Guidelines

for Research Institutions

For the Integrity and Security of Research

August 2025

Summary

This document was developed and proposed by the Working Group on Research Security, established by the Ministry of University and Research. The group includes subject-matter experts as well as representatives of the Conference of Italian University Rectors (CRUI) and the Council of Presidents of Public Research Institutions (COPER). A presentation of the needs and general criteria outlined therein was delivered to the research and academic community during two technical workshops held in October, and at the National Public Conference held on 4 December in Bari.

Guidelines for research institutions

These Guidelines are formulated with the objective of providing universities and research institutions (as defined in the document "National Framework") with operational guidance to strengthen research security. They may be responsibly implemented to enhance awareness, improve the resilience of the research system, and support the development and implementation of effective safeguarding measures.

Awareness and Communication

Institution-Wide Dissemination of Communications - To disseminate timely and effective communications to research staff, technical and administrative personnel, as well as collaborators and students, with the aim of raising awareness and providing information on possible malicious interference by external actors. Such communications should include, for example: information on initiatives that researchers can undertake to mitigate potential risks; the requirements and responsibilities relating to reporting, disclosure, the control of knowledge and technology transfer, and other security checks provided for under Union or national legislation; and the designated contact points to whom assistance requests may be addressed.

Publication and Dissemination of Security Newsletters and Presentations - Regular publication and distribution of security-focused newsletters should be carried out, addressing topics such as, for example, foreign-origin risks and preparation for international travel. Institutions should also organize seminars and presentations on research integrity and security, tailored to specific audiences such as thesis students, PhD students, senior researchers, project leaders, academic leadership, etc.

Dedicated Web Pages on Institutional Websites - Institutions should develop and prominently display dedicated web pages on their official websites containing links and information covering a wide range of topics, including: international research commitments and global collaboration; undue influence and interference (for example -but not limited to- interference by foreign governments); and measures for mitigating related risks. The institutional website should also function as a 'single digital access point' for policies and practices related to research integrity and security. It should host institutional communications and informational materials, guidelines, and the requirements established by national authorities (e.g., Government, Ministries). A link to the website specifically developed by the Ministry -https://www.sicurezzaricerca.mur.gov.it- will also be included.

Fostering Dialogue within the Research Community - Encourage open discussion on research integrity and security during meetings of the institution's governing bodies and across the broader research community, including researchers and relevant technical and administrative staff. Regular meetings

should also be promoted at the level of internal structures -such as departments, institutes, and divisions- focusing on various aspects of research integrity and security.

Training - Organize training modules on key topics including: research integrity and security; conduct during international travel and stays abroad; appropriate protocols for hosting visitors on institutional premises; data protection and cybersecurity; activities subject to export control; and the protection of intellectual property.

To support this effort, the Ministry of universities and research has developed a series of training modules which will be made available on the dedicated website https://www.sicurezzaricerca.mur.gov.it, in the "Informazione/Formazione" section, following the completion of the pilot phase.

Responsibilities of Activity Leads

Project leaders involved in research projects, scientific and academic collaboration programmes, or commissioned/third-party research and innovation activities are invited, prior to the start of their activities, to familiarise themselves with the training module "Integrity and Security", will be made available in the "Informazione/Formazione" section of the website https://www.sicurezzaricerca.mur.gov.it. They are also encouraged to carry out a preliminary self-assessment of any potential risks associated with the planned activity, by accessing the designated area of https://www.sicurezzaricerca.mur.gov.it and completing the self-assessment form. The form will be made available at the conclusion of the pilot phase."

If the activity does not involve **external partners and/or external funding** (see definition on the "National Framework" paper), a simple declaration to that effect will suffice. Otherwise, the activity lead will carry out a risk analysis based on three potential categories of concern:

a) the scientific or technological domain in which the activity is situated;

b) the individuals and institutions involved in the collaboration;

c) the entities providing funding for the activity.

For each category, both theoretical and activity-specific risks will be considered. Upon completion of the form, the system will automatically calculate a **risk level** for each category. Based on these results, the lead will receive a report outlining the recommended mitigation measures, as well as, where appropriate, a suggestion to consult the institution's designated contact point for research security and integrity -where exixting- or the governing bodies of the institution for further guidance. If deemed necessary, and with the knowledge of the activity lead and authorization from the institution's legal representative or their delegate, the institutional contact may consult the national center for research security and integrity for additional guidance.

The activity lead may also choose to consult with their institutional contact before or during the completion of the self-assessment form, should they require preliminary input to better assess the risks associated with the activity. It is also the responsibility of the activity lead to update the self-assessment form whenever changes occur -such as modifications in collaborations or funding sources- or in the event of any other development that could alter the risk profile of the activity.

Data Protection and Cybersecurity

Cybersecurity Awareness in the Context of Scientific Research Activities – Researchers, students, and technical-administrative staff should be informed and trained on basic cybersecurity practices, data protection[1] measures, and the implications of cybersecurity for safeguarding research activities. Dedicated modules on these topics are available in the "Informazione/Formazione" section of the website https://www.sicurezzaricerca.mur.gov.it.

Risk Assessment and Management Measures – A risk assessment should be conducted to evaluate cybersecurity risks associated with scientific research activities, involving relevant stakeholders—including research staff and dedicated technical-administrative personnel (e.g., IT services). Institutions should develop a cybersecurity risk management framework tailored to research activities, which includes the identification of critical information assets, data protection strategies, access controls, network and information system security, and incident response procedures. Institutions are expected to collaborate with the National Cybersecurity Agency[2] (ACN) -with particular regard to compliance with the NIS-2 Directive- as well as with the Italian Data Protection Authority[3] (GPDP), the Agency for Digital Italy[4] (AGID), and other relevant national authorities.

