intellectual property rights. The development of patents can be an explicit political goal in other countries. A patent ensures time-limited protection of a concrete idea in exchange for publication and a detailed description of the idea. The easier the idea can be copied, the greater the likelihood that the patent rights will be infringed. If you apply for a patent, you should be prepared to defend yourself in the courts if the patent is infringed, with the financial consequences this will have. See more about the protection of trademarks, designs and patents on the Norwegian Industrial Property Office's website.

5.2 Partnerships in the higher education field

Higher education institutions are often hierarchical, bureaucratic and conservative systems that largely reflect the values and political ambitions of each country's system of government. The status of students will also largely reflect this set of values, which can be expressed through educational approaches, student-teacher relationships, data protection, etc.

Developing well-functioning international cooperation on education can take a long time. Establishing as predictable and stable framework conditions as possible is crucial to the formation of long-term relationships that can lay the foundation for further cooperation after individual projects or other time-limited activities have been completed.

And, not least, a long-term perspective and institutional support are important if binding cooperation is to be established, especially as regards more ambitious forms of educational cooperation such as joint study programmes and joint degrees. Here, the institutions' administration also plays a central role in relation to development, system knowledge and quality assurance.

Proposed assessments and procedures for the academic environments

- Define the purpose of the cooperation. What are the reasons for the choice of country/countries and partner(s) in terms of added value through cooperation on higher education?
- Are the partners in question accredited and degree-granting higher education institutions?
- Is the teaching cooperation compatible with the Norwegian framework for recognising credits taken abroad?

- Can the plans be implemented without violating applicable legislation in any of the countries, e.g. concerning data protection?
- How are the academic year and the budget year organised, and how does the partner institution organise its system for receiving international students?
- To what extent is academic freedom safeguarded in the curriculum and teaching?
- To what extent can students, employees and others involved in the cooperation be subjected to political pressure?
- What support does the cooperation provide for students and research fellows on exchange stays?
- What are the possibilities of student involvement in research activities? Will such involvement require special security measures?
- What arrangements are in place for helping students to prepare for stays in partner countries and at partner institutions?
- What level of the organisation does the agreement need support from in order to be implemented? Has the cooperation been approved at the correct level?
- Is a residence permit or visa required? What type of permit or visa is required? As regards mobility to Norway, see www.udi.no.

5.3 Agreements on cooperation on research and higher education

Good cooperation agreements based on in-depth knowledge of partner institutions and partner countries are a prerequisite for responsible international knowledge cooperation. Institutional cooperation agreements should be aligned with the institutions' long-term strategies.

Agreements on research and higher education range from mere exchange agreements to research and technology cooperation, and the partners can be public or private actors, including companies.

This does not apply to research agreements between nations, but research agreements at central government level, together with multilateral frameworks and the EU agreements (Science and technology (S&T) roadmaps) with individual countries, can define the terms for partnerships at institutional or corporate level. It is important to be aware of cultural and political differences. For each specific cooperation, consideration should be given to both fundamental national interests and academic values.

According to NUPI's Challenging Knowledge Cooperation report (in Norwegian only), administrative staff at several institutions point out that establishing and following up agreements can be very time-consuming, and that many projects fail to allocate sufficient time for this work.

Proposed assessments and procedures for the institutions' management and administration

- Have joint exchange agreements between several Norwegian institutions and foreign partners been considered? This is particularly relevant for small disciplines and institutions.
- Has consideration been given to academic gains, the cooperation’s importance to the quality of education and research, as well as its relevance and the opportunity to develop knowledge that society needs?
- Have visibility and the impact on the institution's own reputation been considered?
- Is the agreement supported by the employees' professional network? This is important for quality assurance, ownership and follow-up.
- Has the exchange agreement undergone legal and administrative quality assurance?
- Have challenges related to the basis for transferring personal data to third countries been considered?

- Has it been considered whether potential ethical and security-related considerations are under pressure and, if so, has this been taken into account in the agreement? Examples include protection of academic values such as teachers' and students' freedom of expression in teaching situations, data protection and information security.
- Have special agreements been drawn up for practical training mobility that ensures academic follow-up and formal recognition?
- Is a residence permit or visa required? What type of permit or visa is required? As regards mobility to Norway, see www.udi.no.
- Has the cooperation agreement been signed at the correct level?

