CHANGER

CHALLENGES AND INNOVATIVE CHANGES IN RESEARCH ETHICS REVIEWS

EUROPEAN POLICY BRIEF

Challenges and recommendations for research security: Learning from research ethics and integrity

June 2025

RESEARCH SECURITY

Policy Brief at a glance

CHALLENGE	1	2	3	4
	Diverse understanding of RS, where it applies, at which level it should be assessed, who is responsible	**Balance RS considerations with institutional autonomy, avoid resource-intensive approaches**	**Limited institutional experience in RS, scarcity of expertise in RS**	**Lack of best practices, capacity gap, lack of tools to assess and manage RS risks**
POLICY RECOMMENDATION – HOW	**Establish a common understanding and promote RS as a shared responsibility** Use clear terminology Develop training material Identify stakeholders inclusively Continuous, versatile dialogue	**Leverage existing institutional resources** Utilise & adapt training programs on research ethics and integrity Embed RS into the research culture	**Cultivate professional expertise** Up-skill research ethics & integrity experts Re-skill research actors	**Support capacity building and the development of new approaches and tools** Explore innovative approaches (e.g. research security-by-design) Develop RS risk assessment & management tools Fund relevant research
WHEN	Short term	Short/medium term	Short term	Medium term
WHO	EU, HEIs, RPOs	HEIs, RPOs, funding organisations	EU	Funding organisations
TARGET	Cross-country and cross-sectoral cooperation	Institutional autonomy Awareness and training	Expert advice and guidance Informed choices	Capacity building Situational awareness Freedom of scientific research

RS: Research Security; EU: European Union; Higher Education Institutions (HEIs); Research Performing Organisations (RPOs)

WHY IS RESEARCH SECURITY IMPORTANT FOR POLICY?

International and open research has significant value in advancing and accelerating scientific knowledge, fostering global innovation and addressing global challenges. However, the landscape of international research is changing due to rising geopolitical tensions, foreign interference and the use of influential technological advancements for strategic, geopolitical, or economic objectives. In particular, the European Commission (EC) has identified Artificial Intelligence, Quantum technologies and Biotechnologies as 3 out of 4 critical technology areas with the highest likelihood of presenting the most sensitive and immediate risk related to technology security and leakage. Consequently, Higher Education Institutions (HEIs) and Research Performing Organisations (RPOs) -public or private- become prone to **Research Security (RS)** risks that threaten national security, the ethical conduct of research and fundamental human rights.

WHAT IS RESEARCH SECURITY?

> "Research security refers to anticipating and managing risks related to: (a) the undesirable transfer of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries; (b) malign influence on research where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union; (c) ethical or integrity violations, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties."
>
> *(Council Recommendation, 2024).*

In order to mitigate RS risks, HEIs and RPOs need to be supported by policies which are balanced with other considerations, such as competitiveness, open science, international collaboration, academic freedom and, institutional autonomy. Herein, the CHANGER project consortium focuses on specific RS challenges and presents targeted policy recommendations to address them, based on experience and practices from research ethics and integrity.

CHALLENGES RELATED TO RESEARCH SECURITY

1. Research security understanding varies between members of the research ecosystem

RS remains a relatively nascent concept, with varying interpretations and levels of understanding across members of the research and innovation ecosystem, including researchers, academics, industry actors, funding bodies, and policymakers. There is diverse understanding of the research areas, technologies, and products for which RS measures should be considered. Various terms related to RS have been used in guidance and regulatory documents by different countries and organisations, causing further ambiguity of what RS is. It is also unclear who should be held responsible to identify, mitigate, and manage associated risks and at which level (e.g. researchers, institutions, governments, funders). Furthermore, questions remain as to whether legal frameworks governing intellectual property, data protection, cybersecurity, dual-use technologies, and export control suffice to address the full spectrum of RS-related challenges. Even within the research ethics and integrity community, who are well-versed in principles of responsible conduct, there is considerable divergence in the understanding of RS, highlighting a critical gap in coherence and, therefore, the need for conceptual clarity.

2. Balancing institutional autonomy with research security considerations

Efforts to address and mitigate RS risks necessitate adaptations at the institutional level which may be resource-intensive and inadvertently impose significant administrative burden on researchers and their organisations. Such demands could be disproportionate to the scale or nature of the research conducted within HEIs and RPOs, potentially hindering international collaboration, institutional autonomy, and academic freedom. Thus, there is the need to provide HEIs and RPOs sufficient flexibility and autonomy to tailor their procedures to institutional contexts, leveraging existing infrastructures, rather than imposing uniform or horizontal RS requirements that may exacerbate compliance challenges.

