Annotated collection of guidance for secure and successful international R&I cooperation

2022 update

Edited by Gerold Heinrichs, Laura Klueting

chinateam@dlr.de

August 2022, Bonn, Germany

ISBN 978-3-949245-17-6

Preface

This document is an update to the "Analysis of current and publicly available documents on securing international science cooperation" that was published within the EU Knowledge Network on China (EU KNOC) under mandate by the European Commission in March 2021. The 2021 analysis was comprised of two parts: Part 1 presented an annotated collection of a total of 26 country-agnostic as well as country specific guidelines, checklists and other relevant documents on ensuring safe and successful international cooperation in science and technology, whereas Part 2 consisted of meta guidelines that were pulled from nine of the previously analysed documents. The original document can be found here: *https://www.kooperation-international.de/fileadmin/user_upload/GuidelinesAnalysis-2021.pdf*

Since March 2021, several institutions in different countries have published additional documents, or updated existing ones. Although the EU KNOC project is not being continued at the moment, the China team at DLR-PT has decided to carry on the annotated collection (Part 1 of the original document) to support stakeholders in the process of creating their own guidelines for their international cooperation.

This document adds 14 additional recently published/updated guiding documents to the existing annotated collection. New additions are highlighted in bold font in the table of contents. Many of the newly published guiding documents and websites follow a common theme: nine out of 14 focus on research security and integrity.

The collection uses the English language, although some documents were written in other languages as indicated in the profile. The brief categorisation of the documents in the profiles is not based on a structured standard, but is the result of a rough assessment of the editors by comparing the documents. It is intended to give some initial pointers during a quick perusal.

The annotated collection makes no claim to completeness but is instead intended to give an overview on the current situation. Readers are invited to inform the editors about other publicly available relevant and recently published documents.

Table of contents

Australia

University Foreign Interference Taskforce

Guidelines to counter foreign interference in the Australian University Sector (2021 update)

Target audience:	Australian universities
Regional focus:	country agnostic
Thematic focus:	governance and risk frameworks; communication, education and knowledge sharing; due diligence, risk assessment and management; cybersecurity
Structure:	guiding questions; appendix with questions for declaration of interest and glossary
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	26
Most relevant:	p. 8-22

The University Foreign Interference Taskforce was established in 2019 and is made up of university representatives, Department of Education representatives and government security experts. The decision to establish the Taskforce was made in response to meetings between government and university representatives that highlighted growing concerns about foreign interference in Australian universities and undermining of academic freedom.

The Taskforce originally published their guidelines in 2019 and updated them in 2021. The guidelines are intended to support Australian universities in mitigating the risk of undue foreign interference without missing out on the benefits of international research collaboration, and should be used as a tool for risk assessment as well as examination of existing policies and protocols.

The updated guidelines are presented in 4 categories. Within each category, the following recommendations are made:

1. Governance and risk frameworks

- Incorporate measures to counter foreign interference into regular internal audit processes
- Establish clear and transparent risk review and reporting processes
- Establish a responsible office at each university to manage risk and regularly review and communicate security risks and proportionate remediation, monitor foreign cooperation and grants, and review university responses to reported issues

2. Communication and knowledge sharing

- Establish communication plans and training programs to raise awareness among staff and students
- Establish clear reporting channels
- Share best practices with both Australian universities and trusted international partners
- Government support: e.g., through contact points such as the Counter Foreign Interference Coordination Centre

3. Due diligence, risk assessment, and risk management

- Develop processes to manage conflicts of interest: including collecting information on potential conflicts of interest (e.g., at annual intervals) and establishing policies and procedures to manage conflicts of interest
- Conduct due diligence on partners and personnel on a regular basis
- Regularly assess research potential (e.g., potential deployment opportunities)
- Identify a point of contact (e.g., a specialist in international research collaboration) from whom researchers and staff can seek advice and assistance, e.g., in evaluating potential conflicts of interest, dealing with foreign influence, etc. seek advice and support

4. Cybersecurity

- Participate in best practice communities that share cybersecurity information and lessons learned among universities and with government
- Incorporate threat models, best practices, and success measures into the university's internal cybersecurity strategy

The Australian Strategic Policy Institute (ASPI)

Author: Alex Joske (International Cyber Policy Centre)

Hunting the phoenix – The Chinese Communist Party's global search for technology and talent (2020)

Target audience:	governments, universities worldwide
Regional focus:	China-specific
Thematic focus:	Chinese talent-recruitment programs
Structure:	information on talent programs and associated risks; case studies; recommendations
Level of guidance:	relatively detailed
Language:	English
Page total:	64 pages
Most relevant:	p. 27-28

ASPI is an Australian defense, national security and strategic policy think tank. "Hunting the phoenix" points out that greater awareness of potential "brain drain" through Chinese overseas talent-recruitment programs, greater transparency where these programs are concerned, and increased funding to support the retention of talent and technology are necessary. Several case studies and a list of recommendations for governments and universities are included. These recommendations should be introduced alongside existing regulations to promote transparency and accountability, as well as help manage conflicts of interest. The need for increased compliance and enforcement of existing regulations, as well as implementation of these new recommendations, is strongly emphasized.

Some of the proposed recommendations for governments:

- Carry out studies on talent-recruitment programs, brief universities and research institutions
- Ensure that cases of theft, fraud, espionage, and non-compliance are investigated
- Prohibit government employees from joining talent programs
- Include disclosure requirements for any type of funding, as well as staff participation in foreign talent programs
- Establish a public online database of foreign funding received by universities and their employees
- Establish a national research integrity office

Some of the proposed recommendations for universities:

- Carry out audits of participation in talent-recruitment programs by staff
- Update relevant policies and brief staff, especially where disclosure of contracts and foreign renumeration is concerned
- Investigate cases of fraud, misconduct, and nondisclosure, examine why existing regulations and systems failed to prevent them
- Strengthen existing staff travel databases to flag conflicts

Picking flowers, making honey - the Chinese military's collaboration with foreign universities (2018)

Target audience:	governments, universities worldwide
Regional focus:	China-specific
Thematic focus:	research collaboration with People's Liberation Army (PLA)
Structure:	information on PLA strategies and associated risks; recommendations
Level of guidance:	relatively detailed
Language:	English
Page total:	25 pages
Most relevant:	p. 18-20

Also published by ASPI, "Picking flowers, making honey" seeks to inform governments and universities about the risks involved in research collaboration with Chinese universities, research institutes and individual researchers that have ties to China's People's Liberation Army (PLA). It provides in-depth information about ways in which PLA-affiliated scientists have attempted to conceal their ties to the Chinese military in the past and offers a list of 37 recommendations in total that governments and universities should implement to protect themselves against the inadvertent transfer of knowledge and technology, especially in cases where it could be used to advance a non-allied military's capabilities.

Some of the proposed recommendations for governments:

- Deepen national as well as international discussion on PLA collaboration, increase awareness, develop interagency responses, and share relevant information globally
- Improve the visa application screening process to detect deception by PLA scientists
- Re-examine and amend existing export control policies, continuously train and provide resources for university staff that is tasked with export control compliance
- Introduce policies to regulate the scientific training that foreign military personnel can receive
- Regulate or prohibit the use of government funding in collaboration with the Chinese military and other non-allied militaries
- Increase funding for research in strategically relevant research fields, limit or prohibit certain forms of foreign investment in the same fields

Some of the proposed recommendations for universities:

- Build an awareness of the extent of PLA collaboration on campus and develop processes, internal policies and security precautions accordingly
- Increase oversight over visiting scholar and student application

Belgium

Flemish Interuniversity Council

Vlaamse Interuniversitaire Raad

Recommendations for implementing a human rights assessment at the Flemish universities (2019)

Target audience:	Flemish universities
Regional focus:	country-agnostic
Thematic focus:	human rights
Structure:	information on human rights; guidance on assessment; examples; additional resources; indicator checklist
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	24 pages
Most relevant:	p. 9-23

The Flemish Interuniversity Council (VLIR) is an autonomous consultative body that advises the Belgian government on higher education policies and established an ad hoc Working Group on Human Rights in 2018. The working group determined that respecting human rights is fundamental to universities' social responsibility, and that while it is important to raise awareness, this is not sufficient in itself. Therefore, the working group developed a human rights assessment as a practical self-regulation tool to aid universities in implementing new and strengthening existing human rights policies.