Cybersecurity and Research Security – Institutions should implement cybersecurity measures for research activities and prevent internal breaches, adopting safeguards proportionate to the level of risk, the sensitivity of the specific activity, and other relevant contextual factors.

Ongoing Updates and Continuous Improvement – Regulatory developments should be closely monitored, and a culture of continuous updating should be promptly upheld — particularly with regard to Union and national regulations — through collaboration with the competent authorities and the National Centre for Research Security and Integrity.

---

[1] Since 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 -the General Data Protection Regulation (GDPR)- has been fully applicable across all EU Member States. The Regulation establishes a unified framework of measures and obligations to ensure that the circulation of personal data consistently upholds the fundamental rights and freedoms of individuals, thereby contributing to the trust-based environment essential for economic development. It should also be noted that the GDPR sets out specific legal conditions for the transfer of personal data to third countries outside the European Union, in order to guarantee an adequate level of protection for the data being transferred. In particular, where no adequacy decision has been adopted by the European Commission under Article 45 of the Regulation, such transfers are permitted only if the data controller or processor provides appropriate safeguards, including enforceable data subject rights and effective legal remedies, as specified in Articles 46 and 47 of the Regulation.

[2] https://www.acn.gov.it/portale/home

[3] https://www.garanteprivacy.it/

[4] https://www.agid.gov.it/it

Potential Dual-Use Items

Dual-use' goods and technologies—characterised by their potential use for both civilian and military applications—are regulated at both Union and national level.

Research activity, by its very nature innovative, is particularly exposed to the risk of misappropriation and/or unauthorised export of such goods and technologies. There is also the possibility that actors and organisations not aligned with the peaceful objectives of research may seek to obtain information, knowledge and scientific material.

To manage and mitigate risks associated with these vulnerabilities, Italy -like other European countries- has for years allocated dedicated resources through the National Authority UAMA[5] (Unit for Authorizations of Armament Materials) within the Ministry of Foreign Affairs and International Cooperation. These efforts support businesses and research institutions in assessing and managing such risks, in accordance with Regulation (EU) 2021/821[6], and in adopting Internal Compliance Programs for research involving dual-use items, as recommended in Recommendation (EU) 2021/1700[7], which was specifically developed to support research institutions.

For further information on how to manage the activities outlined in this section, please refer to the websites of the designated authorities and to the "Approfondimenti" section of https://www.sicurezzaricerca.mur.gov.it.

Collaborations, Grants, Contracts, and Donations

The self-assessment form and risk mitigation measures provided by the national center for research security and integrity should be used as tools for projects, collaborations, contracts, agreements, grants, and donations whenever external entities are involved (see definition provided on the "National Framework" paper). The analysis shall include the monitoring of any potential export of goods and technologies, the assessment of the terms and conditions for the allocation of funding, and the potential generation and external transmission of sensitive data or information related to critical technologies. In situations requiring additional screening, researchers may contact the institutional contact point for research security and integrity, who will, in turn, assess whether to consult with the National Centre for Research Security and Integrity.

Review, Update, and Enforcement of Conflict of Interest Policies

A Conflict of Interest (COI) refers to any circumstance in which an individual's personal, professional, financial, or other interests -including those of immediate family members- may actually or potentially diverge, or may reasonably be perceived as diverging, from their professional responsibilities to their home institution and the interests of that institution. A COI may exist whenever a reasonable independent observer could question whether the individual's professional

[5] https://www.esteri.it/it/ministero/struttura/uama/
[6] https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng
[7] https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng

actions or decisions -including ethical and objective conduct in studies, research, or clinical activities- are influenced by considerations of personal, financial, or other gain. COI situations may arise when a researcher holds scientific, financial, or educational interests involving entities external to their institution. This includes affiliations, relationships, and interests that may conflict with the researcher's obligations to their institution. Examples include participation in recruitment programs, the awarding of academic positions, collaborations (including unpaid roles), or serving as a *"principal investigator"* on projects in which the home institution is not involved.

Institutions that already have established codes of conduct on conflicts of interest are encouraged to assess their alignment with these guidelines. Institutions that have not yet adopted such policies are strongly encouraged to do so. To support researchers it is recommended that they consult the COI section available in the "Approfondimenti" section of the website https://www.sicurezzaricerca.mur.gov.it.

Security Measures for International Travel

Institutions should develop or update guidelines for international travel and establish a registry to track such trips. When necessary, tailored security briefings should be provided based on the destination or purpose of travel, particularly in cases where there are notable risk factors.
Institutions will refer to the training module "Basic Rules for Travel and Stays Abroad", which will be made available in the "Informazione/Formazione" section of the official government website https://www.sicurezzaricerca.mur.gov.it, and will ensure that researchers have reviewed the material prior to undertaking travel.

Visits by External Personnel to Research Institutions

Institutions should develop or update best practices or handbooks dedicated to visits by external personnel to research facilities. Access logs should be maintained to record key information such as the visitor(s), purpose of the visit, internal personnel involved, and the duration of the visit. Institutions will refer to the training module "Protocol for Managing Visits", which will be made available in the "Informazione/Formazione" section of the official government website https://www.sicurezzaricerca.mur.gov.it. Institutions shall ensure that staff responsible for hosting are made aware of the aforementioned module prior to the visit.