What to include in an agreement

- A formal agreement should contain clauses on open information and a common, mutual obligation to comply with norms, rules and/or special agreements regarding academic freedom, integrity, impartiality (conflicts of interests, conflicts of commitment) and transparency. The agreement should be made public unless competition considerations require secrecy.
- A definition of the partners
- Objectives and the concrete expected results of the cooperation
- A budget, sufficiently detailed to allow no room for doubt about who will bear the costs, as well as reporting procedures, periods, etc.
- A timeline for activities and results
- Agreements on mutual progress reporting
- An agreement on the use of equipment, infrastructure, software and access to digital infrastructure.
- An agreement on access to data: this applies to data generated through the cooperation, but also data and know-how that are brought into the project, and personal data relating to partners and study objects, if relevant.
- An agreement on forms of involvement and follow-up of students in research collaborations, where relevant.
- Definition of expected intellectual property values and rights from the project.
- An agreement on intellectual property rights (IPR). This applies to copyright, patents on trademarks, designs, source code or data, and storage of data. Who has ownership rights, and who can take out a patent? Can results be patented and licensed? How will revenue from licensing be divided?
- Agreements on what should not be disclosed, where competition considerations, other commercial considerations, or considerations for the partner's dedication or expectations dictate secrecy.
- An agreement on rules for publication and crediting from the project. Publication norms vary between subject areas and sectors.

6 Responsibility and coordination at the national level

6.1 Central authorities and responsibilities - who does what in Norway?

Below is an overview of institutions and areas of responsibility that are in various ways important to compliance with the accountability requirement in international knowledge cooperation. Some of these institutions have overall national responsibility and all of them, except the Norwegian Intelligence Service, can give advice to the research and education sector.

- **The National Security Authority (NSM)** is the Norwegian directorate for preventive national security. NSM gives advice on how to secure information, systems, objects and infrastructure of national importance, as well as personnel security. It prepares an annual risk assessment and has a national responsibility to detect, report and coordinate the handling of serious cyberattacks. NSM owns the Norwegian National Cyber Security Centre.

- **The Police Security Service (PST),** Norway's domestic intelligence and security service, is subordinate to the Minister of Justice and Public Security. PST's main task is to prevent and investigate serious crime that threatens national security. PST collects information about individuals and groups that may pose a threat, prepares analyses and threat assessments and provides advice.

- **The Norwegian Intelligence Service (NIS)** is Norway's foreign intelligence service. The service is subordinate to the Chief of Defence, but its work covers both civilian and military issues. The main tasks of NIS are to warn of external threats against Norway and Norway's priority interests, support the Norwegian Armed Forces and defence alliances in which Norway participates, and contribute information of particular interest to Norwegian foreign, security and defence policy. NIS does not give direct advice to individual institutions, but the NIS threat assessment is important for the Norwegian authorities' understanding of risk.

- **The Ministry of Foreign Affairs' Section for Export Control** manages and enforces the regulations relating to export control, and is the authority that decides when an export licence is required. The section can provide advice and guidance on which subject areas and activities are regulated.

- **The Directorate of Immigration (UDI)** considers applications for residence permits etc. in accordance with the Act relating to the admission of foreign nationals into the realm and their stay here (the Immigration Act). The applications must be assessed in relation to circumstances that affect fundamental national interests and foreign policy considerations, cf. the Immigration Act C14 and the Regulations relating to the admission of foreign nationals into the realm and their stay here (the Immigration Regulations) Chapter 19A.

I

- **The Directorate for Higher Education and Skills (HK-dir)** has national responsibility for the administration of higher education, higher vocational education and training and skills policy. HK-dir can be contacted for questions relating to foreign diplomas and international educational cooperation. The Directorate is responsible for ongoing management and follow-up of security in the sector in consultation with the Ministry of Education and Research. It manages KD's Policy for information security and data protection (in Norwegian only) and Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren ('Framework for handling ICT security incidents in the higher education sector' – in Norwegian only). The Directorate can be contacted for questions about the three security domains: information security and data protection, national security and public security, and emergency preparedness.

- **The Research Council of Norway:** The Research Council of Norway is a national strategic research administrative body under the Ministry of Education and Research, but with its own board. The Research Council is responsible for strengthening the knowledge base and helping to meet society's need for research by promoting basic and applied research and innovation. On behalf of the Government, the Research Council (as of 2021) invests NOK 11.9 billion per year, from 15 ministries, in research. The Research Council manages a number of national strategies, plans and policies, such as the Research Council's Policy for Open Science and the Research Council's Policy for Open Access to Research Data.