The working group also provided an indicator checklist to simplify the screening of potential and existing partners and research activities (p. 19-20) and identified some additional steps that can be taken should the indicator diagram reveal a potential risk for human rights violations within a given research collaboration (p. 21-23).

Some of the proposed recommendations to universities are as follows:

- Establish a contact point for questions regarding the human rights assessment, the university's human rights policies and possible human rights violations in new or ongoing collaborations
- Carry out systematic human rights assessments of both new and ongoing collaborations, partners and research activities
- Include human rights clauses in contracts where relevant

Canada

Government of Canada

Safeguarding your research (2021)

Target audience:	Canadian research community
Regional focus:	country agnostic
Thematic focus:	research security
Structure:	"Protect your research"-briefs provided by the Canadian Security Intelligence Service; case studies/scenarios and best practices; links to other resources and best practices as well as external resources; links to courses on research and cyber security
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	n/a
Most relevant:	n/a

The Safeguarding Your Research portal was established as a channel to disseminate key results that the joint Government of Canada-Universities Working Group is producing. The Working Group includes members from the Government of Canada, the university community, and the associations that represent them.

The website provides information on research security and related risks, including theft, interference, or unwanted transfer of knowledge and research results, as well as steps and precautions to counteract these risks.

The portal also includes several checklists:

- National Security Guidelines for Research Partnerships plus complementary Risk Assessment Questionnaire
- Travel security guide for university researchers and staff
- Mitigating economic and/or geopolitical risks in sensitive research projects

Some of the best practice recommendations to protect sensitive research include:

- Conduct due diligence on all members of research teams and assess alignment with the project's research priorities as well as any potential conflicts of interest or affiliation
- Discuss potential project risks with all members of the team and fill out a risk register
- Assess if appropriate data management and cybersecurity measures are in place across all partner institutions involved in a research project
- Ensure that all involved partners and collaborators agree on how intellectual property is handled
- Discuss whether all team members are comfortable with likely uses of the research results

Denmark

Danish Ministry of Higher Education and Science

Guidelines for International Collaboration in Research and Innovation (2022)

Main target audience:	administration of Danish universities and research organizations
Regional focus:	"not like-minded" countries (in this context e.g. according to listings in the Academic Freedom Index, Freedom in the World or the World Justice Project Rule of Law Index or due to lack of separation between civilian and military research)
Thematic focus:	research security
Structure:	Summarized guidelines in three categories (1. Identify and protect your vital research, 2. Get to know your cooperative partners, 3. Protect your institution, staff and students); detailed explanation for each category
Level of guidance:	somewhat detailed, practical guidance
Language:	English
Page total:	28 pages
Most relevant:	p. 10-26

The guidelines were developed by a specifically created committee (URIS) and are intended to assist Danish institutions in taking a balanced approach to international research and innovation collaboration in order to minimize risks, protect own long-term interests, and insist on reciprocity and transparency. This objective is to be achieved by establishing structures and procedures that will guide staff in their projects with international partners and by raising staff awareness on the potential risks of international collaboration.

The following recommendations were collected:

- Identify strategically important research areas, data, equipment and results, assess collaborative relationships in these fields and whether the identified areas are adequately protected, and control access
- Establish standard agreements for international cooperation in which the conditions for intellectual property rights, knowledge and ownership rights are clearly spelled out
- Refer to standards such as The European Code of Conduct for Research Integrity and the Bonn Declaration on Freedom of Scientific Research in international cooperation agreements
- Add positive lists to cooperation agreements that specify which technologies, data, equipment, results etc. may be accessed by the partner. Also consider using negative lists where appropriate
- Share resources, create a culture of awareness and prepare (country-specific) guidelines, workshops, working groups etc. about regulations and their implementation based on specific needs
- Implement background check procedures and share information among institutions
- Prepare a questionnaire to assess added value, compatibility of interests, potential risks, rights to research results etc. in cooperation projects with international partners (example on p. 21)
- Establish clear chains of command and reporting as well as onboarding procedures, including rules for subsidiary employment

EU

European Commission

Basic Principles for effective International Science, Technology and Innovation Agreements (2014)

Target audience:	EU, EU member states
Regional focus:	non-EU countries
Thematic focus:	international STI agreements
Structure:	information on existing bilateral STI agreements used by the EU, its member states, and the USA; information on the impact of existing STI agreements; potential alternatives; recommendations
Level of guidance:	general
Language:	English
Page total:	62 pages
Most relevant:	p. 43-48

The European Commission tasked a consortium with developing a study about existing bilateral Science, Technology and Innovation (STI) agreements, their impact, and potential alternatives such as umbrella agreements between the EU and non-member states. This was preceded by reports that pointed out the strategic disadvantages of a lack of coordination and the lack of a common framework at the EU level, as well as calls that "Europe should act as one to achieve a global playing field for research and innovation" (p. 6).

The study concludes that a coordinated approach to STI agreements with non-EU countries at the European level would result in increased efficiency and effectiveness of international cooperation activities. STI umbrella agreements, meaning agreements that result out of joint action by the EU and member states, are presented as a potential coordinated approach. While the implementation of joint consent umbrellas (legally binding multilateral agreements that present overarching framework conditions for STI cooperation) may be difficult, basic principles umbrellas (not legally binding guidelines to be used at the European level as a basis for STI agreements) are considered a feasible strategy.

EU compliance guidance for research involving dual-use items (2020)

(EU Dual Use Research guidance-draft version for Targeted Consultation)

Target audience:	individual researchers; research organizations
Regional focus:	country agnostic
Thematic focus:	dual-use export controls
Structure:	information on export control regulations and how they affect research organizations; guidelines; information research areas and scenarios where export control regulations might be relevant
Level of guidance:	detailed guidance
Language:	English
Page total:	64 pages
Most relevant:	p. 21-40

The document was drafted to support individual researchers and research organizations in identifying, managing and mitigating the specific risks related to the export of dual use technologies, as well as complying with the appropriate export control regulations. The document will be updated periodically.

Among a total of 60 guidelines that address aspects that organizations should consider when setting up or reevaluating their internal export control compliance policies, the compliance guidance recommends to:

- Establish and communicate clear responsibilities and processes where export control compliance is concerned
- Make relevant training for staff that could potentially take part in research concerning dual use compulsory
- Develop and implement regular risk assessments of partners as well as projects. These could include traditional risk assessment methods as well as data mining or other software solutions
- Consider potential end uses of research
- Perform export screening procedures throughout the research cycle on high risk projects
- Encourage staff to report non-compliance incidents or suspicions thereof
- Protect dual-use items from unauthorized removal, consider access restrictions
- Develop cyber security mechanisms including antivirus checks, firewalls, encryption, audit trails and logs, as well as access controls. Ensure that international partners make use of similar protections where relevant

Tackling R&I Foreign Interference (2022)

Target audience:	European higher education institutions and research organizations
Regional focus:	country agnostic
Thematic focus:	foreign interference and its impact on academic freedom and integrity, governance and risk management, cybersecurity
Structure:	Definition of foreign interference and implications for HEIs and RPOs; definitions, risks and measures to reduce and manage risks in four categories: values; governance; partnerships; cybersecurity
Level of guidance:	somewhat detailed
Language:	English
Page total:	63
Most relevant:	p. 21-59

The EU COM staff working document on tackling foreign interference in research and innovation was prepared together with the EU member states and other stakeholders and published in January 2022. The publication provides a non-exhaustive list of possible risk mitigation measures, based on which universities and research institutions can develop their own strategies tailored to their needs.

