

Research Security in International Scientific Cooperation

June 2026

1. Preamble

Research security is indispensable in times of geopolitical upheaval, systemic rivalries, and the disruption of established partnerships — both to preserve the openness of the international science system and to safeguard scientific collaboration against a variety of risks. The aim of research security is to minimize undue interference in research and teaching, to prevent the unwanted outflow of knowledge and technology, to protect researchers, to shape international research collaboration in an ethical and resilient manner, and to preserve national security and competitiveness.

The goal of an open, integrity-based, and secure science system can only be achieved through the cooperation of all actors within their respective areas of responsibility and accountability. At the national level, Germany is establishing a National Platform for Research Security with the participation of the federal and Länder governments as well as the science organizations, which is tasked to support the scientific community in exercising its own responsibility. The decision on whether and how to engage in international collaborations, as well as the responsibility of reducing potential risks to the greatest possible extent, remains with the research institutions themselves. Research security is therefore a core responsibility of all institutes of the Leibniz Association and of individual researchers.

The following recommendations are addressed in particular to the scientific and administrative leadership of the institutes and are intended to provide orientation and support in developing and establishing solutions specific to the respective institute and discipline.

2. Principles

In view of the disciplinary and organizational diversity of its institutes, the Leibniz Association recommends that institutes, as a first step, consider the following three principles as guidance for implementing measures:

- 1) **Research security as a leadership responsibility:** As a strategic cross-cutting issue, research security falls under the direct responsibility of institute management. Which areas of research security (see Section 3) are relevant to a given institute, and which measures are to be prioritized, is therefore a management decision. This includes, among other things, determining whether the institute's research topics carry potential for misuse, identifying potentially critical research collaboration partners, and examining what measures may need to be taken.
- 2) **Research security as a lean process:** It is recommended to establish — based on management decisions — a transparent research security process with clear responsibilities and accountabilities, for example in the form of an Internal Compliance Program (ICP). This process should be kept lean and integrated into existing processes. As best practice, it is advisable to designate specific contact persons at

the institute for the topic of research security and to ensure their professional qualification. When setting up and further developing this process, it is useful to involve those departments and units responsible for key processes and fields of research security (HR, export control, the ethics in research committee, etc.).

- 3) **Research security as an ongoing responsibility:** Research security is not a one-off process but requires continuous attention and regular updating of knowledge. In order to keep pace with changing requirements, the active use of available advisory and training services is recommended. These include, in addition to the advisory services of authorities and subordinate bodies (such as the National Platform for Research Security), the services of other organizations (such as the DAAD Centre for International Scientific Cooperation (KIWi)). Leibniz Headquarters also offers, among other things, further training and information on the topic, and maintains the Leibniz Wiki on Research Security.

3. Areas of Research Security

Research security — sometimes also referred to as knowledge security, operational security or risk management — touches, as a cross-cutting issue, on overarching strategic policy, human resource management, information/cybersecurity, research ethics, and export control.

- **Strategic policy** encompasses the institution-specific, strategic framework for fulfilling the scientific mission and ensuring the institute's success. Institute management at the executive level should engage with fundamental questions of research security and incorporate these into strategic decisions on research and collaboration objectives.
- **Human resource management** ensures secure procedures for appropriate vetting as well as, where applicable, access regulations — in particular for applicants, visiting researchers and other external collaboration partners.
- **Information/cybersecurity** refers to the protection of information and IT systems — regardless of their form — against unauthorized access, misuse, loss or manipulation. The aim is to ensure confidentiality, integrity and availability through technical and organizational measures, and also to safeguard the protection of intellectual property.
- **Research ethics** addresses the reflection on responsibility in research. Thus, the potential for misuse of research results and possible risks for researchers and research supporting staff should thereby be identified. Upholding scientific integrity and good research practice is an inherent part of any ethically responsible science and requires due consideration — in a verifiable manner — not only in publications, but also in project proposals, throughout the research process and in knowledge and technology transfer.
- **Export control** regulates, as a clearly defined legal framework, the transfer of materials, technology, and knowledge. It thereby serves to prevent proliferation.

For the optimal protection of research and researchers, cooperation between these partially overlapping areas should be ensured within an integrated research security process. With regard to certain political risks (such as the threat of, or actual, criminal prosecution abroad),

coordination with the supervisory board is also advisable. Since risks can never be entirely eliminated, the aim is their systematic reduction.

Which areas take priority is determined primarily by the institute, the research topic, and the collaboration partner. Since the challenges may vary depending on the research discipline and collaboration partner, a case-by-case assessment adapted to the specific context is always necessary. All areas of research security can potentially become relevant for all institutions. Export control issues are not the exclusive concern of the natural, life, and engineering sciences, just as research ethics questions are not relevant only in the social sciences and humanities. Information security represents an increasingly important and permanent responsibility for all institutions, beyond the context of international collaborations. Particularly in the area of security-relevant civilian and non-civilian research, the heightened requirements in terms of research ethics — and often also regulatory requirements — must be observed.

4. Role of the Leibniz Association

The Leibniz Association offers a wide range of opportunities for collegial exchange, skills development, and support in the areas of research security and ethics as well as integrity. Within the various working groups (such as the Working Group on International Affairs or the Working Group on IT) and Leibniz Research Networks, individual areas of research security, or research security as an overarching topic, are already being addressed. The individual institutes can benefit from the association-wide structures and experiences.

Through the Leibniz Wiki on Research Security and the Leibniz Wiki on Information Security, Leibniz Headquarters provides practical guidance for extending and implementing the areas addressed here, particularly through checklists, guiding questions, best practices, and similar resources. Up-to-date references to further internal and external information and networking opportunities, as well as professional events hosted by Leibniz Headquarters, are also found there. The Leibniz Wiki on Research Security (in German) is available at: forschungssicherheit.leibniz.wiki. The Leibniz Wiki on Information Security (in German) is available at: informationssicherheit.leibniz.wiki. The Leibniz Commission for Research Ethics and the Executive Board Representative for Research Ethics serve as key contact persons on research ethics matters. Leibniz Headquarters also provides advice on establishing research ethics committees at Leibniz institutes and on identifying experts on specific topics.