

Toolbox on Knowledge Security and Open Science

Annex to the report “Openness and Security: Two Pillars, One System”

Project partners:

University of Bern (project leader)

Center for Security Studies (ETH)

University of Applied Sciences and Arts Western Switzerland (HES-SO)

Commissioned and supported by swissuniversities

Contents

1.	Recommendation 1: Develop a comprehensive Knowledge Security policy.	5
2.	Recommendation 2: Establish dedicated Knowledge Security officers or specialised internal units.	5
3.	Recommendation 3: Implement Knowledge Security training and awareness programmes.	8
4.	Recommendations 5, 6 and 7: Knowledge Security measures in Open Science and Open Science as a Knowledge Security measure	8
5.	Incentives & evaluation alignment	9
1.	Comprehensive guidance or risk appraisals	10
2.	Content	10
2.1	Subjection to export controls	10
2.2	Lists of critical technologies.....	11
2.3	Determining dual-use potential of research projects.....	11
3.	Partners	12
3.1	Comprehensive assessment tools	12
3.2	Embargoes and sanctions.....	13
3.3	Assessing the networks of institutions or researchers	13
3.4	Lists of critical institutions due to military proximity	14
3.5	Other considerations	14
4.	Infrastructure	14
Annexes		15

This toolbox is designed to support researchers and research institutions in navigating the evolving landscape of Knowledge Security, in particular in the context of Open Science.¹ It builds on the shared understanding reflected in the G7 Common Values and Principles on Research Security and Research Integrity that “openness and security are not contradictory but complementary and mutually reinforcing.”

In its report, the swissuniversities'-led National Working Group on Knowledge Security identifies weaknesses in the Swiss system in managing Knowledge Security, notably a lack of “dedicated expertise in knowledge security assessment and risk management”: “Traditional academic administrators may not have the specialised knowledge required to evaluate complex security implications of research projects or international partnerships. This capability gap represents a fundamental challenge that must be addressed through training, recruitment, or external support mechanisms.”²

The report *Openness and Security: two pillars, one system*³ is one step into the direction of filling that gap. This toolbox, that complements the broader report, provides practical guidance, examples, and operational tools.

The toolbox is addressed to university management, and only indirectly to researchers. The tools herein can be used and adapted to the institution-specific context and governance framework.

It aims at helping identify, assess, and manage potential risks while preserving the openness, international collaboration, and academic freedom that are fundamental to scientific progress. Measures should remain proportionate to actual risks, avoid unnecessary bureaucracy, and be applied in a non-discriminatory manner.

The toolbox is guided by five underlying principles.

1. “As Open As Possible, As Secure As Necessary”: Research outputs, methods, and collaborations should default toward openness unless legitimate risks require controlled access.
2. Proportionality: Security controls should be proportionate to actual risk, avoiding excessive bureaucracy that suppresses collaboration or innovation.
3. Researcher enablement: Researchers should not carry the full burden of compliance. Institutions must provide infrastructure, training, advisory services, and administrative support.
4. Transparency and accountability: Knowledge Security decisions should be documented, reviewable, and governed through clear institutional procedures.

¹ For a definition of “Open Science”, please see the report to which this toolbox belongs: University of Bern/Center for Security Studies/Haute école spécialisée de Suisse occidentale: *Openness and security: two pillars, one system*, Bern: 2026. We follow the UNESCO’s definition and focus on the two dimensions of open access and open research data.

² [Swissuniversities – Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities](#), p. 8.

³ The report lays out the regulatory framework on Knowledge Security and Open Science internationally and in Switzerland, asks and identifies which risks to Knowledge Security actually exist in the specific context of Open Science, explains which factors lead to or increase risks to Knowledge Security in Open Science and describes how institutions in Europe and Switzerland currently address Knowledge Security risks in Open Science. Before concluding and providing recommendations, we dare to provide an outlook into the future of Knowledge Security and Open Science.

5. International collaboration preservation: The goal is not de-globalization of science, but resilient, ethical, and secure collaboration.

The toolbox is structured into two sections: Section 1 lists tools for addressing Knowledge Security in the specific context of Open Science. Section 2 is dedicated to other risk assessment and classification tools and guidance that are not specific to the Open Science context, but that institutions might deem useful in addressing Knowledge Security risks and for reinforcing their risk management frameworks.

