METHODOLOGICAL RECOMMENDATION

FOR RISK MANAGEMENT IN RESEARCH SECURITY AT THE INSTITUTIONAL LEVEL

The presented set of documents for enhancing resilience against illegitimate interference in the higher education and research environment has been developed, in response to the requests of Czech higher education and research institutions and in an effort to prevent a fragmented approach by these institutions to the issue of illegitimate interference, within the framework of the Interdepartmental Working Group for Combating Illegitimate Interference in the Higher Education and Research Environment, with significant contributions from the Ministry of Education, Youth, and Sports, the Ministry of the Interior, and the Czech Academy of Sciences, and in consultation with representatives of other Czech higher education and research institutions.

TERMINOLOGY

For the purposes of this methodology and related materials (i.e. *Methodological recommendation defining the minimum scope of due diligence and risk management in cooperation with third parties within the context of strengthening the resilience of the higher education and research environment against illegitimate interference*; *Strengthening resilience against illegitimate interference in the higher education and research environment*), the following terms are defined as follows:

Academic Institution

A term used as an alternative for higher education and research institutions, either collectively or individually, depending on the context.

Security Research

Refers to research, development, and innovation activities aimed at identifying, preventing, preparing for, and protecting against illegal actions or actions that intentionally harm (European) communities, individuals, organisations, or structures, including tangible and intangible assets and infrastructure, ensuring operational continuity after such actions, and mitigating their consequences (also applicable in the case of natural disasters and industrial accidents).

Research Security

Organisational and systemic procedures for evaluating and managing security risks in the area of research and education, which reduce the risks associated with illegitimate interference in the higher education and research environment.

The primary goal of research security is the comprehensive protection of the research ecosystem, which also encompasses the protection of national and economic interests.

Sensitive Data/Information

Refers to data and information that an academic institution protects as part of sensitive research and education or considers confidential by its own decision, or that must be protected based on regulatory requirements.

Sensitive Areas of Research and Education

Refers to areas of research and education that carry an increased risk of illegitimate interference and for which enhanced protection is sought, including:

- Critical technologies for the economic security of the EU,
- Selected fields of research and education,
- Selected cooperation with third parties,
- Dual-use goods and technologies, and military material,
- Any other area that an academic institution chooses to classify as sensitive.

Foreign Power

Refers to a foreign state or its authority, or a supranational or international organisation or its authority, as well as any other individuals or legal entities, regardless of nationality or location, involved, even partially, in advancing the interests of a foreign state or organisation through illegitimate interference.

Due Diligence

Refers to a set of measures aimed at eliminating or reducing the risks of illegitimate interference on academic institutions arising from cooperation with third parties.

Identification Data

1. For individuals: name, surname, date of birth, and nationality.
2. For legal persons: name and registered office.
3. In other cases: a designation or name, and any other necessary information to identify the partner unequivocally.

Critical Technologies for the Economic Security of the EU

Refers to a list of technological areas defined in the European Commission's Recommendation of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States[1] and its Annex[2].

1 COMMISSION RECOMMENDATION of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States; C(2023) 6689 final

2 ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 final

Illegitimate Interference

Refers to unwanted interference on people, decisions, or processes. This includes foreign malign influence as well as criminal (e.g., corrupt) behaviour and undesirable lobbying. These are usually activities that are covert, deceptive, coercive or corrupt and which the perpetrator of illegitimate interference (foreign power, corruption, lobbying in violation of the law or generally accepted social ethical rules) carries out himself or through a third party and which threaten or damage the interests of higher education and research institutions.
Alternatively, the term foreign interference is also used.

Partner

Refers to any legal or natural person with whom higher education and research institutions are in, or intend to establish, a partnership.

Partnership

A relationship or collaboration established by a cooperation agreement or other written agreement (e.g., memorandum of understanding, distribution of responsibilities in research teams) between an academic institution and a third party. In some cases, it may involve a less formal or even informal contractual relationship (including implied contracts) between an academic institution's employee and a third party.

Employee of a Higher Education or Research Institution/Academic Institution

Refers to a student, intern, academic or research worker, other employees, or individuals in another contractual relationship with the academic institution, as well as others involved in the institution's activities.

