CESAER

The strong and united voice of universities of science and technology in Europe

Input note

Topic:	Research security as a collective responsibility: empowering universities, enabling Europe
Date:	27 October 2025
To:	EU institutions, member states, partners and stakeholders
From:	CESAER

Research is one of Europe's greatest assets. It drives knowledge, innovation, and prosperity, and underpins Europe's global competitiveness. This excellence depends on attracting and retaining top talent and on ensuring timely access to and dissemination of latest scientific knowledge. While these drivers of excellence increasingly face restrictions in sensitive areas, such as dual-use technologies, a key condition for sustaining excellence remains academic freedom.

Academic freedom is a cornerstone of Europe's research and innovation ecosystem and the European Research Area. As a fundamental right, it underpins the principles of research integrity, open science, transparency, and trusted international cooperation. However, academic freedom – and the aforementioned principles – can only flourish when research security is safeguarded.

Without adequate measures, research becomes vulnerable to misuse and loss of trust, risking restrictive responses that erode openness. Proportionate safeguards instead create the stable conditions in which academic freedom, scientific excellence, and international collaboration can thrive. Therefore, proportionate, risk-based measures are needed to protect the research community from misuse and undue influence by (non-)state actors posing economic, strategic, or security risks.

The need for implementing such measures has become more pressing as research faces growing risks: foreign interference, misuse, compliance pressures, and ethical challenges. These concerns were highlighted in the May 2024 Council recommendation on enhancing research security. Universities of science and technology, built on openness, collaboration, and excellence, are at the forefront of addressing these challenges.

Strengthening research security should be understood as an evolving process. For some universities, this may start with a simple contact point; for others, it may involve comprehensive institutional policies, supported by dedicated staff and robust governance. Many institutions have already taken first steps — raising awareness, establishing procedures, and building capacity — and are committed to going further.

Research security is not about closing doors but about building resilience through collective responsibility and trust. Europe's strength depends on how well its actors work together, making a level playing field across the continent essential—not by defaulting to the strictest standards but by ensuring consistent application of rules and adequate support by national authorities so that universities and researchers face fair and comparable expectations wherever they operate.

Only by working together, Europe can remain open, innovative, and globally competitive. This input note builds on two years of work within CESAER since our pioneering 2023 white paper, and sets out key recommendations to help Europe strengthen research security while safeguarding the benefits of scientific excellence and open science.

To succeed, action is needed in five interlinked areas: building a strong institutional foundation; incentivising and empowering researchers; integrating openness and security; ensuring responsible collaboration; and assuming collective responsibility by co-creating a European level playing field.

1. Building a strong institutional foundation: research security as a journey

Many universities face an uncertain and complex landscape in research security. Institutions often lack clarity on where to begin, how to build momentum, and how to balance legal, ethical, and academic considerations that span multiple departments.

A practical way to start implementing measures is to view research security not as a single policy or checklist, but as a gradual, institution-wide journey. Building a strong foundation begins with small, visible steps—such as leadership signalling commitment, raising awareness, and offering simple tools and guidance—before evolving into more advanced structures such as advisory teams, dedicated officers, and integrated governance frameworks. With appropriate tools, additional resources, and sufficient support from governments and the EU, research security can be embedded into existing governance structures and linked to scientific integrity, ensuring that it grows sustainably over time.

Early steps. Lessons learned and best practices for **universities** that help build a strong institutional foundation for research security:

- **Ensure visible commitment from senior university leadership**, signalling that research security is an institutional priority.
- **Create a multidisciplinary structure** by connecting research offices, legal advisers, technology transfer staff, human resources staff, and researchers to exchange expertise and assess risks collaboratively, even without introducing new resources.
- **Provide accessible guidance and practical tools** by publishing intranet pages, FAQs, templates, and decision trees to help researchers navigate risk assessment, compliance, and reporting.
- **Raise awareness** by conducting campaigns and encouraging researchers to carry out initial risk self-assessments, recognising that culture change takes time.