Most, but not all tools referenced in the toolbox have been developed in the context of the swissuniversities project on Knowledge Security and Open Science (marked below as “**Project deliverable**”). We have also compiled existing resources that we deemed useful. In cases where links are no longer active, users are encouraged to search for the publication title online.

The following sections take up the recommendations of Chapter 6 of the report *Openness and Security: Two Pillars, One System* and suggest concrete practical tools for implementing them.

1. Recommendation 1: Develop a comprehensive Knowledge Security policy.

Knowledge Security should be integrated into institutional strategy, research governance, and risk management frameworks. Institutions should establish clear Knowledge Security policies covering key areas such as due diligence procedures for international collaborations, technology transfer protocols, information security measures, and mechanisms for reporting Knowledge Security concerns. It should be aligned with national and institutional rules on export controls, data protection and intellectual property.

These policies should be developed in consultation with the research community to ensure that they are practical, proportionate, and transparent. At the same time, they should minimise unnecessary administrative burdens while remaining sufficiently flexible to respond to evolving risks and regulatory requirements.

Open Science should be taken into account in this policy and within operations as a matter of course. As a best practice, institutions should, in addition, adopt a dedicated policy on Knowledge Security in Open Science that:

- Defines the national and the institution's risk appetite regarding openness versus restriction
- Provides concrete and institution-specific guidance
- Differentiates between disciplines and risk levels (e.g. humanities vs dual-use STEM fields).

In line with recommendations 5, 6 and 7 of the report *Openness and Security: Two Pillars, One System*, we recommend that at the operational level, Open Science practices are seen and used as Knowledge Security measures and that Open Science practices are improved through Knowledge Security measures.⁴ This approach ensures that both domains become mutually reinforcing, all the while reducing the risk of creating yet another administrative procedure.

2. Recommendation 2: Establish dedicated Knowledge Security officers or specialised internal units.

In order to develop and properly implement the policies and procedures as mentioned above in Chapter 1, Section 1, institutions need to invest into a support structure that covers both legal, compliance and security aspects as well as Open Science. Due to the overlapping nature of Knowledge Security and Open Science, the separate units should be trained in the other area respectively.

The following service portfolio is recommended to institutions:

1. Open Science helpdesk: publishing and repository support

⁴ A practical tool is suggested in Chapter 1, Section 4 of this toolbox.

This service is the front door for researchers who want to publish outputs openly and comply with funder or institutional requirements.

Core functions

- Open-access publishing support: advice on publisher policies, APC funding, transformative agreements, and rights retention
- Repository support: depositing articles, datasets, software, theses, and other outputs in institutional or disciplinary repositories
- Metadata and discoverability: ensuring outputs are properly described, linked (ORCID, DOI, grant IDs), and indexed
- Licensing guidance: helping researchers choose appropriate licenses (e.g., Creative Commons)
- Compliance monitoring: checking adherence to funder mandates and institutional Open Science policies

2. Data stewardship: FAIR and secure data management, including Knowledge Security risks in Open Science

This service ensures that research data are both reusable and protected appropriately.

FAIR data management

- Findable: persistent identifiers and rich metadata
- Accessible: controlled or open access mechanisms
- Interoperable: use of standards and common formats
- Reusable: documentation, provenance, and licensing

Security and governance functions

- Data classification (public/ internal/ confidential/ restricted, or: open/ restricted/ classified/ export-controlled, etc.)
- Secure storage and access controls
- Encryption, backup, and retention policies
- Support for Data Management Plans (DMPs)

Knowledge Security role in Open Science

A modern data stewardship unit also evaluates whether making data openly available could create Knowledge Security risks. Examples include dual-use research data, sensitive infrastructure information, strategic technologies, or data subject to contractual or national restrictions.

The steward, therefore, performs or coordinates in collaboration with Knowledge Security compliance officers (see below):

- Risk identification
- Risk assessment (likelihood and impact)
- Risk mitigation (partial release, embargoes, controlled access, anonymization)
- Documentation of decisions

3. Knowledge Security compliance officer

Institutions should appoint Knowledge Security officers and/or establish a Knowledge Security committee to support implementation and decision-making.⁵ They advise researchers and leadership, coordinate risk assessments, review complex or high-risk cases, provide clear escalation pathways for difficult decisions, and ensure consistent and proportionate application of policies across the institution and the effective and harmonised integration of Knowledge Security into other units within the institution (e.g. Open Science or international affairs offices, etc.).