Perpetrator of Illegitimate Interference

This term refers to any individual, regardless of whether they act independently or on behalf of a state, company, or organisation, and regardless of the forms and methods of illegitimate interference they employ. The term "attacker" is also sometimes used. They typically pursue their interests in violation of democratic principles, the legal order, and good morals. They seek the easiest possible way to advance their interests, with the vast majority of such activities targeting a specific individual (in this context, a member of the academic community or an employee of the academic institution).

Regional Studies

This refers to academic disciplines focused on the study of local and regional contexts of societal and environmental development, i.e. the context and realities of a given region.

Third Party

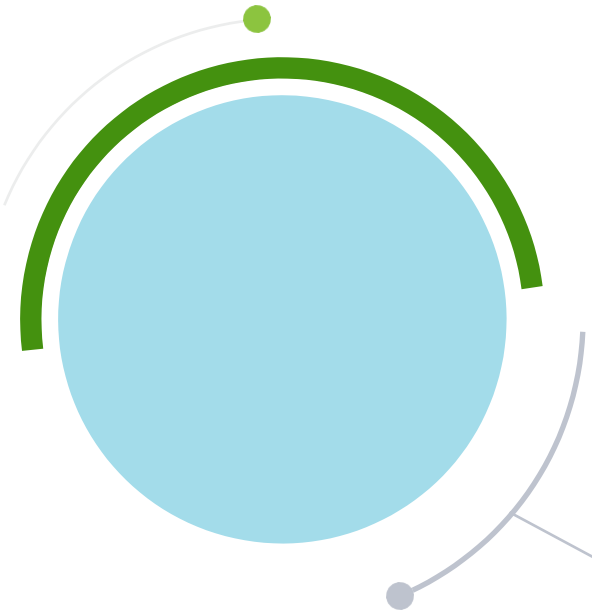
This refers to any legal or natural person, public authority, or other entity representing or acting on behalf of a state that is not a member of the European Union (EU)[3], the European Economic Area (EEA)[4], or the European Free Trade Association (EFTA)[5].

Third Country

This refers to a country other than the Czech Republic. The term "third state" is also used alternatively.

R&D&I or RDI

The acronym R&D&I refers to Research, Development, and Innovation.
Other terms used are interpreted in accordance with the European Commission's Communication on the Framework for State Aid for Research, Development, and Innovation (2022/C 414/01).



3 https://european-union.europa.eu/easy-read_cs

4 https://www.europarl.europa.eu/factsheets/cs/sheet/169/the-european-economic-area-eea-switzerland-and-the-north; Norway, Iceland and Liechtenstein

5 https://eur-lex.europa.eu/CS/legal-content/glossary/european-free-trade-association-efta.html; Iceland, Liechtenstein, Norway and Switzerland

INTRODUCTION

This document serves as a methodological guide for risk management in relation to research security within academic institutions in the Czech Republic and is intended as an implementation document to accompany the general methodology for **Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment**.

The purpose of this document is to provide guidance to the leadership of academic institutions and to professionals in the field of research security on how to implement measures to enhance institutional resilience and to introduce specific tools for risk management in protection against threats of illegitimate interference on academic freedoms and the disruption of institutional autonomy. The goal of these measures and tools is to prevent and counter such threats, thereby ensuring the credibility of research conducted within higher education and research institutions.

The terms used in this material have the meanings provided in the glossary of terms in the general methodology for Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment.

This material draws upon policies and documents issued by the EU concerning illegitimate interference, as referenced further in this text, and on ISO standards issued for information and cybersecurity agendas by the International Organization for Standardization (**ISO – About ISO**) and the Czech Standardization Agency (**Czech Standardization Agency (agentura-cas.cz**), particularly the ISO/IEC 27000 series for Information Security Management Systems (ISMS), specifically including standards ČSN EN ISO/IEC 27001 and 27002.

I. INSTITUTIONAL RESILIENCE

EU POLICY AND NATIONAL INITIATIVES

The development of EU policy and the approach of the Czech government to the issue of institutional resilience in higher education and research institutions, as well as to research security, is described in the general methodology for **Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment**. This methodology highlights that the preparation of the **European Research Area Policy Agenda for 2025–2027**, along with discussions on the upcoming EU Framework Programme for Research and Innovation, places clear emphasis on **strengthening research security**. The EU repeatedly affirms the critical importance of research, development, and innovation for sustainable development, prosperity, competitiveness, and the economic and social status of Europe, while also promoting openness in international research collaboration. However, it also expects equal conditions and reciprocity from partner states and institutions, based on fundamental academic values and respect for intellectual property. In light of the current global political developments, the EU underscores the need for so-called "**balanced openness**". This term refers to the balance between fostering open collaboration with international partners and enhancing research security.