- **The National Research Ethics Committees (FEK)** are the most important national agency for research ethics. These committees are tasked with ensuring that public and private research is conducted in accordance with recognised research ethics norms. FEK is a management body for research ethics issues in all disciplines, affiliated to the Ministry of Education and Research. The committees are independent, cf. Section 3 of the Research Ethics Act. They provide advice and guidance on ethical issues based on their guidelines. FEK shall assist the institutions in their work on research ethics.

- **Innovation Norway**: Innovation Norway is a state-owned Norwegian enterprise established by special legislation. Its objective is to be the Norwegian State and the county authorities' instrument for achieving profitable business development throughout the country. Innovation Norway gives advice on start-up, growth strategies and exports, and offers financing, consultancy services, expertise, networking and profiling services.

- **Sikt** is the research and education sector's supplier of digital infrastructure. Sikt is responsible for managing, developing and acquiring digital services, offering a digital foundation for the sector, providing advice on data protection and information security, archiving and disseminating data for research, and providing digital tools for teaching and the administration of education.

- The **Norwegian Data Protection Authority**'s task is to oversee the data protection regulations and help ensure that individuals' rights are not violated through the use of information that can be linked to them.

- **The Council for Public Security and Preparedness in the Research and Education Sector:** The Ministry of Education and Research has appointed the Council for Public Security and Preparedness in the Research and Education Sector as a voluntary measure to strengthen work on public security and preparedness. The council contributes to the sharing of best practices and has developed guides on security and preparedness for the sector.

- **The Norwegian Industrial Property Office** is an agency organised under the Ministry of Trade, Industry and Fisheries. The Norwegian Industrial Property Office provides know-how and expertise about intellectual property rights and assets, enabling businesses and institutions to protect their investments and competitive position, and create economic growth in Norwegian society.

- **Eksfin** (Export Finance Norway) is a governmental institution under the Ministry of Trade, Industry and Fisheries. Eksfin aims to make Norwegian export industries financially competitive abroad. Eksfin can furnish government loans and guarantees that promote specific sales contracts, export-promoting investments in Norway, or other types of transactions that contribute to Norwegian value creation and employment.

Literature and resources

Academic freedom

- Academic Freedom Index: https://www.v-dem.net/our-work/research-programs/academic-freedom/
- Bonn Declaration on Freedom of Scientific Research
- Cases published by the Australian Government's Department of Education: https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-governance-and-risk-frameworks
- International Science Council (2021) *A Contemporary Perspective on the Free and Responsible Practice of Science in the 21 Century*.
- The Kierulf Committee drew up a proposal for a declaration on academic freedom of expression and a set of ground rules for free speech in the research and higher education sector. NOU 2022:2 Academic freedom of expression – A good culture of free speech must be built from the bottom up, every single day
- Report on the status of academic freedom in the EU Member States: State of play of academic freedom in the EU member states: Overview of de facto trends and developments
- SAIH: Activism Under Attack Understanding the Repression of Student Activism
- Scholars at Risk: Free to Think Report
- Scholars at Risk: Values and Home and in Partnerships
- The European Charter for Researchers

Research ethics

- The European Code of Conduct for Research Integrity
- International resources on research ethics referred to by the National Research Ethics Committees: https://www.forskningsetikk.no/en/resources/external-resources/
- Guidelines for promoting Research Integrity in Research Performing Organisations
- The National Research Ethics Committees:
  - Guidelines| Research Ethics
  - Resources | Research ethics
- OECD (2022) Integrity and Security in the Global Research Ecosystem, Open Science, Technology and Industry Policy Papers no. 130
- Research ethics guide published by the National Committee for Medical and Health Research Ethics: Medical and health research in low- and middle-income countries
- Research ethics and prevention – sikresiden

Open research and sharing

- Research Council of Norway (2021) How should we share research data? Report and recommendations relating to licensing and making data available
- Research Council of Norway (2022) Investering i infrastrukturer for FAIR forskningsdata og særlig relevante forvaltningsdata for forskning. Organisering og finansiering av datainfrastruktur for best mulig utnyttelse. Anbefalinger fra datainfrastrukturutvalget. ('Investment in infrastructure for FAIR research data and public administration data of particular relevance to research. Organisation and funding of data infrastructure for best possible utilisation. Recommendations from the data infrastructure committee' – in Norwegian only).