Primary responsibilities⁶

- International collaboration assessments: identify partners, funding sources, jurisdictions, and strategic technology areas; assess risks of unwanted transfer of knowledge, technology, data, or expertise
- Staff recruitment screening: review appointments in sensitive research areas; identify conflicts of interest, undisclosed affiliations, or sanctions concerns
- Student screening (where legally permitted and institutionally adopted): assess access to highly sensitive facilities, datasets, or technologies; apply proportionate, risk-based measures
- Open Science risk management: review whether planned publications, preprints, software releases, or data sharing could create Knowledge Security concerns; coordinate mitigation measures before release
- Training and awareness: provide guidance to researchers, supervisors, administrators, and leadership

This role should not function as a blanket gatekeeper for international collaboration. Good practice is risk-based, proportionate, and transparent, balancing academic freedom with security obligations.

4. Legal and export controls office: regulatory support

This service provides the formal legal and regulatory interpretation that underpins the other functions.

Typical responsibilities

- Export control classifications and sanctions screening
- Contract review
- Intellectual property advice
- Data protection and privacy compliance
- Record keeping and audit support
- Liaison with national authorities

5. How the four services fit together

Open Science helpdesk → Data stewardship → Knowledge Security officer → Legal & export controls

For example:

- A researcher wants to publish a paper and release a dataset
- The Open Science helpdesk assists with repository deposit and licensing
- Data stewardship checks FAIRness, confidentiality, and potential security sensitivities
- If the project involves sensitive data, the Knowledge Security officer gets involved in risk assessment and -management

⁵ See also the recommendation of the National Working Group here: [Swissuniversities – Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities](#), Section 4.1, as well as recommendation 2 of the report *Openness and Security: Two Pillars, One System*.

⁶ See also the recommendation of the National Working Group here: [Swissuniversities – Knowledge Security in Switzerland: A Strategic Framework for Higher Education Institutions and Authorities](#), Section 4.2 and Annex 3.

- If controlled technology or sanctions issues arise, the Legal/export controls office determines the applicable legal requirements.
- The researcher receives one coordinated decision path rather than conflicting advice from multiple offices.

3. Recommendation 3: Implement Knowledge Security training and awareness programmes.

The precondition for successfully implementing Knowledge Security measures into institutional operations is awareness and acceptance within the researchers' community. Initiating a bottom-up movement, rather than imposing top-down requirements, will prove more effective and sustainable. The following tools are meant to support institutions in raising awareness and informing about Knowledge Security (in Open Science).

- **Project deliverable:** Do's and Don'ts for Knowledge Security in Open Science (Annex 1)

Concise reflection and guidance tool, intended to raise general awareness

For whom: Researchers

When: Timeless tool

- **Project deliverable:** Slides on "Introduction to Knowledge Security in Open Science" (Annex 2)

What: Slides introducing Knowledge Security in Open Science, to be adapted according to each institution's needs and priorities.

For whom: University administration, tasked with raising awareness among researchers.

When: Timeless tool; could be shared during onboarding of new staff and/or during regular trainings.

4. Recommendations 5, 6 and 7: Knowledge Security measures in Open Science and Open Science as a Knowledge Security measure

The following tools are meant to support institutions in integrating Knowledge Security into Open Science practices and to use Open Science practices as Knowledge Security tools.

- **Project deliverable:** Knowledge Security Management Plan (for Open Science, KSMP) (Annex 3)

What: Suggestion for a comprehensive questionnaire that can be used as a risk assessment tool to determine Knowledge Security risks while implementing Open Science. It is a tool to point out certain risks and raise awareness.

For whom: To be completed by researchers in collaboration with data stewards and Knowledge Security officers.

When: As early as possible in the research process, but the latest before publication of data.

- **Project deliverable:** Decision tree on data sharing (Knowledge Security in Open Science) (Annex 4)

What: A practical decision tree that complements and operationalises the Knowledge Security Management Plan (for Open Science). The KSMP can clarify or provide indications on how to answer the questions posed in the decision tree.

For whom: researchers, possibly in collaboration with data stewards and Knowledge Security officers.
When: As early as possible in the research process, but the latest before publication of data.