The European Commission calls for the mobilisation of science to better protect its interests, values, and expertise under the principle "**as open as possible, as closed as necessary**", and along with this, encourages academic institutions to invest in specialised expertise in research security.

Based on current experiences, it is now evident that researchers can become tools through which autocratic and illiberal governments illegitimately acquire cutting-edge knowledge and technologies, often using unscrupulous practices and methods, frequently under the guise of seemingly trustworthy international academic collaboration.

According to the **Proposal for a Council Recommendation on enhancing research security,** malign or illegitimate interference in the field of research, development, and innovation (RDI) is particularly understood to include:

- Undesirable transfer of critical knowledge, know-how and technology that may affect the security of the EU and its Member States, for instance if channelled to military purposes in third countries.
- Misuse of research activities to spread disinformation, influenced by third countries or parties.
- Incitement of self-censorship among students and researchers, leading to the undermining of institutional autonomy.
- Violations of scientific ethics or research integrity, resulting in the misuse of knowledge and technologies to suppress or undermine fundamental democratic values.

RESPONSIBILITY OF ACADEMIC INSTITUTIONS

The proposed new Act on Research, Development, Innovation, and Knowledge Transfer from November 2023 anticipates, in connection with RDI funding, the introduction of the concept of "institutional resilience" and, alongside it, the obligation of "precautionary principle or precautionary approach". These are duties aimed at ensuring research security and protection against illegitimate interference, with such obligations to be established both on the side of funding providers and recipients.

The term "**institutional resilience**" is not currently defined in a binding manner. It should be understood as the ability of an academic institution to establish and implement a system of measures to strengthen research security against illegitimate interference and to protect the reputation of higher education and research institutions. This involves, in particular, ensuring safe international research and academic collaboration, including compliance with binding sanctions, management of intellectual property, and risk management, especially in areas of research with significant transformative potential in knowledge and technologies, in areas related to dual-use technologies and military materials, as well as in research where there is a risk of misuse of knowledge or technologies to violate human rights and freedoms.

In line with institutional autonomy and academic freedom, academic institutions are regarded by both the EU and the Czech government as **primarily responsible** for their international collaborations and for implementing measures to ensure institutional resilience. A significant portion of the work in strengthening the resilience of research and higher education institutions will therefore involve changing the approach of individual departments and their staff towards the openness of academic collaboration, particularly in the preparation and execution of research. Here, it will be essential to find a new balance between openness and research security, with a focus on protecting intellectual property.

II. SECURING RESEARCH

PROTECTION OF RDI OUTPUTS vs. OPEN SCIENCE?

The Council's Recommendation on enhancing research security emphasises the condition of **"openness as needed"** and calls for a balance between open access in science and education on the one hand, and the protection of intellectual property on the other. The openness of the academic environment should therefore be increasingly considered from the perspective of research security at all stages of research collaboration. Even during the preparation and implementation of a research project, the protection of sensitive research data and information should be ensured, and effective security measures should be implemented to protect against unwanted interference on research and the illegitimate use of its results.