The working document recommends to:

- **Identify potential threats to academic freedom with regard to potential partners** (consult the Academic Freedom Index (AFI) as a first point of orientation; assess the partner's research, educational and institutional environment; analyse potential motives and capabilities for instrumentalization of European researchers and institutions/restriction of their academic freedom)
- **Assess institutional vulnerabilities** (review potential dependencies and existing cooperation agreements; monitor external appointments such as the awarding of honorary degrees to researchers; provide training; establish a reporting procedure on threats to academic freedom)
- **Strengthen commitment to academic freedom and integrity at the institutional and individual levels** (address identified vulnerabilities; offer training; incorporate academic freedom and integrity into core curriculum; frequently reaffirm the importance of academic freedom and integrity; strengthen awareness of academic freedom and academic values among students and academic and administrative staff; support scholars who conduct research on topics that are suppressed by external actors; establish specific support programs for scholars and students from countries where academic freedom is threatened; help to protect persecuted researchers or students; sign a pledge to democracy)
- **Continue to cooperate with partners in repressive settings** (avoid stigmatization or alienation of students, researchers, or institutions from non-liberal settings; build awareness and understanding of how repressive settings can affect scientific freedom; review ethics procedures to ensure that high-risk research in repressive settings is not automatically rejected; provide guidance and tailored technical support on data and data security to address surveillance risks; establish a contingency plan to deal with harassment, detentions, and disappearances; commit to transparency and tailored screening mechanisms regarding collaborations in repressive settings)

- **Publish a code of conduct on foreign interference** (to protect academic freedom, data and intellectual property; excellence and openness in science; ethics, integrity and trust), which also covers measures to identify foreign interference, whistleblower protection and procedures on how to deal with internal conflicts of interest
- **Establish a foreign interference committee** (responsible for raising awareness through education and training; monitoring potential risks; managing research data and other knowledge in international collaboration; providing advice and support to involved researchers; risk management and mitigation; investigating foreign interference)
- **Develop general prerequisites for the implementation of a risk management system** (ensure scientific freedom and academic integrity within partnerships and optimize and strengthen procedures; raise awareness of possible risks in partnerships and ways to minimize them; develop a risk management strategy; provide training on export control laws and foreign direct investment screenings; identify and protect "crown jewels" and build understanding of potential technological, security and economic interests of third countries; define minimum due diligence requirements for various forms of partnerships; establish a risk management subcommittee or working group)
- **Establish a smooth process for concluding sound agreements** (identify safe and low-risk areas of international cooperation; prepare partnerships based on strategic vision; build in-depth knowledge of the partner organisation in the context of its national scientific system)
- **Carefully negotiate partnership agreements** (ensure a clear regulation of responsibilities, financial resources, intellectual property, data management and open science)
- **Monitor compliance with agreements** (including an assessment of the results of the collaboration to draw lessons for future engagement)
- **Increase awareness of cybersecurity risks** (offer training in data protection technologies, cyber hygiene, risk identification and avoidance; establish an escalation process in the event of suspected cyberattacks and set up a point of contact; create and communicate a list of the top 10 cybersecurity risks; publish newsletters and best practices in dealing with cybersecurity incidents)
- **Detect and block cyberattacks by foreign actors** (conduct regular open source intelligence (OSINT) investigations and implement alert capabilities; develop screening procedures for researchers and administrative staff; procure certified cybersecurity equipment and develop ways to protect data; establish physical access controls; develop a centralized management approach to operating systems and applications; establish two-factor authentication for accessing critical services and sources; enforce "block lists" related to malicious websites)
- **Respond to and remediate cybersecurity attacks caused by foreign interference** (develop situational responses such as sharing lessons learned, update common blacklists, reputation systems, and databases; develop an incident handling plan; reduce response times; conduct investigations and follow disciplinary actions for offending staff; involve law enforcement, intelligence and security agencies, intellectual property offices, and data protection authorities)

Finland

Ministry of Education and Culture

Recommendations for academic cooperation with China (2022)

Target audience:	Finnish universities and research institutions
Regional focus:	China-specific
Thematic focus:	Value conflicts, security and geopolitical concerns
Structure:	Explanation of benefits and challenges in the cooperation with China in three different risk categories; recommendations
Level of guidance:	general guidance
Language:	English
Page total:	17 pages
Most relevant:	p. 13-14

The recommendation paper was prepared by the Finnish Ministry of Education and Culture in cooperation with stakeholders from Finnish higher education institutions and research institutes.

The recommendations aim to ensure that Finnish HEIs and research institutions can continue to engage in cooperation with Chinese partners based on an understanding of the potential challenges and risks as well as on the basis of their own principles and values. The paper emphasises the responsibility of autonomous higher education and research institutions as the starting point for all international cooperation and calls for a commitment to the following goals:

1. Safe cooperation and partnerships based on institutions' own principles and positions

- Raise awareness on potential risks in international cooperation, include international partnerships in risk management mechanisms, perform risk analyses prior to cooperation, agree on regular partnership evaluations and exit criteria
- Set up internal intervention and communication strategies for problem and crisis situations

2. Ethical and value-based choices

- Ensure that the principles of academic freedom and integrity are part of internal and external communication and reflected in international cooperation agreements
- Evaluate the terminology of agreements and consider cultural and/or political content and ideological connotations

3. Awareness of risks

- Contribute to an understanding of the applicability of research to weapons of mass destruction, military use or use contrary to human rights
- Ensure compliance with export control regulations as well as binding UN and EU sanctions
- Raise awareness on the relationship between academic objectives and security risk

Germany

Commission of Experts for Research and Innovation

Report on Research, Innovation and Technological Performance in Germany 2020 (2020)

Target audience:	German Federal Government
Regional focus:	no overall focus; partly China specific
Thematic focus:	cyber security; knowledge exchange; equal competition; mutually beneficial cooperation; dual-use
Structure:	Information about current developments/challenges; recommendations on measures
Level of guidance:	general guidance
Language:	English (German version)
Page total:	147 pages
Most relevant:	p. 14-15; p. 53-54; p. 71-72

The Commission of Experts for Research and Innovation (EFI) publishes yearly reports on Germany's research, innovation and technological performance. The annual report for 2020 includes cybersecurity and knowledge exchange between Germany and China among its main topics.

Recommended measures applicable or specifically related to China include:

- Build cybersecurity expertise that covers technical, ethical and legal aspects
- Make information on cybersecurity topics and advisory services easily accessible
- Create a level playing field for direct investment in German and Chinese companies
- Establish a central competence center to offer legal advice and specific expertise relating to the cooperation with Chinese partners
- Expand expertise on China

Federal Office for Economic Affairs and Export Control (BAFA)

Export Control in Academia Manual (2019)

Target audience:	academic and research sector; individual scientists
Regional focus:	country agnostic
Thematic focus:	export control, foreign trade law
Structure:	information about export control regulations and their impact on the academic sector; case studies; recommendations for universities
Level of guidance:	detailed guidance
Language:	English
Page total:	108 pages
Most relevant:	p. 84-95

The manual was set up by the German Federal Office for Economic Affairs and Export Control (BAFA) in collaboration with several German research institutes and the Technical University of Berlin to raise awareness among higher education institutions on export control, and to provide support on the application of foreign trade law if needed.

BAFA's recommendations include suggestions such as:

- Ensure compliance with export control regulations and foreign trade law through personal responsibility and frameworks defined by the institution
- Consider setting up an Internal Compliance Program (ICP) to facilitate compliance with relevant regulations, provide risk analyses, keep records, and perform audits
- Identify and clearly assign responsibilities within the research organization, consider appointing an export control officer and provide relevant training
- Include export control compliance regulations in relevant manuals and codes of conduct
- Tailor due diligence on export regulation compliance to the specific fields of research that the organization is involved in
- Keep detailed records of activities that fall under export control regulations
- Ensure that all members of the organization are aware of their duty to comply with export control regulations and know whom to contact
- Implement control mechanisms such as the 4-eyes principle
- Regularly review internal export control compliance policies to ensure that they are up to date and effective
- Develop an anonymous reporting procedure for suspected or actual violations of foreign trade laws and export control regulations
- Protect listed items from theft by use of access controls, authorization concepts, password protection, encryption, firewalls, storage and email policies etc.

German Academic Exchange Service (DAAD)

No red lines - science cooperation under complex framework conditions (2020)

(German original title: Keine roten Linien – Wissenschaftskooperationen unter komplexen Rahmenbedingungen)

Target audience:	German higher education institutions
Regional focus:	country agnostic
Thematic focus:	framework conditions in the partnering country, opportunities and risks of international collaboration, overall performance and fit of the partner institution, embedding the partnership into the institutional strategy
Structure:	criteria catalog, guiding questions, additional resources
Level of guidance:	detailed guidance
Language:	German
Page total:	57 pages
Most relevant:	p. 9-54

The DAAD's Competence Center for International Science Cooperation (KIWi) published these guidelines to support higher education institutions in independently weighing up risks and opportunities in their research cooperation with international partners. The guidelines are supplemented by selected references and represent an experience-based foundation, on the basis of which different actors in higher education institutions can decide which aspects should be considered in their own risk and opportunity assessments. The document has been prepared in collaboration with universities and experts and is to be continuously developed and updated.

The guiding questions provided by the DAAD are arranged along six broad criteria. The first four provide an overview over opportunities, potentials, challenges and risks of international science cooperation projects and cover political, sociopolitical and legal aspects. The fifth and sixth criteria refer more specifically to the evaluation process of the participating partner institutions.