- **Project deliverable:** Knowledge Security risks in Open Science: Risk mitigation measures (Annex 5)

What: Compilation of measures mitigating the risks identified in the Knowledge Security Management Plan. Can be used as a follow-up tool to the KSMP or the decision tree, once risks have been identified and/or once a decision has been taken concerning the level of restriction of a dataset.

For whom: Researchers in collaboration with data stewards and Knowledge Security officers.

When: As soon as risks are identified, but the latest before data publication.

u^b

5. Incentives & evaluation alignment

Knowledge Security and Open Science can both be strengthened through incentives and the alignment of an institution’s evaluation system, complementary to possible CoARA-standards. The objective is to reward researchers for responsible openness and secure research conduct.

For instance, the following elements can be included into an existing promotion criteria framework:

Domain	Example indicator
Open access	Percentage of openly accessible publications
Open data	FAIR-compliant datasets deposited
Reproducibility	FAIR code, workflows, protocols
Public engagement	Citizen science and societal impact
Responsible collaboration	Completion of due diligence procedures
Secure data practices	Appropriate handling of sensitive data

In a similar manner, institutional awards could be handed out for the same activities and internal grants could take Open Science and Knowledge Security criteria into account.

In Chapter 3 of the report Openness and Security: Two Pillars, One System, we analyse the factors that lead to or increase risks to Knowledge Security. The following tools support institutions in assessing the likelihood of legal and security risks beyond Open Science along these factors (content of the research (output), partners, and infrastructure).

u^b

1. Comprehensive guidance or risk appraisals

The following two tools cover several legal and security risks and, therefore, do not fit into the one of the categories (content, partners, infrastructure).

- Government of the Netherlands (2022): [National knowledge security guidelines](#)
What: Guidance on threat assessment, legal framework, risk assessment, risk management, international partnerships, recruitments and cybersecurity
For whom: Institutions of higher education and their management
When: Before or while implementing institutional governance structures
- DLR Projektträger/Safeguarding Science (2024): [Due Diligence in Science](#)
What: Guidance mainly on risks related to recruitments and international collaborations
For whom: Institutions of higher education and their management
When: Before or while implementing institutional governance structures

2. Content

2.1 Subjection to export controls

- Swiss export control lists
 - [Goods Control Act](#)
 - [Goods Control Ordinance](#)
 - [War Material Act](#)
 - [War Material Ordinance](#)
 - Chemicals Control Ordinance (in [German](#), [French](#), or [Italian](#))
 - Ordinance on the Export and Brokering of Goods for Internet and Mobile Communications Surveillance (in [German](#), [French](#), or [Italian](#))
 - Annexes listing the goods that are export-controlled (in [German](#), [French](#), or [Italian](#))
- Foreign provisions with extraterritorial application
 - The US regulations on sanctions, embargoes and export controls are extraterritorial in nature. They are applied worldwide if certain connecting criteria are met:
 - US persons: all US citizens, all persons residing in the USA and persons with a US residence permit (e.g. green card), regardless of their location; all natural and legal persons who are residents or domiciled in the USA; and all companies domiciled in the USA and their foreign branches.
 - US products, including products that are at least 10% or 25% based on products of US origin (e.g., a drone that uses US software for control).

- US export control regimes:
 - Export Administration Regulation (EAR): Dual use goods ([Commerce Control List](#))
 - [International Traffic in Arms Regulations \(ITAR\)](#): Military goods
- Help for searching the goods lists:
 - The goods lists are only available in German, French, or Italian. If you need the goods lists in a different language, you can consult the EU Dual-use goods list (Annex 1 to [Regulation \(EU\) 2021/821](#)), which is available in all EU languages. It is not 100% identical to the Swiss list, so be sure to check back whether the entry you found is the same in the Swiss list.
 - Keyword indices to determine whether a certain good/technology/software is subject to export controls
 - Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA): [Joint, non-binding glossary for Part I of the Export List and Annex I to the EU Dual-Use Regulation](#) (in German). This keyword index is based on the EU Dual-use goods list, so you need to verify whether the entry you found is the same on the Swiss list.
 - Bureau of Industry and Security (BIS): [Interactive Commerce Control List](#). This is the US dual-use goods list, which is searchable with keywords. Again, as the Swiss list is not 100% identical to the US list, you must check back whether the entry you found is the same in the Swiss list.