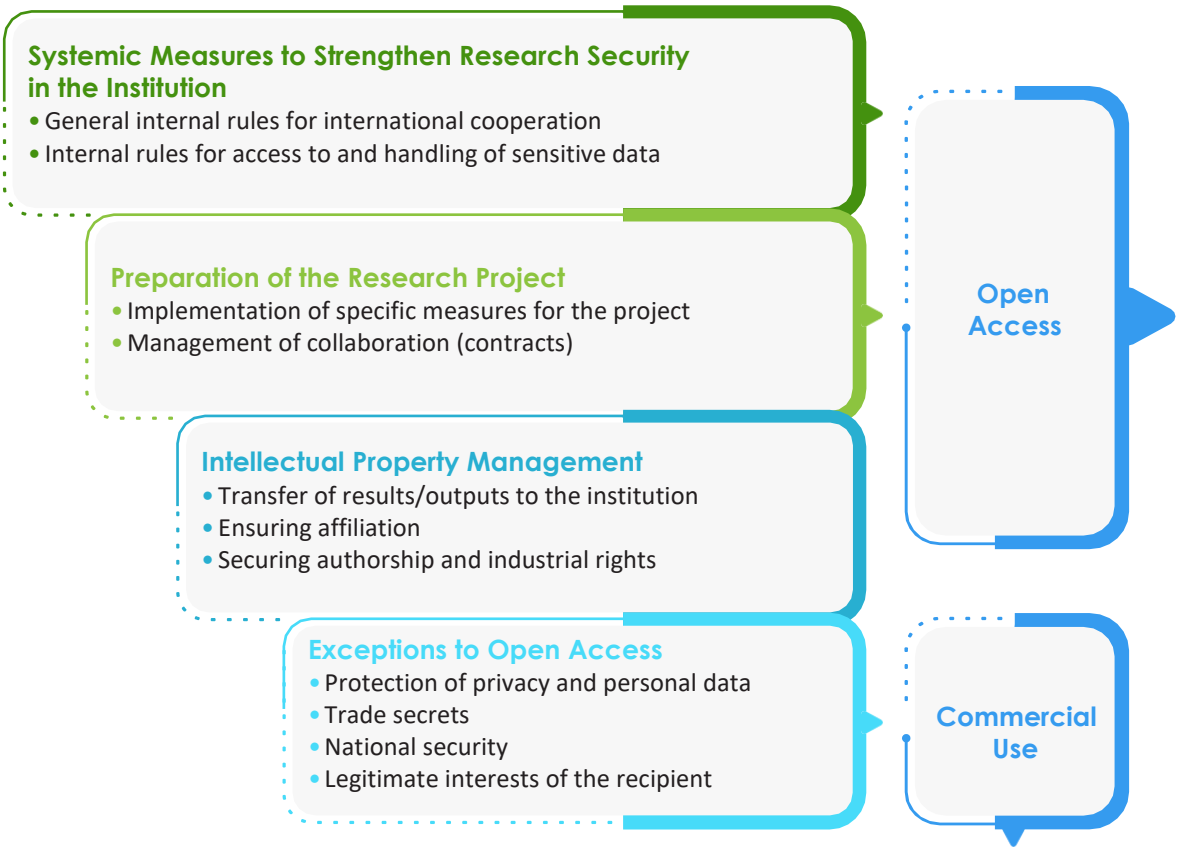
Such a requirement **is certainly not in conflict with the EU's interests in Open Science**, which aims at the reproducibility of scientific findings and open access to publications, data, and software for their unrestricted use. The requirement for Open Access to research data is realised only after the results of a research project have been achieved and when the management of intellectual property should already be in place, as well as the application of exceptions to open access for reasons of privacy, civil security, or military or commercial reasons.

The principle of open access to information about research data and to research data, as per Directive (EU) 2019/1024 of the European Parliament and of the Council on open data and the reuse of public sector information, has been reflected in Czech legislation under Sections 12 and 12a of Act No 130/2002 Coll., on Support for Research, Experimental Development, and Innovation, as amended by Act No 241/2022 Coll., effective from 1 September 2022. This national legislation also establishes the possibility of refusing to provide research outputs/results in cases where such provision would disproportionately infringe on the right to privacy and personal data protection, the right to protect trade secrets, national security, or other legitimate interests of the recipient. Recipients may also refuse to provide research data if the research or development was not fully funded by public funds. Additionally, a one-year timeframe after the conclusion of grant support has been introduced, during which it is not necessary to publish research data, in order to allow for the commercialisation of scientific results.

According to the **Guidelines on Open Access Rules for the Horizon Europe programme**, the decision on whether to publish through open access should come only after a broader assessment and determination of whether to publish directly or to first seek legal protection for the project's results.

A general interpretation of Open Science in the context of illegitimate interference in higher education and research environments is available in the general methodology for Strengthening Resilience Against Illegitimate Interference in the Higher Education and Research Environment.