3. Lack of research security expertise

Most HEIs and RPOs are currently in the early steps of engaging with the complex and evolving landscape of RS. As they begin to develop policies, frameworks, and institutional strategies to address RS considerations, these organisations face significant uncertainty. At present, there is limited institutional experience to draw upon, and a notable scarcity of expertise in RS capable of offering informed guidance and practical support. This lack of a well-established knowledge base and expert community hampers the ability of HEIs, RPOs, and individual researchers to proactively identify and manage potential risks.

4. Lack of capacities and tools

At present, there is a notable absence of established models or best practices to systematically and effectively integrate RS considerations into the research lifecycle. Researchers across disciplines lack the necessary competencies and institutional support to adequately identify, assess, and mitigate RS-related risks. This capacity gap is further intensified by the unavailability of practical, fit-for-purpose tools to assess and manage RS risks, limiting researchers and their institutions in navigating the complex RS challenges. The current situation underscores a critical need to actively involve researchers to take RS considerations in the research design with the support of context-specific tools.

POLICY IMPLICATIONS AND RECOMMENDATIONS

1. Establish a common understanding and shared responsibility

All members of the research ecosystem acting at diverse levels are required to have a common and clear understanding of what RS is, the risks involved and their implications. Even more so, the concept of RS is not static, and requires to be versatile enough to respond to the changing research environment, emerging technologies and increasing geopolitical tensions. Therefore, a common understanding of RS should be established through the: a) use of clear definitions and standardised terminology of RS in relevant documents, and b) development of training material to educate members of the research ecosystem providing clarifications on (mis)apprehended overlaps with other notions (e.g. dual use, misuse, intellectual property, data protection, and cybersecurity). Along with conceptual clarity, in order to align efforts to tackle RS across nations, institutions and, sectors, RS should be promoted as a shared responsibility by a) identifying relevant stakeholders in an inclusive manner (HEIs, RPOs, researchers from the public and private sector, national and European research funding agencies, policy makers at the national and European level, scientific associations and bodies, intergovernmental organisations) who share not only the same concerns but also the same interests to form alliances, and b) inviting all actors to a continuous and versatile dialogue, which will foster communication and support joint actions to effectively tackle the global challenges. Similarly to the ethical conduct of research which is a collective responsibility of all parties involved, RS risks cannot be addressed unless all members of the research and innovation ecosystem combine efforts.

The **EU** is invited to establish a common understanding of RS in the short term, by leveraging the ERA governance structures and the European Centre of Expertise on Research Security to be established at the Union level (Council Recommendation, 2024). HEIs and RPOs are also invited to establish a common understanding of RS and promote RS as a shared responsibility at the institutional level, through appropriate training programs at the institutional level (see also Policy Recommendation 2).

2. Foster institutional autonomy by leveraging existing resources

To avoid resource-intensive and excessive administrational burden, HEIs and RPOs should use procedures and practices already in place at the institutional level to tackle RS risks. As a first step, existing research ethics and research integrity training programs that cover aspects of dual use, misuse, and conflict of interest should be enriched with aspects of cybersecurity, intellectual property, but also keep researchers up to date with responsible internationalisation of research, foreign travel security, insider threat awareness and identification, and, due diligence. This will allow HEIs and RPOs to adopt context-specific training programs, which are tailored to their research activities, and embed RS considerations in the culture of ethical conduct of research and research integrity. Subsequently, HEIs and RPOs can gradually assess whether the establishment of new practices and/or structures, such as institutional RS Committees, are deemed necessary or not to tackle RS risks.

HEIs and RPOs are invited to adapt existing resources, such as training programs on ethics and integrity, in the short/medium term, to address RS. **National and European funding organisations** are also invitedto support such adaptations through appropriate funding.

3. Cultivate professional expertise

Developing a robust base of professional expertise in RS is critical to ensure that national authorities, HEI and RPOs have access to reliable, context-specific advice and guidance. The establishment of a dedicated cohort of RS experts will be instrumental in supporting the implementation of effective and proportionate RS mechanisms. Such expertise can be cultivated through targeted capacity building efforts which are essential to bridge current capacity gaps, and should include a) up-skilling of professionals currently working in adjacent domains such as research ethics, research integrity, (cyber)security, critical knowledge in emerging and disrupting areas, and legal compliance, and b) re-skilling of existing members of the research ecosystem, such as research managers and compliance officers.