The corresponding guiding questions cover a broad range of topics, such as:

- general aspects to consider when visiting the partnering country (who to contact in case of emergency while abroad, whether cell phones and computers have been adequately secured to make transfer of confidential data possible, etc.)
- status of bilateral relationships/relationships with the EU
- potential sanctions against the partner country and their impact on the science sector
- potential for instrumentalization or political, strategic or ideological goals
- potential for misuse of research results, compliance with export control laws
- legal framework and independence of courts of laws in the partner country
- science policy framework (is there a legal framework to regulate export/regulations for joint publications etc., is academic freedom guaranteed, are certain research fields prioritized, etc.)
- potential civil-military links at the partner institution

German Association of Chinese Studies (DVCS)

Guidance by the German Association for Chinese Studies on the Interaction of German Academic Institutions with the People's Republic of China (2018)

(German original title: Handlungsempfehlungen der Deutschen Vereinigung für Chinastudien e.V. zum Umgang deutscher akademischer Institutionen mit der Volksrepublik China)

Target audience:	German universities and research institutions
Regional focus:	China-specific
Thematic focus:	agenda-setting, legal context, academic integrity
Structure:	guidelines/suggestions
Level of guidance:	somewhat detailed guidance
Language:	German
Page total:	4 pages
Most relevant:	p. 1-4

The German Association for Chinese Studies (DVCS) is a non-profit association for China scholars from German-speaking countries. The DVCS published 16 guidelines in total with the intention of facilitating successful and mutually beneficial German-Chinese research cooperation while accounting for the challenges constituted by different political systems.

Some of the suggestions to universities and research institutions are as follows:

- Add a clause to cooperation agreements with Chinese partners that states that any legal disputes shall be carried out before a German court of law
- Include China experts in the discussions before cooperation agreements are finalized or extended,
- Make the content of cooperation agreements, especially where funding is concerned, transparent and openly accessible
- Include an exit clause in cooperation agreements
- Avoid long-term financial dependencies
- Perform rigorous background checks on Chinese partners
- Protect the academic freedom of Chinese partners
- Inform the head of the institute or an ethics council if lobbying efforts become apparent

German Rectors' Conference (HRK)

Guidelines and standards in international university cooperation (2020)

Target audience:	German higher education institutions, individual university members
Regional focus:	country agnostic
Thematic focus:	strategy and governance; joint teaching and learning; joint research; universities as transnational spaces
Structure:	guidelines within four broad categories
Level of guidance:	general guidance
Language:	English (German version)
Page total:	6 pages
Most relevant:	p. 3-6

The German Rectors' Conference (HRK) is a voluntary association of state and state-recognized universities in Germany. HRK considers international cooperation to be of great value to German higher education institutions and believes that "it is important to proactively identify realms of possibility, without jeopardizing one's own values and standards in the process" (p.2).

The guidelines were developed with the intention of providing German universities and research institutions with a means for critical evaluation of and orientation for setting up and maintaining new and existing cooperation projects and international partnerships. The document will be reviewed and updated at regular intervals.

Some of the proposed guidelines and standards are as follows:

- Equal partnerships with transparent communication
- Balanced funding models that avoid dependencies
- Knowledge of the partner including cultural differences, values and principles
- Robust and transparent due diligence processes, clear allocation of responsibilities
- Adherence to institutional rules as well as scientific, ethical and legal standards
- Academic integrity and freedom
- Intercultural dialogue

The document, which does not have a specific regional focus, was supplemented by the "Guiding Questions on University Cooperation with the People's Republic of China", which go into more detail on how to implement the proposed guidelines specifically in the cooperation with China.

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

Target audience:	German higher education institutions
Regional focus:	China-specific
Thematic focus:	strategy and governance; academic integrity; knowledge security; quality in cooperation; intercultural aspects
Structure:	objectives, guidelines/guiding questions, further reading
Level of guidance:	detailed, practical guidance
Language:	English (German version)
Page total:	18 pages
Most relevant:	p. 6-17

HRK developed a total of 59 guiding questions that address specific concerns in the cooperation with Chinese partners together with a number of experts on China. Although the majority of German-Chinese research collaboration is considered to be mutually beneficial in most cases, and even essential in some fields, CCP influence on the curricula and bureaucratic processes at Chinese universities as well as negative impacts on academic freedom have become a growing concern in recent years. However, rather than cutting ties with China, the HRK proposes to strengthen dialogue and cooperation while being mindful of one's own values as well as the potential challenges involved.

In this context, the guiding questions are intended to map out both necessary and optional courses of action in the establishment and further development of partnerships with China.

The guiding questions include suggestions such as:

- Clearly define responsibilities within the university as well as within partnerships
- Develop and implement control mechanisms and review procedures
- Make funding decisions and concepts transparent, avoid one-sided or long-term dependencies
- Write exit clauses into contracts
- Establish a contact point or person for advice regarding cooperation with China, as well as a person who Chinese students and scholars can approach with questions
- Implement clear reporting mechanisms for incidents relating to foreign interference etc.
- Ascertain whether the objectives of the participating institutions are compatible
- Invest in and make use of expertise on China, individual actors on the Chinese side, and risk-prone areas of research
- Ensure that all partners observe research, ethical, and legal standards

Global Public Policy Institute (GPPi)

Authors: Asena Baykal, Thorsten Benner

Risky Business: Rethinking Research Cooperation with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks (2020)

Target audience:	foundations, universities, research organizations, civil society organizations, think tanks in democratic countries
Regional focus:	non-democracies (China, Russia, Turkey)
Thematic focus:	agenda-setting; academic integrity; knowledge security; intelligence-sharing
Structure:	information on democratic values and red lines; information regarding potential risks of cooperation with non-democracies; strategies to counteract risk; guidelines
Level of guidance:	very detailed, practical guidance
Language:	English
Page total:	58 pages
Most relevant:	p. 35-52

The Global Public Policy Institute (GPPi) is an independent non-profit think tank that published this study to support actors in democratic countries in the process of rethinking scientific cooperation with non-democracies and provide strategies that can aid risk management.

The document states that neither cutting all ties with non-democratic partners nor conducting business as before should be the way forward; rather, the GPPi urges universities and research organizations in democratic countries to reaffirm and clearly state their values and red lines while being aware of the potential challenges and risks before engaging in research cooperation or exchange with non-democracies such as China.

Among 74 guidelines in total, the GPPi suggests to:

- Invest in and make use of country-specific expertise
- Offer preparatory and follow-up seminars for participants in international cooperation projects
- Conduct background checks on potential partners and organizations
- Foster topic-specific expertise, especially on dual use technology, to better assess risk
- Develop a categorization system of risk-prone areas of research
- Make use of tools such as the Academic Freedom Index, the Australian Strategic Policy Institute's China Defence Universities Tracker, and the German BAFA's list of sensitive research areas
- Implement access restrictions where dual use or other sensitive technologies are concerned
- Maintain incident trackers and share these among organizations in democratic countries
- Include exit strategies in cooperation agreements

Industrial espionage and spying on competitors in Germany and Europe (WISKOS)

Risks for the German research location - Guidelines for dealing with scientific espionage and spying on competitors in the scientific context

(German original title: Risiken für den deutschen Forschungsstandort - Leitfaden zum Umgang mit Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext)

Target audience:	German universities and research institutions
Regional focus:	country agnostic
Thematic focus:	scientific espionage
Structure:	information on espionage activities; recommendations; additional resources
Level of guidance:	somewhat detailed
Language:	German
Page total:	28 pages
Most relevant:	p. 19-23

WISKOS is a project funded by the Federal Ministry of Education and Research (BMBF) that focused on a threat analysis of economic and scientific espionage.