2.2 Lists of critical technologies

- DLR Projektträger/Safeguarding Science (2026): [Lists of critical and sensitive technologies – scope, purpose and intended audience](#) (*this publication explains lists developed by different actors and countries*)
- [EU list of critical technologies](#)
- US Critical and Emerging Technologies List ([January 2026](#))
- Canadian [Sensitive Technology List](#)
- ETH list of critical technologies (listed in this article: [Dual use and sanctions: these applications require security screening – Staffnet | ETH Zurich](#))

2.3 Determining dual-use potential of research projects

- **Project deliverable:** Questionnaire on dual-use potential (Annex 6)

What: A comprehensive questionnaire on determining the dual-use potential of a given research project in artificial intelligence/machine learning, biotechnology, chemistry, robotics, cybersecurity, materials science, energy systems, quantum technologies, aerospace, synthetic biology, or neuroscience. A tool to raise awareness and determine risks, mitigation strategies or institutional or government oversight.

For whom: Addressed to researchers.

When: Throughout the entire research lifecycle: during project planning, whenever a project enters a new phase or produces unexpected results, before transferring results or materials to collaborators, and prior to the publication or other dissemination of research findings.

- Robert Koch Institut (2013): [Dual use potential of life science research](#) (Section 3)

What: The Robert Koch Institute's Code of Conduct for Risk Assessment and Risk Mitigation establishes principles and procedures for identifying, assessing, and mitigating the dual-use potential of research in the life/health/medical sciences.

For whom: Primarily researchers, project leaders, and managers, particularly those conducting life sciences research involving pathogens, toxins, or other research with potential dual-use implications.
When: Throughout the entire research lifecycle: during project planning, whenever a project enters a new phase or produces unexpected results, before transferring results or materials to collaborators, and prior to the publication or other dissemination of research findings.

- Netherlands Biosecurity Office (2021): [Dual-use Quickscan](#)

What: The Dual-Use Quickscan is an online self-assessment tool that helps life sciences researchers identify potential dual-use aspects of their research through a structured questionnaire and raises awareness of biosecurity risks.

For whom: Researchers working with microorganisms or related biological knowledge and technologies.

When: At any stage of the research lifecycle, from project design to publication.

- Joint Research Centre & University of Liège: [TIM Dual-Use Web Platform](#) (STRIKE project, Units G.II.7 and T.5)

What: TIM Dual-Use is a web-based text mining platform that maps scientific publications, patents, and EU-funded research projects to identify research with potential dual-use relevance based on the EU dual-use control list and emerging technologies. It supports awareness, trend analysis, and institutional compliance by helping users identify potentially sensitive research outputs. Can be used to detect dual-use research or research involving export-controlled items retroactively (i.e. after publication).

For whom: Research institutions, universities, policymakers, and export control practitioners.

When: To screen existing research outputs and monitor dual-use technologies for awareness, compliance, and strategic analysis.

3. Partners

3.1 Comprehensive assessment tools

- **Project deliverable:** Knowledge Security self-assessment for researchers and evaluation matrix for institutional management (Annex 7)

What: Self-assessment for researchers wishing to engage in international collaborations that analyses and raises awareness of Knowledge Security risks. The (optional) accompanying matrix allows university management to evaluate the self-assessment through a traffic light system.

For whom: The self-assessment is for researchers starting a new international collaboration. The evaluation matrix is a tool for university management/leadership that helps decision making.

When: Before an international collaboration is concluded.

- German Academic Exchange Service/Kiwi (2025): [Die KIWi-Checkliste Wissenssicherheit](#) (in German)

What: The KIWi Knowledge Security Checklist is a practical self-assessment tool that helps identify and reflect on Knowledge Security risks in international research collaborations through a structured set of questions covering partners, funding, export controls, intellectual property, and research ethics.

For whom: Individual researchers, or institutional management or administration when implementing institutional processes.

When: Before or during the establishment of international research collaborations, as an initial risk assessment.

- European Commission (2024): [Research Security – Building blocks for risk appraisal](#)

What: The European Commission's Building Blocks for Risk Appraisal provides a framework for assessing research security risks in international research and innovation collaborations. It proposes a structured, context-based appraisal covering the research field, partners, country context, and project-specific factors to support informed decision-making rather than restrict collaboration.

For whom: Research performing organisations, research funders, and higher education institutions.

When: Before establishing international research partnerships or awarding research funding.