- The Research Council's Policy for Open Science
- Online resource on open data sharing from Sikt https://www.openscience.no/apen- forskning/forskningsdata/fair
- Online resource on open research from Sikt https://www.openscience.no/en
- **Open Data Directive (2018) – implementation of Directive (EU) 2019/1024 on open data and the re-use of public sector information in Norwegian law is under consideration. This will also have a bearing on data published in connection with publicly funded research.**

Risk management at the institutional level

- Council for Public Security and Preparedness in the Research and Education Sector: Guide to risk and vulnerability analyses in the research and education sector
- Cases: https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies
- Sikresiden.no is created by and for Norwegian universities, university colleges and research establishments. The website is intended to help students and employees to know what to do when something happens and how to work preventively. The website covers travel, online fraud and cyberattacks, among other things.
- Governing document for the work on security and emergency preparedness in the Ministry of Education and Research's sector

Information security

- Directorate for Higher Education and Skills (2022) Information security and data protection in higher education and research. Risk and status assessment 2022.
- The Ministry of Education and Research's Policy on information security and data protection in higher education and research
- The National Security Authority (NSM) has drawn up a set of Core Principles for ICT security
- NSM has drawn up a guide to the valuation of information (in Norwegian only)
- Sikt's web application can be used by Norwegian educational institutions to exchange personal data in a secure manner: Nomination - Felles studentsystem
- The University of Oslo offers the Nettskjema service, which provides secure transfer of personal data about researchers and students.

Export control

- Stanford University: 'Export Controls Decision Tree'.
- Council for Public Security and Preparedness in the Research and Education Sector: Kontroll med kunnskapsoverføring ('Control of knowledge transfer'– in Norwegian only)
- Guidelines for control of knowledge transfer (in Norwegian only)
- Export Control and Academia Manual – German Federal Office for Economic Affairs and Export Control
- EU Summary of the Dual-Use Export Control Regulation
- EU compliance guidance for research involving dual-use
- Report No 26 to the Storting (2018-2019) – Eksportkontroll av forsvarsmateriell fra Norge I 2018, eksportkontroll og internasjonalt ikke-spredningsarbeid ('Export control of defence materiel from Norway in 2018, export control and international non-proliferation work' – in Norwegian only).

Employees and students

- https://www.sikresiden.no/en has a checklist of what people should do if they experience threats.
- Human Rights Watch documents and provides advice to counteract pressure against researchers and students.
- NSM's personnel security guide
- OsloMet's webpages for responsible internationalisation (in Norwegian only).

Employees and students abroad

- Recommendations for travel https://www.sikresiden.no/en
- ANSA - For those who study or want to study abroad
- Example of contingency plans and inclusion of students on exchanges abroad (University of Bergen)
- For Norwegian students abroad | Sjømannskirken – Norwegian Church Abroad (sjomannskirken.no)
- Emergency number app | Sjømannskirken - Norwegian Church Abroad (sjomannskirken.no)
- Transfer of personal data out of the EEA (in Norwegian only), Norwegian Data Protection Authority
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level protection of personal data.
- The Ministry of Foreign Affairs' travel app 'Reiseklar' : https://www.regjeringen.no/en/tema/utenrikssaker/reiseinformation/reiseklar/udapp_reiseklar/id2877128/
- The University of Oslo's IT advice for employees abroad: https://www.uio.no/english/services/it/security/lsis/travel.html
- The Ministry of Foreign Affairs' travel information and country pages in Norwegian only)

Partnerships in the research field

- The National Research Ethics Committees Medical and health research in low- and middle-income countries Research ethics guide.
- Equitable Partnerships Resource Hub | UKCDR
- TRUST (2018) Global Code of Conduct for Research in Resource-Poor Settings

Agreements in the field of higher education and research

- Knowledge about countries
  - Academic Freedom Index (AFi)
  - Universal Human Rights Index
  - Corruption perceptions index
  - Economist Intelligence Unit
- Accountability in international cooperation agreements in education
  - Accountability in international cooperation agreements (oslomet.no) (in Norwegian only)
  - Preparing contracts and agreements | NMBU (in Norwegian only)

Reports, guides, policy documents and white papers

Academic freedom of expression – A good culture of free speech must be built from the bottom up, every single day (NOU: 2022:2).