The procedure related to the implementation of protective measures for research data during the preparation and execution of projects and their accessibility can be schematically expressed as follows:



OBJECTIVE

The organisational and systemic procedures for evaluating and managing risks in international cooperation in the form of illegitimate interference aim to achieve a status of **trustworthy research**. In general, this refers to research where the openness of the academic environment and research security are balanced because the academic institution:

- **Has a system in place to protect against threats to intellectual property and sensitive research, against interference in decision-making processes, and against damage to the reputation of the institution and its staff.**
- **Protects sensitive data and information (about research, its staff, and the organisation) and is able to ensure the confidentiality, integrity, and availability of RDI information.**
- **Facilitates the best possible use of international cooperation while protecting intellectual property, sensitive research, and personal data.**
- **Is aware of potential risks in academic cooperation in the current global context.**
- **Makes informed decisions.**
- **Protects its institution and staff from misuse/abuse.**
- **Finally, it promotes integration and international cooperation in R&D by providing assurance to partners that risks are appropriately managed.**

AREAS OF MEASURES

Specific measures to protect against illegitimate interference, which academic institutions should consider adopting, can be divided into the following categories; a more detailed explanation of these measures is provided in **Part III of this document**:

- **Protection Against Illegitimate Interference in the Activities of Higher Education and Research Institutions**

  This includes classifying sensitive research areas and sensitive data and information according to the specific activities of the institution, ongoing projects, and current international collaborations within the institution. It is recommended to have a prior thorough description of internal processes and the flow of data and information within the institution. Institutions should analyse the security risks of international cooperation in accordance with the **Methodological Recommendation for Cooperation with Third Parties**. The institution should also assess the need to audit existing scientific and partnership collaborations to identify risks of illegitimate interference and take measures to mitigate these risks.

- **Implementation of a Rigorous Intellectual Property Protection System**

  The institution must evaluate whether the research outputs/results have or could have commercial value, and if so, ensure that such outputs/results are protected. Current legislation requires that rights to project outputs/results are primarily transferred from researchers (and other parties who contributed to the results/outputs) to the institution where these individuals are employed. The institution must consider whether the results/outputs can be practically utilised. If the commercial or other utilisation of a given result/output is not anticipated or cannot be realised within a reasonable timeframe, the result/output along with the associated data should be published (even with a delay), allowing for Open Access.

- **Ensuring Information and Cybersecurity**

  Institutions should adopt effective measures to ensure their information and cybersecurity to safeguard the confidentiality, availability, and integrity of data and information, whether in oral, printed, or electronic form.

Institutions should establish a system of authorisations and access to resources so that their data is protected while also being shareable where appropriate or required, and at the same time, maintaining their validity and current relevance.

- **Compliance with Binding Regulations and Rules**

  Institutions must take necessary measures to ensure compliance with generally binding regulations, including mandatory rules for protection against security threats and risks. In addition to standard procedures for public procurement and GDPR, which also include whistleblower protection, it is essential, depending on the institution's primary activities and current projects, to assess restrictions due to international sanctions, control regimes, and obligations to screen foreign investments.

III. MEASURES AT THE LEVEL OF ACADEMIC INSTITUTIONS

STEPS FOR ACADEMIC INSTITUTIONS

The task for academic institutions will be to implement the agenda of institutional resilience according to their specific needs at their respective departments, and to **tailor individual measures to their field of activity and the specific needs of ongoing research projects**. The internal processes and mechanisms that support the resilience of the institution should include:

- Systematic integration of the agenda related to strengthening resilience and protection against illegitimate interference.
- Establishment of competencies, securing resources and support.
- Methodologies for various activities within the institutional resilience agenda.
- Communication, educational, and awareness-raising activities.

An effective tool for assessing the need to implement measures to protect research security at individual departments will be the **internal risk management procedures**. Given the common fundamental mission of higher education institutions and the similar primary activities of research institutions, at least within scientific fields, such internal procedures at individual departments will be largely similar. They will include general guidelines for risk identification, rules for evaluating potential partners, and procedures for decision-making regarding international cooperation with increased risks, among others.

Therefore, academic institutions should simultaneously create a space for building a community at both national and international levels to address security issues in educational and research activities and to share experiences and exchange information with one another. **This is especially important for pooling resources and expertise**. Leadership should support meetings at the level of founders, providers, national authorities, and the EU for the purpose of exchanging and improving knowledge of best practices in institutional resilience, new technologies and services, as well as threats or vulnerabilities of academic workplaces. It will also be beneficial to establish and maintain contact with relevant authorities for addressing specific security incidents.