WISKOS suggests that higher education institutions should

- Perform a risk analysis of different research areas to determine their individual risk profile and adjust policies and processes accordingly
- Train staff and researchers according to their individual risk
- Appoint a member of staff as security officer or consider involving external security advisors
- Exercise greater oversight over visiting scholars
- Track researchers' career paths after they leave the institution
- Make use of confidentiality agreements
- Enforce both physical and digital access controls where necessary
- Ensure compliance with security protocols, especially where sensitive data is concerned
- Contact the police or the state or federal criminal investigation offices when suspicions of espionage arise

Working Group China Research

(AG China-Forschung)

Pathways to Research with China - Knowledge, Approaches, Recommendations (2020)

(German original title: Wege in die Forschung mit China – Wissen, Zugänge, Empfehlungen)

Target audience:	German universities and research institutions
Regional focus:	China-specific
Thematic focus:	existing successful cooperation with China; background information
Structure:	information about the Chinese higher education system and relevant preconditions; information about Chinese economic interests; potential steps towards building cooperation agreements; best practice examples
Level of guidance:	detailed background information on Chinese context
Language:	German
Page total:	78 pages
Most relevant:	p. 7-9, 48-74

The Working Group China Research was appointed by Lower Saxony's Ministry for Science and Culture. The white paper advocates for a knowledge-based approach to cooperation with China. To that effect, it offers detailed background information on the Chinese higher education sector as well as economic areas of interest, and presents a number of examples to illustrate how and on which topics joint research between Germany and China has been conducted. It gives an overview of different projects and the partners involved and makes recommendations based on the respective experiences. Two examples of preparatory activities for research cooperation projects are also included. Each example had its own characteristics, but within the included case studies, the following overarching observations about prerequisites and conditions for the successful research cooperation with China were made:

- Mutual trust is key for joint projects as well as for being able to conduct on-site research
- Balanced funding increases efficiency and effectiveness of projects
- An on-site presence is recommended for continuous implementation of projects
- Symposia and joint publications are important activities for both sides
- Involvement of young scientists enhances positive effects
- Long term strategic research partnerships often include other aspects such as teaching and industry cooperation

The White Paper offers the following recommendations:

- Establish relevant advisory bodies at the federal level
- Develop matching processes to support the establishment of contacts and collaborations
- Develop a monitoring system to support the systematic setup of research cooperation projects and STI cooperation strategies based on China expertise

Japan

Director General for Science, Technology and Innovation

Guidelines for Collaboration of Universities and National Research and Development Agencies with Foreign Companies (2019)

(Japanese original title: **大学・国立研究開発法人の外国企業との連携に係るガイドライン**)

Target audience:	Japanese universities and National Research and Development Agencies
Regional focus:	country agnostic
Thematic focus:	objectives; risk management; technology transfer; export control
Structure:	information on relevant laws/regulations; examples of existing initiatives; recommendations
Level of guidance:	general; partly practical
Language:	Japanese
Page total:	32 pages
Most relevant:	p. 1; p. 5- 22; p. 23-31

The guidelines were put together by the Japanese government to address collaboration between Japanese universities and research institutes with foreign companies. The document delivers information on relevant laws, risk management, and administrative considerations, clarifies appropriate approaches to collaboration, and assesses benefits of collaboration. It concludes that to lead in global competition, Japanese universities and research institutions have to intensify their collaboration with foreign companies.

The following measures should be taken to create mutually beneficial relationships and prevent unintended technology transfer or reputational risk: high-level risk management system, compliance with laws and regulations (e.g. Security Export Control, Unfair Competition Prevention Act, Japanese Bayh-Dole Act), systematic mechanisms and organizational structure for process management and development, monitoring, follow-up.

The guidelines include specific examples of initiatives taken by Japanese and foreign (German, American, French, British) universities and public research institutions.

Netherlands

Dutch government and knowledge sector

National Knowledge Security Guidelines (2022)

Target audience:	Dutch knowledge sector
Regional focus:	country agnostic
Thematic focus:	Core academic values, risk assessment and management, legal frameworks and codes of conduct, cyber security, procurement and contracting, human resources policy
Structure:	Definition of knowledge security; guidelines in 9 sections; list of sources and contacts; references to additional information on various topics and subtopics
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	55 pages
Most relevant:	p. 4-7, 13-54

The guidelines for knowledge security were jointly developed by the Dutch knowledge sector and the Dutch central government and are intended to be used by the Dutch knowledge sector as a starting point for addressing questions regarding undesirable knowledge and technology transfer, covert influencing of education and research and ethical issues. They aim to ensure that international collaboration can take place safely and are explicitly intended as a living document that will be updated according to new experiences and insights. The primary audience are board members of knowledge institutions.

The guidelines are presented in nine categories and include guidance such as:

Protecting core academic values (such as academic freedom and research integrity)

- Require both Dutch and foreign researchers, lecturers and visitors to subscribe to and abide by the Netherlands code of conduct for research integrity
- Take knowledge security into account when drafting cooperation agreements, e.g. regarding the extent to which data is to be shared or only viewed
- Set up an ethics committee within the institution, e.g. to advise on international cooperation with partners from countries in which fundamental human rights are not respected and on the ethical use of research results, and to whom researchers can report issues relating to international cooperation that pose ethical dilemmas
- Ensure that measures do not lead to exclusion, suspicion or discrimination against foreign students and researchers

Treat assessment

- Raise awareness on the nature of threats and how they may manifest themselves, e.g. methods that state actors use to acquire knowledge and technology, as well as activities aimed at gaining influence and causing interference in the operations of knowledge institutions

Legal frameworks and codes of conduct

- Pay attention to dual use classifications and technology readiness level of basic research (e.g. by using the TRL assessment tool by the Canadian government), comply with existing regulations, such as EU rules for the export of dual-use products and technology and consult with the Central Import and Export Office in case of uncertainty
- Keep in mind enhanced supervision in a limited number of disciplines as required by international sanction regimes
- Subscribe to codes of conduct such as the Universities of the Netherlands Knowledge Security Framework and the EU guidelines on tackling foreign interference in research and innovation
- Stay up to date with legislation that is currently being prepared, such as the screening framework for individuals seeking to gain access to disciplines with great risk to national security, which is to enter into force during the course of 2023

Risk assessment

- Identify sensitive domains of knowledge within the institution, conduct risk analyses for each and chart the institution's "crown jewels" (domains that pose risks associated with knowledge transfer and within which the institution is an international leader)
- Estimate country-specific risk profiles based on public threat information, such as the State Actors Threat Assessment and international rankings
- Perform background checks of foreign partners or clients in cooperation with the institution's security coordinator, including paying attention to signals such as a lack of available information on the internet, while considering potential motives and being aware of potential financial or other forms of dependence

Risk management

- Regulate standard processes at the central level
- Establish a Knowledge Security Advisory Team
- Provide an overview of security-sensitive partnerships, funding and foreign PhD students and visiting researchers at board level
- Review physical and digital protection measures

International partnerships

- Involve legal and security experts in the drafting process of cooperation agreements, and never renew high-risk agreements automatically
- Evaluate partnerships and agreements regularly
- Consider knowledge security in the process of procurement and contracting

Human resources policy

- Train staff to be conscious of knowledge security and to pick up on signals of increased risk, provide special training programmes for visiting researchers from countries with increased risk profiles
- Implement a visitor protocol for visits to sensitive sites and business trips to countries with increased risk profiles

Cyber security

- Invest in awareness raising
- Pay continuous attention to cyber security at the board level
- Ensure chain cooperation in the event of a cyber attack

Contact Point for Knowledge Security (2022)

Target audience:	Dutch knowledge sector
Regional focus:	country agnostic
Thematic focus:	knowledge security
Structure:	Information on academic core values, human resource policies, risk analyses and threat assessments, tools and frameworks; contact form
Level of guidance:	practical guidance
Language:	English
Page total:	n/a
Most relevant:	n/a

The National Contact Point for Knowledge Security is a collaboration between several Dutch ministries, and offers help to anyone connected to a knowledge institution with questions about opportunities, risks and practical matters concerning international cooperation.

The NCP website is continuously being updated with relevant information on topics such as risk analyses and threat assessments.

Sources include:

- Legal Frameworks and Codes of Conduct
- Risk management for foreign visitors and business trips abroad
- Risk Profiles
- Case studies

Leiden Asia Centre (LAC)

Authors: Dr. Ingrid d'Hooghe, Jonas Lammertink

Towards Sustainable Europe-China Collaboration in Higher Education in Research (2020)

Target audience:	European higher education and research institutions
Regional focus:	China-specific
Thematic focus:	sustainable, mutually beneficial cooperation
Structure:	information on current research climate in China; information on the current state of European-Chinese collaboration; analysis of 5 existing guideline documents; list of 17 recommendations
Level of guidance:	general guidance
Language:	English
Page total:	82 pages
Most relevant:	p. 55-57

The Leiden Asia Centre (LAC) is an independent research center for knowledge on modern East Asia. "Towards Sustainable Europe-China Collaboration in Higher Education and Research" aims to provide a framework to aid European universities and research institutions in the establishment and further development of beneficial and sustainable research collaboration with Chinese partners. Collaboration with China is considered to have become essential for research and innovation in Europe, but some of the challenges and risks need to be met with better coordination on the European side, as well as strong measures that safeguard academic integrity and freedom, keep knowledge secure, and ensure mutually beneficial cooperation on the basis of reciprocity.