3.2 Embargoes and sanctions

- Switzerland:
 - CH-SECO: [Engine for searching for subjects of sanctions](#) (individuals/entities)
 - CH-SECO: [Swiss sanction measures](#) (content available in German, French, or Italian)
- Foreign provisions with extraterritorial application
(US sanctions and embargoes must be applied to all US-citizens and green card holders, no matter their residence. EU sanctions must be complied with by all EU citizens and legal entities incorporated or registered under the law of an EU Member State - regardless of their country of residence or domicile. The same applies to UK citizens and legal entities with regard to UK sanctions)
 - US-Office of Foreign Asset Control (OFAC): [Sanctions Programs and Country Information](#)
 - US-OFAC: [Sanctions List Search](#)
 - EU-sanctions and embargoes: [Sanctions map](#)
 - UK sanctions and embargoes: [Trade sanctions, arms embargoes, and other trade restrictions - GOV.UK](#)

3.3 Assessing the networks of institutions or researchers

The following tools are commercial tools that are quite expensive and integrating them into an institution's due diligence processes can create dependencies. Most of the presented tools are focused on detecting networks involving sanctioned or military partners.

The European Commission is currently (2026) working on developing a public due diligence platform.

- [China Defence Universities Tracker](#)

A subscription-based tool that monitors more than 180 Chinese entities with links to defence, intelligence, and technology research. It enables users to explore potential dual-use capabilities, consult relevant sanctions listings, and assess global collaboration risks. The Tracker is designed as a targeted analytical resource for understanding institutional relationships. It is neither a profiling tool for individuals nor a basis for blanket restrictions, and it should not be interpreted as a blacklist. Rather, its purpose is to support informed, proportionate decision-making. While extensive, the Tracker is not exhaustive. Institutions not included may still present risks, and entries in the database may not capture the full scope or nature of an institution's links to defence and security sectors.

- [Strider Technologies](#)

Strider is a subscription-based tool that delivers an external, open-source intelligence view of the global research landscape. It identifies gaps between an individual's stated experience and public records due to prior research output, institutional engagement and long-term professional presence. It also offers a unified view across organisations, staff and research units, as well as continuous monitoring of nation-state risk.

u^b

- [Kharon](#)

Kharon is a risk intelligence platform that supports sanctions compliance, export control due diligence, supply chain risk management, and third-party screening. It uses open-source intelligence, network analysis, and data analytics to identify hidden relationships between individuals, organisations, ownership structures, and restricted or high-risk actors.

- [Xapien](#)

Xapien is an AI-powered due diligence and third-party risk assessment platform. It automates background research on individuals and organisations by combining information from the open web, news sources, corporate registries, sanctions and watchlists, and other commercial datasets into a single, source-backed report.

- [Dimensions Research Security](#)

This subscription-based tool maps international affiliations, collaborations, and funding flows. It supports the identification of dual appointments, participation in foreign talent programs, and potential links to sanctioned entities, thereby helping institutions better assess and manage collaboration risks.

3.4 Lists of critical institutions due to military proximity

- Government of Canada: [Named Research Organisations List](#)
- [Entities identified as Chinese military companies operating in the US](#)
- [Japanese End User List](#)
- Australian Strategic Policy Institute: [China Defence Universities Tracker](#)

3.5 Other considerations

- [World Justice Project Rule of Law Index](#)
- [Democracy Index](#)
- [Human Rights Index 2025: Best and Worst Countries Ranked](#)
- [Human Freedom Index](#)
- [Freedom House Index](#)
- [Academic Freedom Index](#)
- [Corruption Perception Index](#)

4. Infrastructure

Risks to Knowledge Security in relation to infrastructure can be assessed using the Knowledge Security Management Plan proposed in Chapter 1, Section 4.

Annexes

Click to download:

1. [Do's and Don'ts for Knowledge Security in Open Science](#)
2. [Slides on “Introduction to Knowledge Security in Open Science”](#)
3. [Knowledge Security Management Plan \(for Open Science\)](#)
4. [Decision tree on data sharing \(Knowledge Security in Open Science\)](#)
5. [Knowledge Security risks in Open Science: mitigation measures](#)
6. [Questionnaire on Dual-use potential](#)
7. [Checklist for researchers and evaluation matrix for institutional management for international collaborations](#)

u^b