Advanced steps. Lessons learned and best practices for **universities** that help to further strengthen a solid institutional foundation for research security:

- **Align research security** measures with existing processes and committees, rather than creating separate, siloed processes.
- **Engage in sector-wide dialogue** by exchanging best practices and lessons learned between universities.
- **Provide structured training modules** tailored to researchers and administrators, and support staff.
- **Develop a roadmap with milestones** for gradually expanding research security policies and support structures. The roadmap should clearly outline key steps, responsibilities, and institutional structures, highlighting where individual researchers fit within the overall process.
- **Set up a dedicated advisory team** and establish dedicated roles to provide legal, technical, and academic support for sensitive cases, streamline risk assessment, and offer support to researchers.

2. Incentivising and empowering the researcher

Researchers are often best placed to recognise technological risks related to research security in their work, but they frequently lack clear incentives, consistent guidance, and sufficient support to address them. Awareness of research security risks amongst the researcher community varies widely, while increasing pressures to secure funding and publish heighten the likelihood that critical risks may be overlooked.

Universities have a key role in empowering researchers as active partners in safeguarding knowledge by providing clear responsibilities, targeted training, and recognition for their contributions to research security.

To enable universities to empower researchers effectively and ensure robust research security, EU institutions, national governments, and—where relevant—regional authorities must provide adequate support, resources, and coherent policy frameworks.

Early steps. Lessons learned and best practices **for universities** that help incentivise and empower researchers:

- **Provide publicly available training, online resources, and sector guidelines** for researchers, and create safe channels to flag concerns or incidents.
- **Implement a structured, proportionate "risk check"** alongside ethics approval or data management planning, making it a natural part of project design and tailored to the level of risk and type of research.
- **Build peer networks and share practical experiences with colleagues** through organising lab meetings or departmental forums, so that knowledge about risk scenarios circulates informally as well as formally.

Advanced steps. Lessons learned and best practices **for universities** that help incentivise and empower researchers:

- **Incentivise, recognise and reward researchers who contribute to safeguarding research** through career support, acknowledgment in performance reviews, and integration into professional development programmes.
- **Define clear responsibilities for researchers and support staff and provide structured guidance** through ethics committees, advisory teams, and dedicated contact points, recognising researchers and support staff as partners in keeping research secure.
- **Integrate research security and risk management training across all career stages.** While early-career researchers should be given the opportunity to develop these skills as part of doctoral and postdoctoral programmes, targeted training for senior researchers is essential, given their international engagement and exposure to potential security risks.

We call on the EU institutions to:

- **Improve the integration of research security into the reviewing process of the EU funding programmes** and improve the availability of information for researchers, support staff and universities to make informed decisions, for instance by further stimulating research funding organisations to make necessary information available as outlined in the 2024 Council recommendation.
- **Empower researchers and universities to make informed decisions by establishing an EU-level research security helpdesk** and engage with universities and other research performing organisations in developing a virtual toolkit or academy offering and disseminating practical templates (e.g., risk assessment checklists, collaboration agreements, publication review forms), case studies, and guidance in assessing and managing research security risks.
- **Provide dedicated EU-level and national funding** and clear policy guidance to support universities in further advancing research security structures as part of the European Research Area, ensuring they have the resources and regulatory clarity to implement proportionate measures without hindering international collaboration.

3. Integrating openness and security through a mutually reinforcing approach

Universities of science and technology frequently face the challenge of balancing open science requirements with the need to protect sensitive knowledge. Although such considerations have long existed in relation to for example commercially sensitive information and protection of personal data, they have received far less attention in the context of research security. While research funders often mandate open publication of results to promote scientific excellence, the lack of clear guidance on research security can result in fragmented approaches or overly cautious practices.

Embedding research security into open science frameworks allows universities to adopt risk-aware, proportionate measures that protect knowledge while enabling responsible collaboration. At the EU level, academic freedom must be legally guaranteed to ensure researchers can pursue their work independently, while principle-based guidance, tools, and secure platforms are essential to further integrate openness, security, and safeguards Europe's research community, both sensitive technologies and the individual researchers.

Lessons learned and best practices for **universities** to build a mutually reinforcing approach:

- **Align research security with codes of conduct, ethics policies, and open science strategies,** supported by clear governance and resources, demonstrating how improved research data management and risk-aware practices can simultaneously safeguard sensitive knowledge and promote openness.
- **Integrate risk assessment into research workflows** by including lightweight, structured checks in project planning to flag security concerns while maintaining openness where feasible.
- **Promote best practices for research security that provide guidance and clear instructions**. Help researchers identify security risks, integrate safeguards into workflows, and adopt risk-aware data sharing and publication practices.