Council for Public Security and Preparedness in the Research and Education Sector (2021) Kontroll med kunnskapsoverføring (notat) ('Control of knowledge transfer (memo)' – in Norwegian only).

Council for Public Security and Preparedness in the Research and Education Sector (2022) Risiko- og sårbarhetsanalyse i kunnskapssektoren. En nasjonal veileder. ('Risk and vulnerability analysis in the research and education sector. A national guide' – in Norwegian only)

National Research Ethics Committees Medical and health research in low- and middle-income countries Research ethics guide.

Norwegian Agency for Public and Financial Management (DFØ) risk management guide – in Norwegian only).

Directorate for Higher Education and Skills (2022)Information security and data protection in higher education and research: Risk and status assessment 2022. (In Norwegian only)

Research Council of Norway (2017) The Research Council of Norway's Policy for Open Access to Research Data

Research Council of Norway (2019) The Research Council of Norway's Policy for Open Access to Research Data

Research Council of Norway (2020) The Research Council of Norway's Policy for Open Access to Research Data

Research Council of Norway (2021) How should we share research data? Report and recommendations relating to licensing and making data available.

Gåsemyr, Hans Jørgen, Kristin Fjæstad og Malin Elisabeth Tvedt Hogstad (2022) Utfordrende kunnskapssamarbeid: Etiske og sikkerhetsrelaterte utfordringer som forskere og kunnskapsinstitusjoner møter i internasjonalt samarbeid. NUPI report 6 2022).

Ministry of Education and Research (2020) Policy on information security and data protection in higher education and research, circular F-04-20.

Ministry of Education and Research (2021) Panorama. Strategy for cooperation on research and higher education with Brazil, Canada, China, India, Japan, Russia, South Africa, South Korea and the USA (2021–2027)

Ministry of Education and Research (2021) Governing document for the work on security and emergency preparedness in the Ministry of Education and Research's sector.

Report No 5 to the Storting (2022-2023) Long-term plan for research and higher education 2023–2032.

Report No 8 to the Storting (2020–2021) A world of opportunities – International student mobility in higher education

Report No 9 to the Storting (2022–2023) National control and digital resilience to safeguard national security. As open as possible, as secure as necessaryhttps://www.regjeringen.no/no/dokumenter/meld.-st.-9-20222023/id2950130/ (in Norwegian only)

National Security Authority (2020) Core Principles for ICT security

National Security Authority Personnel security guide

National Security Authority Security management guide

Norwegian University of Science and Technology (NTNU) (2017) Code of ethics for employees at NTNU

New Act relating to universities and university colleges (NOU 2020: 3.

The Police Security Service, the National Security Authority, the Police and the Norwegian Business and Industry Security Council (2017) Guidelines for security in employment relationships. Before, during and on termination.

Guidelines for responsible international cooperation from selected countries, the EU and the OECD

Department of Education, Skills and Employment (2019): Guidelines to Counter Foreign Interference in the Australian University Sector

EU Commission (2022) Tackling R&I Foreign Interference

European Commission, Directorate-General for Research and Innovation (2022) Tackling R&I Foreign Interference. Staff Working Document.

German Rectors' Conference (2020) Guiding Questions on University Cooperation with the People's Republic of China

Ministry of Interior of the Czech Republic Counter Foreign Interference Manual for the Czech Academic Sector

New Zealand Government Due Diligence Assessments For Espionage and Foreign Interference Threats

New Zealand Government Trusted Research Guidance for Institutions and Researchers

OECD (2022) Integrity and Security in the Global Research Ecosystem

The Swedish Foundation for International Cooperation in Research and Higher Education (STINT) (2020) Responsible Internationalisation Guidelines for Reflection on International Academic Collaboration

Swiss Universities (2022) Towards Responsible International Collaborations: A Guide for Swiss Higher Education Institutions

Danish Ministry of Higher Education and Science (2022) Afrapportering Udvalg om retningslinjer for internationalt forsknings og innovationssamarbejde ('Report – Committee for guidelines for international cooperation in research and innovation' – in Danish only)

Universities of the Netherlands (2020) National Knowledge Security Guidelines – Secure International Collaboration

Universities UK (2020) Managing Risks in Internationalisation Security Related Issues

Flemish

Interuniversity Council (VLIR) (2019) Recommendations for Implementing a Human Rights Assessment at the Flemish Universities

Direktoratet for
høyere utdanning
og kompetanse

post@hkdir.no hkdir.no