The implementation of institutional resilience measures at specific workplaces will not be possible without the support of the highest leadership of academic institutions and the acceptance of responsibility for this agenda by staff at all managerial levels.

It will also be crucial that the **measures adopted are proportionate**, with full respect for the principle of "reduce risks, not separate", and that the solutions implemented impose **minimal administrative, organisational, and financial burdens on the institutions**.

RISK MANAGEMENT

The following text is **intended primarily for professionals** who will be responsible for the agenda of research security risk management at academic institutions. The scope and nature of the recommendations provided below do not offer a comprehensive and detailed description of individual procedures and guidelines but can provide an overview of effective risk management tools, the impact of these issues on other agendas, their interconnection, and serve as a basis for creating more in-depth and cohesive implementation materials tailored to the needs of the given institution.

According to the **Proposal for a Council Recommendation on enhancing research security,** the goal of these measures is to ensure the economic security and resilience of the EU. In this context, risk management should focus primarily on measures against:

- The undesirable transfer of critical knowledge, know-how, and technologies that could be used, for example, for military or intelligence purposes in third countries.
- Malign influence on research through the manipulation of students and staff, aimed at spreading disinformation or achieving self-censorship in favour of illegitimate interests of third parties within the academic institution.
- Violations of research ethics or integrity, where knowledge and technologies are used to suppress academic freedom and fundamental democratic values.

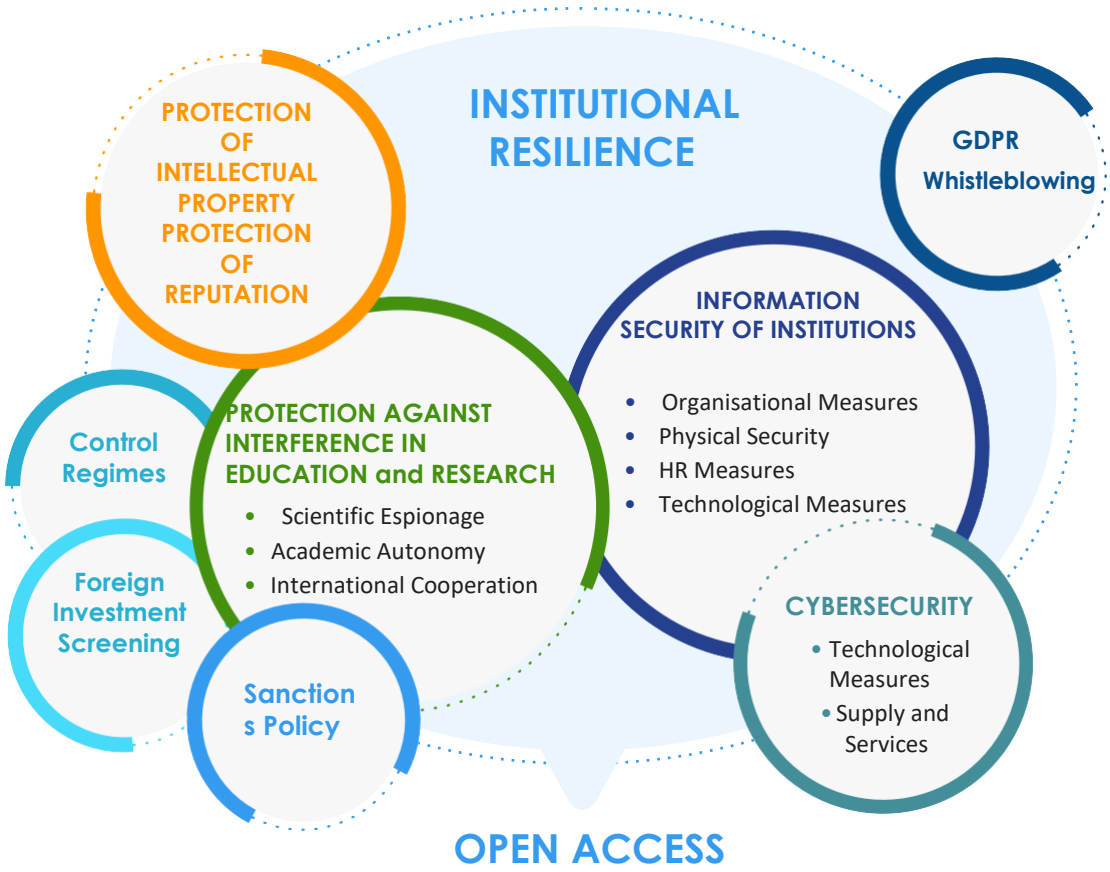
To establish risk management procedures related to research security, it will be useful to draw on **international standards** used in organisations, regardless of their legal form and subject of activity, for ensuring information protection, such as ČSN EN ISO/IEC 27001 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" and ČSN EN ISO/IEC 27001 27002 "Information security, cybersecurity and privacy protection — Information security controls".