We call on the EU institutions to:

- **Integrate research security explicitly into EU open science policies and vice-versa**, signalling that safeguarding sensitive knowledge and promoting openness are mutually reinforcing priorities.
- **Establish a legal framework at the EU level that guarantees academic freedom and protects researchers' independence.** Establish clear legal protections to ensure that researchers can pursue their work independently and without undue interference, reinforcing academic freedom, research security, and openness across Europe.
- **Ensure that research security includes the protection of individual researchers,** not just technologies. Develop EU-wide guidance and frameworks to be implemented at national level to safeguard researchers' safety and well-being when this is at risk, building on best practices at leading universities.
- **Actively engage stakeholder organisations in structured dialogue to help universities strengthen their resilience** against threats to academic freedom, institutional autonomy, foreign or political interference, and extraterritorial legal pressures.
- **Promote the development of federated secure data platforms** that enable data sharing and working with data across domains and countries, ensuring interconnections between initiatives such as the European Open Science Cloud, the Common European Data Spaces, and GAIA-X. These federated platforms should have built-in safeguards inspired by the FAIR principles meeting open science and research security standards, offer clear guidance to users, and integrate export control and sanctions considerations into their design and operations.

4. Ensuring responsible collaboration: compliance, screening, and international partnerships

Navigating international collaborations responsibly present universities with a delicate balance: fostering open, innovative research while complying with export controls, sanctions, and regulations for example on dual-use technologies. At the same time, Inconsistent guidance and uneven screening practices can create gaps, duplication, or overly cautious approaches, potentially limit collaboration and increasing administrative burden.

Responsible collaboration requires risk-aware, proportionate measures at multiple levels. Universities need clear internal procedures, dedicated compliance contacts, and mechanisms to assess partners and projects. National authorities and the EU institutions play a critical role in providing guidance, financial support, and secure platforms to enable informed decision-making, promote best practices, and ensure that partnerships are evaluated consistently and responsibly.

Lessons learned and best practices for **universities** that help advance responsible collaboration and compliance:

- **Assess institutions and affiliations rather than nationality alone** during risk-based screening of partners and map key collaborations to identify strategic risks.
- **Establish internal compliance focal points**. Set up dedicated legal, tech-transfer, and research security contacts to advise researchers and liaise with authorities to interpret and implement rules and regulations proportionately.
- **Establish transparent processes and scalable monitoring** by defining clear procedures for risk assessment, approvals, and reporting, and maintaining registers of sensitive projects.
- **Frame research security as part of research integrity** in institutional communication, emphasising shared values rather than only compliance.
- **Coordinate and facilitate networks** where universities can exchange lessons learned and best practices on responsible international collaboration.

We call on national governments to:

- **Establish national advisory bodies (national contact points) and safe digital platforms,** as recommended in 2024 Council recommendation, for universities and their researchers to discuss with the national authorities for instance when faced with a challenging specific challenging situation, report risks and access guidance while preserving academic freedom.
- **Prevent the creation of 'autonomy traps'**, situations in which universities may seem to be autonomous but are not provided the resources and the means to effectively exercise it, or are encumbered with autonomy and responsibilities in areas not related to their core mission.

- **Provide scalable training modules, workshops**, and make additional resources available to enable capacity-building and avoid autonomy traps.
- **Provide clear guidance on minimum standards and boundaries** for risk assessment, due diligence, and compliance practices. This ensures sufficient uniformity while allowing universities necessary flexibility in implementation.
- **Issue transparent criteria and guidance** for evaluating partnerships, scholarships, and collaborations with third countries, together with universities and other research performing organisations.