Some of the suggestions LAC offers are as follows:

- Invest in expertise on China, especially in knowledge about Chinese higher education institutions, their political ties, developments in higher education in China, and developments in science and technology
- Develop and implement safeguards for academic integrity, academic freedom, and knowledge security
- Establish a joint coordinating entity at the national level to facilitate a cooperative approach to the challenges and risks involved in collaboration with Chinese partners
- Develop appropriate guidelines that are proportionate to the specific risk and tailored to scholars in specific research fields
- Engage and share knowledge with other EU member states

The Hague Centre for Strategic Studies (HCSS)

Authors: Frank Bekkers, Willem Oosterveld, Paul Verhagen

Checklist for Collaboration with Chinese Universities and Other Research Institutions (2019)

Target audience:	Dutch universities and research institutions
Regional focus:	China-specific
Thematic focus:	academic freedom; knowledge transfer; agenda-setting
Structure:	guiding questions
Level of guidance:	general guidance
Language:	English
Page total:	18 pages
Most relevant:	p. 3-15

The Hague Centre for Strategic Studies (HCSS) is an independent think tank that published these guidelines with the aim of ensuring academic freedom as well as mutually beneficial partnerships, and counteracting against the inadvertent transfer of science and technology to China. Previously, HCSS and the Leiden Asia Centre (LAC) worked on a mapping of risks and challenges of the collaboration with China. HCSS hopes to enhance the benefits of research cooperation for the Netherlands rather than discourage cooperation entirely.

Among the outcomes of the HCSS/LAC joint study is a list of 10 guiding questions that were designed to provide support to universities and research institutions by helping them to assess the challenges and risks involved in collaboration with China. Some of the suggestions are as follows:

- Determine the objectives of the research project and how the collaboration with a Chinese partner will help to achieve them
- Determine how the project will be funded and how this affects partners on both sides
- Ensure a balanced partnership that allows access to research results for all those involved
- Ensure that all those involved are aware of potential challenges and risks
- Consider potential restrictions on academic freedom
- Ensure appropriate data management policies

Universities of the Netherlands (UNL)

Framework Knowledge Security (2021)

Target audience:	university administrators, researchers, the university sector as a whole, and relevant Dutch ministries
Regional focus:	country agnostic
Thematic focus:	Knowledge security; academic freedom; governance and policy frameworks; due diligence; information provision/communication; knowledge sharing
Structure:	Principles and concepts; overview over opportunities and risks of international collaboration in R&I and existing laws and regulations; governance structures and risk management
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	38
Most relevant:	p. 24-35

The framework was created by an interdisciplinary working group with experts on knowledge security from Dutch universities and other institutions and published by Universities of the Netherlands (UNL, formerly VSNU). The document is intended to support universities in shaping their institutional policy and individual researchers in balancing the openness of science and preventing undesired knowledge transfer.

The framework provides a base for assessing the opportunities and risks of international collaboration, and supports university administrators in making policies and decisions related to knowledge security.

An overarching recommendation made by UNL is to set up Knowledge Security Advisory Teams within universities. Smaller universities should consider whether advisory teams can be set up in a multi-university context. The core team should be equipped with experts in the fields of safety risk management, information security and international collaboration. Additional experts are to be consulted depending on the specifics of the case (e.g. experts in the fields of data, privacy and ethics, intelligence and security, contracting etc.)

Some of the other recommendations made in the framework are:

- Communicate an ongoing inventory of countries, companies and degree programmes with heightened risk (provided by the central government) to faculties, programmes and research groups
- Further develop framework and decision-making processes; define a decision tree with impact areas and associated risk analysis processes that includes information on which analysis is required for which type of collaboration; develop a decision-making structure that specifies which type of collaboration and/or knowledge security risk requires advice or agreement at which level
- Develop training and awareness of all staff focused on knowledge security and include knowledge security in the university's risk management system
- Develop confidential whistle-blower policies to allow anonymous reporting of suspicions of illegal or immoral practices within the university
- Keep a centralized record of collaborations with partners outside the EU

New Zealand

Government of New Zealand

Trusted Research Guidance (2021)

Target audience:	New Zealand's research and innovation sector; particularly STEM researchers
Regional focus:	country agnostic
Thematic focus:	research security
Design:	Outline of potential risks; recommendations in three categories (collaborating with research partners; Using legal frameworks; Helping researchers to stay safe)
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	40
Most relevant:	p. 18-38

The guidance was developed as a collaboration between New Zealand's research and university communities and the New Zealand Government's Protective Security Requirements and aims to help New Zealand's research and innovation sector to get the most out of international collaboration while keeping their research secure.

Suggested steps to protect research should be proportionate to the risks and balanced to support the benefits of international collaboration and are grouped into three main areas:

1. Collaborating with research partners

- Include ethical, legal, national security and financial considerations in due diligence processes
- Check for conflicts of interests with research and funding partners and regularly discuss security arrangements and needs
- Segregate research and control access (digital and physical) where necessary to protect intellectual property, research or personal data
- Include research security considerations in funding proposals
- Demonstrate transparency to research partners and maintain visibility of research projects within the institution, e.g. at departmental meetings
- Develop an understanding of risks to cyber security, communicate which systems contain critical or highly sensitive data to IT staff and ensure that effective arrangements are in place

2. Using legal frameworks

- Ensure compliance with export controls, privacy legislation, and the Overseas Investment Act
- Be aware of the different legislative frameworks that international research partners or funders operate under and any legal requirements that may affect the collaboration
- Understand the impact of contractual arrangements and expectations
- Regularly check whether research is patentable or of commercial value, and explore an early framework agreement or process for agreeing which sensitive material can be sanitised without damaging the overall ability to publish

- Establish an agreed process for deciding what can be published and what must be protected with partners or sponsors
- Think carefully before disclosing information when research is not patented

3. Helping researchers to stay safe

- Follow cyber security best practices, such as enabling two-factor authentication, using password managers, and removing unnecessary app permissions
- Make sure that autorun is disabled on work computers and that antivirus software runs auto-scans on USB drives before any data is accessed
- Be aware of the techniques that phishers use in emails, and report suspicious emails immediately
- Check visa requirements and ensure correct visas are in place for overseas researchers and international students
- Help overseas researchers and visitors to avoid conflicts of interests and uphold security processes
- Ensure that visiting researchers are recorded in human resources systems and consider confidentiality and non-disclosure agreements where necessary
- Conduct risk assessments for staff working overseas, e.g. relating to export control and national security laws as well as intellectual property arrangements in the countries that they are working in
- Protect staff going to overseas conferences, e.g. by ensuring that payments do not create conflicts of interest and being clear on areas of research that can and cannot be talked about

OECD

OECD Global Science Forum

Integrity and Security in the global research ecosystem (2022)

Target audience:	all stakeholders in the research ecosystem
Regional focus:	country agnostic
Thematic focus:	research security and integrity
Design:	Policy recommendations and options for action; glossary; existing frameworks for research collaboration; relationship between research integrity, research security, international collaboration and security and foreign interference challenges; policy initiatives and actions that are being implemented in several countries to address research security and integrity concerns
Level of guidance:	detailed
Language:	English
Page total:	73 pages
Most relevant:	p. 9-15

In 2020, the OECD Global Science Forum launched a project on "Integrity and Security in the Global Research Ecosystem" and established an international expert group to oversee and implement the project.