These standards are part of the so-called "information security", within which organisations address the protection of sensitive data and information either based on their autonomous decision (considering the information significant and confidential) or as required by state regulatory demands (e.g., personal data). **Information security protection measures** are typically divided as follows:

- Organisational measures = measures at the level of internal regulations and guidelines.
- Human resources measures = measures at the HR level.
- Physical security measures = measures at the level of physical security of premises, equipment, and physical access to them.
- Technological measures = measures at the level of hardware and software and cyberspace.

The need for individual measures in a specific academic institution should be assessed concerning its primary and secondary activities and current research projects based on an internal evaluation of the need to address specific reputational and financial risks or increased risks of influencing internal self-governing processes. Decisions on the adoption of security measures will be entirely within the competence of the academic institution and should always be implemented thoroughly, purposefully, and **proportionately to the identified and assessed risks and their impacts**.

Institutional resilience measures in academic institutions and the establishment of a risk management system to enhance research security will have implications for the competencies of various departments within the institution. **The intersection of individual agendas** related to ensuring trusted research can be schematically demonstrated as follows:



IV. EXAMPLES OF MEASURES TO STRENGTHEN RESEARCH

ORGANISATIONAL MEASURES

Organisational measures will primarily involve the development of internal guidelines and regulations.

Internal directives should address the following:

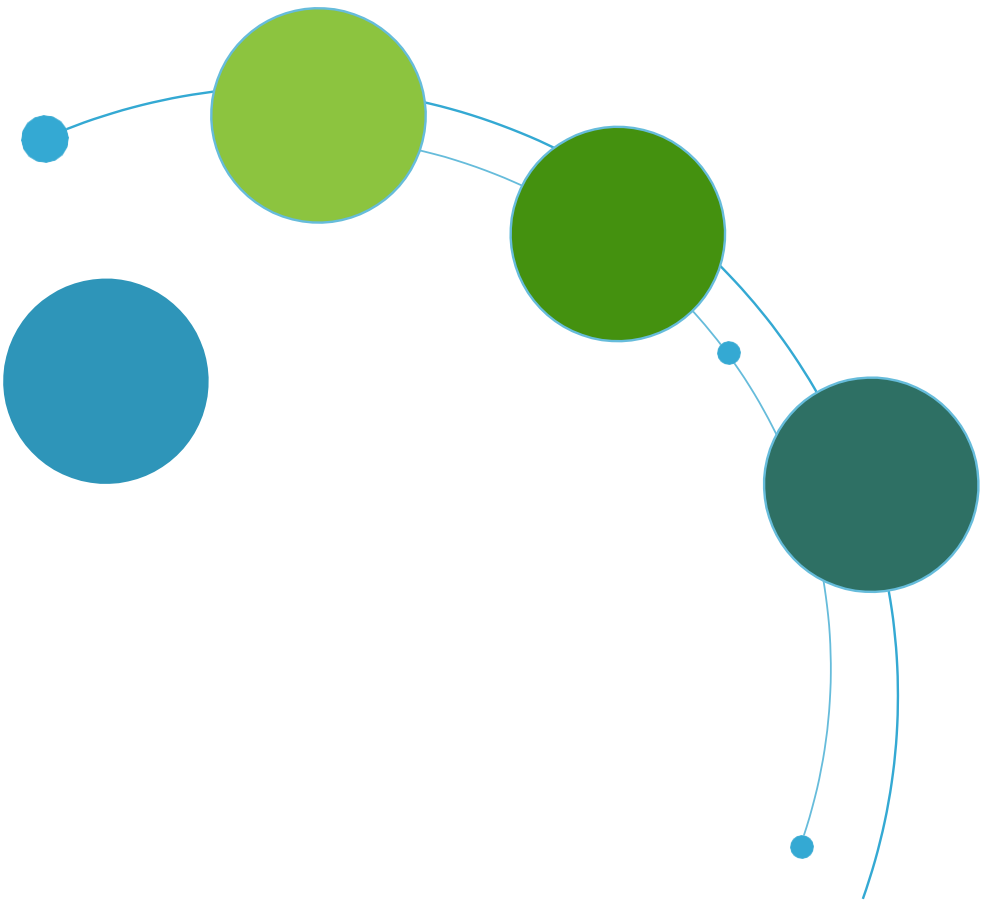
- **Establishment of basic policies and goals of the** security agenda within the institution, securing human and financial resources, and setting competencies, which will be the responsibility of the top management of the institutions – this will involve a declaratory document from the highest management expressing a commitment to implementing and improving protective measures to enhance research security within the institution.
- **Identification of the institution's own needs and risks**, which will primarily involve the following:
  - Conducting thorough classification of sensitive data, information, and outputs, i.e. such data that the academic institution protects as knowledge in sensitive areas of research and education, either from its own decision or based on state regulatory requirements.
  - Identifying sensitive areas of research and education in line with the **Methodological Recommendation for Cooperation with Third Parties**, i.e. assessing the increased risk when conducting research in projects related to:
    - Critical technologies significant for the economic security of the EU.