We call on the EU institutions to:

- **Establish a secure European database of research partners** to support the informed and consistent decision making of universities in relation to global engagements and performing due diligence, providing an alternative to commercial tools such as the recently renewed ASPI Chinese Defence Universities Tracker.
- **Explore the feasibility of establishing a secure, anonymised federated information exchange and peer learning platform at EU level** where university personnel, member states and relevant authorities can share useful information related to research security incidents, best practices, and lessons learned, strengthening collective oversight and peer learning.
- **Establish a European Centre of Expertise on research security** as called for by the 2024 Council recommendation on research security and ensure the coordinated action and transparent dialogue between any forthcoming contact points and help desks related to research security. And, broaden the target group of the SME sanctions helpdesk to provide support to universities and researchers at EU level.
- **Provide harmonised guidance and enhanced legal clarity on export control and sanctions compliance** for universities by ensuring that EU member states interpret and apply existing rules consistently by establishing an EU-level helpdesk to offer guidance and best-practice advice on technical assistance, intangible technology transfer, and country-specific risks, while respecting that legal authority remains with national authorities.
- **Enhance the EU sanctions tracker's usability** by allowing universities and research performing institutions to easily search for applicable technology-related sanctions, including clear categorisation by country, sector, and type of restriction, with regular updates and guidance on interpretation.
- **Clearly integrate dual-use technology safeguards into Horizon Europe,** as elaborated in our 2024 dual-use technology position.

5. Assuming collective responsibility by co-creating a European level playing field

Ensuring effective research security across Europe remains challenging due to fragmented rules, ambiguous definitions, and uneven levels of support and guidance among member states. These divergences can create confusion, siloed approaches, and inconsistent safeguards, hindering universities—and Europe as a whole—in developing coherent research security strategies. At the same time, it is crucial to recognise that universities are not, and should not be, tasked with intelligence or counter-espionage responsibilities.

Enhancing research security requires research-performing organisations, national authorities, and EU institutions to assume collective responsibility and co-create a European level playing field.

We call on national governments to:

- **Allocate additional targeted funding to universities** to enable the development of research security structures, implementation of training, and establishment of cross-departmental coordination without further burdening existing constrained institutional budgets.
- **Develop national guidelines and FAQs** in close collaboration with the research and innovation community to assist universities in implementing research security measures and setting up internal systems.
- **Foster national cooperation and knowledge exchange.** If not yet organised by the sector itself, establish working groups that bring together research organisations, national authorities, and advisory bodies to share lessons, harmonise practices, and coordinate support.
- **Establish trusted channels to provide universities with relevant, proportionate information** (e.g. on high-risk entities or individuals), enabling secure intelligence sharing and informed risk assessments while respecting legal and data protection boundaries.
- **Define and communicate a clear division of tasks and responsibilities** between authorities and universities. For example, visa and entry screening responsibilities should remain with national authorities, while universities retain autonomy over institutional partnerships. This avoids duplication, overreach, and legal uncertainty.

We call on the EU institutions to:

- **Implement or coordinate research security measures** at EU level to avoid undesirable ('waterbed') effects amongst member states.
- **Define clear EU-wide standards and terminology.** Develop consistent definitions for "research security," "responsible internationalisation", "technical assistance" and related concepts to guide universities and member states in coherent implementation.

- **Launch dedicated EU funding calls** to support the development of European-wide educational tracks for research security experts and HR staff. These should include training modules, workshops, and resources that build research security skills consistently across institutions, strengthening both the European Research Area and the European Education Area.
- **Establish a European Research Security Forum** for regular exchanges between universities, member states, relevant authorities, and the European Commission to ensure shared understanding around responsibilities and exchange lessons learned and best practices.

Conclusion

Strengthening research security across Europe is essential to safeguard academic freedom, protect researchers and knowledge, and enable open, excellent science. Achieving this requires universities, national authorities, and EU institutions to share responsibility, implement proportionate risk-based measures, and foster a level playing field across Europe.

By embedding research security into institutional practices, supporting researchers, integrating openness and security, ensuring responsible collaboration, and promoting multi-level cooperation, Europe can remain open, innovative, and globally competitive.

Collective action, clear guidance, and adequate resources will ensure that research security strengthens — rather than restricts and weakens — the independence, trust, and excellence of Europe's research and innovation ecosystem.

For more information, please contact Advisor for Research Vincent Klein Ikkink.

This document can be referenced using https://doi.org/10.5281/zenodo.17453941