The expert group's policy report identifies and analyses good practices to safeguard national and economic security whilst protecting freedom of enquiry, promoting international research cooperation, and ensuring openness and non-discrimination and makes suggestions for specific actions under seven overarching recommendations:

1. Underscore the importance of freedom of scientific research and international collaboration as a key element of the global research ecosystem

- Governments should promote international collaboration (including researcher mobility) while taking a proportionate risk management approach
- Research and higher education institutions should maintain welcoming and inclusive environments and ensure that academic freedom is respected

2. Integrate research security considerations into national and institutional frameworks for research integrity

- Governments should aim to establish national contact points for research security or centres of expertise
- Research and higher education institutions should organize dedicated workshops and develop training programs

3. Promote a proportionate and systematic approach to risk management in research

- Governments should support responsible self-management (including capacity building) by higher education institutions and professional associations

- Science and security agencies should ensure regular information exchange and promote mutual understanding of the benefits and risks involved in international collaboration
- Governments, funding agencies, research and higher education institutions should regularly assess security strategies and adjust policy initiatives or actions to ensure effectiveness while monitoring for unintended consequences (such as discrimination against specific groups or reductions in research collaborations)

4. Promote openness and transparency in relation to conflicts of interest or commitment

- Governments and research providers should work together to raise awareness of research security issues
- Funding agencies and research and higher education institutions should establish transparent processes to ensure due diligence when establishing research partnerships and monitoring ongoing projects

5. Develop clear guidelines, streamline procedures, and limit unnecessary bureaucracy

- Governments, funding agencies, research and higher education institutions should develop clear and unambiguous guidelines and transparent processes to minimise administrative burdens on researchers
- Governments and funding agencies should limit additional administrative burden related to security measures and, where possible, leverage existing processes

6. Work across sectors and institutions to develop more integrated and effective policy

- Governments should support better coordination between different ministries or departments with an interest in research security
- Ministries or agencies responsible for education, science and innovation should facilitate collaboration and exchange of information among the different actors in the research ecosystem (funding agencies, research and higher education institutions, and the academic research community)
- Higher education and research institutions should share information on research security issues and the cases that they are confronted with, both within their institution and with other stakeholders

7. Enhance international information exchange on research integrity and security

- Governments, funding agencies, research and higher education institutions should organise international dialogues to exchange information on challenges and good practices relating to research integrity and security
- Research integrity and security issues should be explicitly considered in developing scientific cooperation agreements between national governments, funding agencies, research and higher education institutions
- OECD and other international organisations with a remit for science, technology, and innovation (STI) policy should work with countries to promote exchange of information and policy development on research integrity, research security, and international collaboration

Sweden

The Swedish Foundation for International Cooperation in Research and Higher Education (STINT)

Responsible Internationalisation: Guidelines for reflection on international academic collaboration (2020)

Target audience:	Swedish universities and research institutions
Regional focus:	country agnostic
Thematic focus:	political, social, cultural and legal context of the partner country; motivation for collaborating; strategic design of collaborations
Design:	information highlighting benefits and risks; guiding questions
Level of guidance:	general guidance
Language:	English
Page total:	12 pages
Most relevant:	p. 6-10

The Swedish Foundation for International Cooperation in Research and Higher Education (STINT) was set up by the Swedish government. These guidelines, which were developed in cooperation with several Swedish universities, are intended to aid members of Swedish higher education institutions in assessing and approaching international collaboration. STINT views internationalization of research as generally positive, as it generates value and aims to enhance research quality.

Among a total of 30 guiding questions, STINT suggests to:

- Clearly define the objectives, forms and outcomes of the collaboration
- Ensure that funding is transparent and balanced
- Assess whether the type of funding poses risks regarding academic integrity and freedom
- Offer support to help all those involved understand the political, social, and cultural context of the partner country
- Closely assess risks for dual use of research results
- Research intellectual property rights and data protection regulations in the partner country
- Consider ethical aspects and the potential for infringements on academic freedom

United Kingdom

Academic Freedom and Internationalisation Working Group (AFIWG)

MODEL CODE OF CONDUCT: Protection of Academic Freedom and the Academic Community in the context of the Internationalisation of the UK HE Sector (2021 up-date)

Target audience:	UK higher education institutions
Regional focus:	country agnostic
Thematic focus:	academic freedom
Structure:	key definitions; information on benefits and risks of internationalization; responsibilities; best practice recommendations
Level of guidance:	general guidance
Language:	English
Page total:	8 pages
Most relevant:	p. 3-6

The Academic Freedom and Internationalisation Working Group (AFIWG) is an initiative to strengthen academic freedom in the context of increasing internationalization. AFIWG regards the internationalization of the academic sector as overwhelmingly positive, but intends to raise awareness to the challenges and risks involved, including those associated with violations of academic freedom.

To protect against threats to academic freedom, AFIWG calls for increased transparency and accountability across the higher education sector. AFIWG suggests to:

- Implement thorough risk assessments and due diligence of both potential research collaboration partners as well as topics and reference publicly available data (such as the Academic Freedom Index and SAR's Academic Freedom Monitoring Project) to evaluate potential threats to academic freedom and the academic community before entering into cooperation agreements, accepting funding, donations and gifts from international partners, and when planning fieldwork and field trips abroad
- Agree on, implement, monitor and regularly re-evaluate/adapt measures to safeguard academic freedom
- Designate an individual with internal institutional responsibility for the protection of academic freedom and the academic community
- Develop confidential reporting mechanisms for incidents relating to threats to academic freedom
- Support members of higher education student whose academic freedom is at risk
- Incorporate measures to protect academic freedom into Memoranda of Understanding (MOUs)
- Make summary information on all foreign gifts and donations public
- Include training on risks to academic freedom in pre-departure training courses in preparation for field trips abroad, and consider enhanced travel insurance which covers politically motivated or arbitrary detention by state authorities
- Provide anonymised summary data on cases related to restrictions of academic freedom in annual reports and provide detail on actions taken to mitigate risk

Centre for the Protection of National Infrastructure (CPNI)

Trusted Research Guidance for Academia (2022 update)

Target audience:	UK higher education institutions, particularly researchers in STEM fields
Regional focus:	country agnostic
Thematic focus:	research security; intellectual property and data protection; compliance with legal frameworks
Structure:	information on potential risks of international collaboration; recommendations
Level of guidance:	somewhat detailed
Language:	English
Page total:	21 pages
Most relevant:	p. 3-20

The Centre for the Protection of National Infrastructure (CPNI) provides security advice to businesses and organizations across the UK. The Trusted Research Guidance for Academia was developed to ensure and maintain mutually beneficial international cooperation while protecting intellectual property and sensitive research.

CPNI suggests to:

- Ensure that due diligence processes include ethical, financial, legal and national security considerations to inform decision-making
- Ensure maximum transparency to avoid conflicts of interest
- Enforce access controls where necessary in order to protect intellectual property and data
- Implement effective cyber security mechanisms
- Perform background checks on potential partners and affiliated institutions
- Ensure compliance with export control and technology transfer regulations
- Consider end uses and the potential for patenting throughout the research cycle
- Exercise oversight over visiting scholars and visitors to campus
- Ensure that intellectual property and research data is protected while traveling overseas
- Take steps to protect IT devices from phishing attacks etc.

Trusted Research also provides several other types of guidance, including:

- Trusted Research Checklist for Academia
- Trusted Research Guidance for Senior Leaders
- Trusted Research Implementation Guide
- Countries and Conferences Guide

Universities UK (UUK)

Managing Risks in Internationalisation: Security Related Issues (2020)

Target audience:	UK higher education institutions
Regional focus:	country agnostic
Thematic focus:	academic integrity; knowledge security; protecting values, reputation, people, campuses, research, and transnational education; establishing reporting infrastructures; individual responsibility
Structure:	guidelines underpinned by several case studies and scenarios; links to additional resources; guiding questions
Level of guidance:	very detailed and practical guidance
Language:	English
Page total:	61 pages
Most relevant:	p. 14-47, p. 55-57

Universities UK (UUK) is special interest group for universities in the United Kingdom. These guidelines were published with the intention of enabling universities to protect themselves, their staff and students as well as managing specific risks associated with internationalization while actively pursuing international cooperation and dialogue. UUK provides several case studies and suggests a number of additional resources.

Most importantly, UUK suggests that universities and research institutions should:

- Identify their institution's individual risk profile, regularly review as risks change over time, and develop/adapt policies and processes accordingly
- Provide annual risk reports to governing bodies
- Encourage staff to raise concerns about partnerships
- Establish clear codes of conduct, policies, and legal agreements along with relevant training, especially where sensitive areas of research are concerned
- Develop a reporting infrastructure through which both staff and students can report any concerns and receive support, regularly update this infrastructure as threats evolve over time
- Develop and implement cybersecurity strategies and contractual agreements to protect intellectual property
- Comply with export control legislation
- Include appropriate exit strategies along with a mutual understanding of what could trigger an exit with any cooperation agreement

USA

Association of American Universities (AAU); Association of Public and Land-grant Universities (APLU)

University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus (2020)

Target audience:	US universities
Regional focus:	country agnostic
Thematic focus:	risk assessments; export controls; cybersecurity; intellectual property; technology control; travel safeguards; academic freedom
Structure:	recommendations; example measures
Level of guidance:	general
Language:	English
Page total:	7 pages
Most relevant:	p. 1-7

According to the findings of a 2019 survey of American universities by the AAU and the APLU, the document presents a summary of methods that some universities have already implemented to address risks related to foreign interference. Universities are encouraged to implement similar measures to ensure the security of their research and protect academic integrity on their own campuses.