The EU is invited to promote training of experts in the short term, through the European Centre of Expertise on Research Security to be established at the Union level (Council Recommendation, 2024), which is expected to contribute to the creation of an EU-wide community of practice. This community of practice could be further strengthened by the inclusion of expert RS advisors who have received appropriate training and have acquired the necessary competences to provide their insights and offer evidence-informed policies to countries, HEIs and RPOs.

4. Support capacity building

Research funding should be provided to explore innovative approaches that build capacities in researchers and their institutions to address RS challenges, as well as to develop risk assessment tools for RS. As an example, we propose the novel concept of “research security-by-design”, which is based on the principle of “ethics-by-design” as implemented in the CHANGER project. “Research security-by-design” is based on the idea that RS risks should be identified and mitigated already from the initial phase of the project design, in which researchers and RS experts are engaged in reflection and dialogue to effectively minimise RS threats in complex research projects. This approach contributes to the creation of situational awareness for researchers, to the empowerment of freedom in scientific research and informed choices to be implemented in the project design. Additionally, embedding RS considerations in research design strengthens research oversight and minimizes the necessity of developing new structures, such as institutional RS Committees.

Appropriate funding is necessary to explore “research security-by-design” or other innovative approaches, to develop RS risk assessment tools for researchers but also by HEIs and RPOs, as well as to develop benchmarking tools for HEIs and RPOs to assess their capacities for risk identification and management. European and national funding agencies are invited to embrace this critical Policy Recommendation, that will support research in RS and will provide novel tools to manage RS threats. Such initiatives can be covered by existing EU framework programmes and national funds.

WHY THESE POLICY RECOMMENDATIONS?

The proposed policy recommendations, which should be considered as complementary to existing guidance, can be implemented in short and medium term without the creation of new structures, such as new national or institutional RS Committees. The advantage of the proposed approach is multifold: a) It cultivates the integration of RS considerations in the existing research culture of ethical conduct of research and research integrity, fostering a seamless integration of common principles and values; b) It avoids the imposition of excessive procedural compliance, which could be perceived by researchers and their institutions as an administrative burden, risking detraction from understanding

the importance of safeguarding RS; c) It fosters shared responsibility, capacity building and proactive responsiveness to risks associated with international collaboration, while maintaining freedom of research; d) It facilitates context-specific adaptations at the research design phase, allowing institutions to implement measures proportionate to the specific risks associated with individual research projects, and thus foster institutional autonomy. Such an approach allows also to gradually raise awareness on the fact that in some cases, the research community may be required to cooperate with a specialized expert community, not directly linked to research, such as law enforcement, intelligence and security agencies.

FURTHER READING

1. Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States (2023). Available here
2. Council Recommendation on enhancing research security (2024). Available here
3. Tackling Foreign Interference - Staff Working Document. EC DGRI (2022). Available here
4. Taking European knowledge society seriously. EC DGRI (2007). Available here
5. Council of the European Union. Presidency note for the exchange of views on "Knowledge security and responsible internalization" (2023). Available here
6. Integrity and research in the global research ecosystem. OECD Science, Technology and Industry Policy Papers (2022). Available here
7. Guidelines for researchers on dual use and misuse of research. VLIR (2022). Available here

AUTHORS

Vasiliki Mollaki
(NCSRD) vmollaki@iit.demokritos.gr
Xenia Ziouvelou (NCSRD)
Konstantina Giouvanopoulou (NCSRD)
Vangelis Karkaletsis (NCSRD)

CONTRIBUTORS

Tina Garani (UNIWA)
Jeanne Mifsud Bonnici (RUG)

PROJECT IDENTITY

CHAllenges and innovative chaNGes in research Ethics Reviews (CHANGER) aims to promote changes in research ethics reviews by strengthening the capacities of researchers to incorporate ethical judgements in the project design and implementation, and by supporting capacity building of Research Ethics Committees (RECs) to address new challenges posed by new technologies, new players and new forms of research.

CONSORTIUM

Coordinator
National Centre for Scientific Research “Demokritos”, Athens, Greece

FUNDING SCHEME
European Union HORIZON-WIDERA-2023-ERA-01-12, GA No. 101131683

DURATION
3 years (January 2024 - December 2026)

BUDGET
€2,9M

www.changer-project.eu

Funded by the European Union under grant agreement No 101131683. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.