AAU and APLU recommend to:

- Build awareness, especially about export control regulations and other disclosure requirements
- Provide relevant training to staff and students
- Strengthen cyber security and data protection measures
- Continuously update conflict of interest and conflict of commitment policies
- Develop international travel policies including security briefings, review of travel plans, and ensure that electronic equipment is protected from potential cyber security threats before, after, and during international travel
- Exercise oversight over visitors to campus
- Strengthen existing policies and employ staff with relevant experience to ensure compliance with export control regulations
- Form task forces that can coordinate risk assessments
- Assign clear responsibilities and points of contact

Human Rights Watch (HRW)

Resisting Chinese Government Efforts to Undermine Academic Freedom Abroad. A Code of Conduct for Colleges, Universities, and Academic Institutions Worldwide (2019)

Target audience:	higher education institutions worldwide
Regional focus:	China-specific
Thematic focus:	academic freedom
Structure:	code of conduct with 12 recommendations
Level of guidance:	partly specific recommendations
Language:	English
Page total:	3 pages
Most relevant:	p. 1-3

Human Rights Watch (HRW) is an international human rights-focused NGO. HRW created this code of conduct based on more than 100 interviews that were conducted between 2015 and 2018 in Australia, Canada, France, Great Britain and the United States with academics, graduate and undergraduate students and administrators from a range of different institutions. It is designed to support higher education institutions in ensuring their academic integrity and protecting the academic freedom of their students, particularly those who work on or are from China.

Some of the proposed recommendations to worldwide institutions of higher education are as follows:

- Recognize threats to academic freedom and academic integrity
- Strengthen commitment to and policies for academic freedom on campus
- Develop and implement reporting mechanisms and incident trackers
- Offer support and flexibility to students and scholars whose progress or careers are under threat due to Chinese curtailment of academic freedom
- Monitor activities of all organizations on campus that receive Chinese funding
- Publicly disclose sources of Chinese funding as well as projects and collaborations with Chinese counterparts

National Science and Technology Council

Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise (2021)

Target audience:	US higher education institutions
Regional focus:	country agnostic
Thematic focus:	research security
Structure:	information on benefits and risks of international cooperation; recommended practices
Level of guidance:	detailed
Language:	English
Page total:	22 pages
Most relevant:	p. 6-15

The National Science and Technology Council (NSTC) was established to coordinate the US government's science and technology policies. The document emphasizes the benefits of an open research environment, but stresses that this openness must be supported by appropriate safeguards. These guidelines were developed to aid higher education institutions in protecting their academic integrity and the security of their research.

Among a total of 21 recommendations, NSTC suggests to:

- Include all members of a given institution in the establishment of an organizational approach to research security
- Assess the institution's specific risk profile and develop policies and processes accordingly
- Centralize review and approval processes for international research cooperation
- Develop strict conflict of interest, conflict of commitment and disclosure policies
- Consider digital persistent identifier policies
- Develop appropriate training and guidance for staff, scholars and students
- Ensure compliance with all relevant policies and regulations
- Establish policies for securely hosting visiting scholars and other foreign visitors to campus
- Develop and maintain data security protections

National Science and Technology Council (NSTC)

Guidance for implementing national security presidential memorandum 33 (NSPM-33) on national security strategy for United States government-supported research and development (2022)

Target audience:	ministries, government agencies, funding agencies
Regional focus:	country agnostic (but China is explicitly mentioned as one of the countries that threaten research security)
Thematic focus:	research security and integrity (especially of state-funded research and innovation)
Structure:	general recommendations; guidelines for 5 key topics covered under NSPM-33 (1. Standardized disclosure requirements, 2. Digital Persistent Identifiers, 3. Consequences for violation of disclosure requirements, 4. Information sharing, 5. Research security programs)
Level of guidance:	detailed, practical guidance
Language:	English
Page total:	34 pages
Most relevant:	p. 1-21

The guidance was developed by the National Science and Technology Council's (NSTC) Subcommittee on Research Security to guide implementation of the National Security Presidential Memorandum (NSPM-33), issued in January 2021.

NSPM-33 primarily aims to protect intellectual capital, prevent misappropriation of research results, and ensure responsible use of taxpayer funds. At the same time, it seeks to maintain an open, attractive environment to foster research and innovation and to avoid xenophobia. To this end, the memorandum calls for disclosure requirements for actors in the R&D system to be strengthened and standardized to promote clarity and reduce bureaucratic hurdles. The memorandum also requires the establishment of research security programs at research institutions, directs departments and agencies to share information about individuals whose activities could threaten the security and integrity of research, and prohibits federal personnel from participating in foreign talent programs.

In the guidance, the NSTC calls for the development of standardized application forms and instructions that can be used by each federal funding agency and adapted as needed. The goal of these standardized forms is to ensure that the same information must be disclosed in the same manner when applying for funding from all research funding agencies. Digital Persistent Identifiers are to be increasingly used for this purpose. The subcommittee is also planning standards for the requirements of research security programs as well as a standardized and centralized certification process as the next step.

The guidelines are organized into 5 topic areas. Within each topic area, recommendations include the following:

1. Standardized disclosure requirements

- Forms for initial disclosure as well as for annual updates should be standardized and supplemented with clear, uniform instructions. NSTC will provide templates for this purpose.
- Disclosure requirements for researchers include, for example, their organization, position, and participation in foreign talent programs as well as other contracts with foreign programs/possibly other activities abroad, existing and intended funding sources, etc.

2. Digital Persistent Identifiers (DPI)

- DPI profiles should include all required disclosure information, be updated once a year, and be accessed by research institutions as soon as the researcher has given his/her permission to do so.
- Researchers who are supported by federal grant funds shall all be registered with a DPI service. For others, use of a DPI service is not mandatory, but may be requested by research authorities.

3. Consequences for violation of disclosure requirements

- NSTC will develop a template for a standard procedure that research agencies can use when they suspect non-compliance with disclosure requirements.
- Violations of disclosure requirements may result in criminal, civil, and/or administrative consequences. Other possible consequences: e.g., rejection of applications, withholding of grant funds, entry into a database to support award decisions.

4. Exchange of information

- Funding agencies may share information with law enforcement, the Department of Homeland Security, and states about individuals who, for example, have violated disclosure or other obligations, are participating in foreign talent programs, or whose activities clearly indicate an intent to threaten the security and integrity of research, to the extent that such sharing is consistent with privacy laws and other legal restrictions.

5. Research security programs

- Research institutions receiving grant funds in excess of $50 million per year must have a demonstrated certified research security program. Programs must cover topics such as cybersecurity, foreign travel security, insider threats, and export controls, as appropriate.
- The U.S. Government will provide standardized technical assistance to support the development of training content and programmatic guidelines, tools, and best practices.
- The U.S. Government should support the formation of a community consortium to develop and maintain research security program information and implementation resources for research organizations.
- To the extent possible, the development of program content should be a collaborative effort between the government and research organizations.

University of Rochester

International Research & Global Collaboration (2019)

Target audience:	University of Rochester community
Regional focus:	country agnostic
Thematic focus:	disclosure policies; hosting visitors; travel; publications
Structure:	overview over relevant policies; guidelines
Level of guidance:	general
Language:	English
Page total:	13 pages
Most relevant:	p. 5-12

The University of Rochester published these guidelines to ensure mutually beneficial cooperation with international partners and compliance with relevant policies and regulations in an environment that increasingly raises concerns about the risks and challenges involved in international academic collaboration.

The university recommends to:

- Disclose all types of collaborative activities that involve foreign entities; all types of foreign or domestic funding, grants, and gifts; and participation in foreign talent programs
- Exercise greater oversight over visiting scholars and short-term visitors
- Ensure data and intellectual property protection, particularly where sensitive research is concerned
- Ensure that publications are affiliated with the university
- Register travel abroad with the university. Avoid bringing sensitive data to the destination, consider using a sanitized laptop