  - Controlled dual-use items as defined by European and national legislation, i.e. goods, software, and technologies that can be used for both civilian and military purposes.
  - Civil security research, regional studies, and applied research.
  - Collaboration with third parties from high-risk countries.
  - Other areas as determined by the academic institution.
- Identifying activities within the institution that involve handling sensitive data/information and/or relate to sensitive research and educational areas, including high-risk international collaborations at the given workplace.
- Describing the flow of sensitive data and information within workplaces, laboratories, and systems of the institution.
- Monitoring regulatory constraints arising from international sanctions and obligations concerning the review of incoming foreign investments, such as when a foreign investor enters a spin-off, or legal regulations concerning protection against security threats and risks.

- **Managing International Cooperation:** This will involve:
  - Setting internal rules for assessing the risk of international collaboration from the perspective of illegitimate interference, based on evaluating the combination of key risk factors, including:
    - The specific area of research and innovation in which the international collaboration is to take place.
    - The risk profile of the specific partner – whether the organisation is based within or outside the EU.
    - The risk profile of the country where the partner is headquartered or from which it is controlled or owned. Further recommendations for tools to assess the risk of specific international collaboration projects are elaborated in the **Methodological Recommendation for Cooperation with Third Parties**.
  - Transferring decision-making on high-risk collaboration to a higher level.
  - Assessing the need for and conducting audits of existing international collaborations within specific projects, particularly if they are carried out in sensitive areas of research and education.
  - Evaluating risks associated with illegitimate interference on projects for early-career university and research staff, particularly during foreign internships.
- **Risk Mitigation:** This will involve setting up measures to enhance research security, particularly in sensitive areas of research and education, by:
  - Establishing a system of authorisations and access to individual sensitive data and information based on their nature, location, and level of risk, considering the principle of "need to know" to ensure confidentiality, availability, and integrity of such data.
  - Establishing or revising internal rules for conducting international collaboration, both in relation to the institution’s activities and individual researchers.

- Adopting rules to **limit or prohibit so-called technical assistance and intangible transfer of technology** in the area of controlled dual-use items. According to European legislation, technical assistance may include the provision of higher education and conducting applied research.
- Developing or revising internal regulations to **ensure the management and protection of the institution's intellectual property**; this includes addressing copyright issues, transferring proprietary rights to the academic institution, securing licensing agreements before publication, and protecting patents and other industrial property rights.
- Adopting rules for **entering into memoranda and contracts for conducting international research and academic collaboration** with countries or institutions with heightened security risks, including:
  - Creating framework documents to ensure balanced and reciprocal cooperation, such as mutual data sharing and utilisation.
  - Binding agreements in collaboration contracts—particularly regarding the use of the results of the cooperation, addressing authorship and proprietary rights, securing financial contractual obligations, and setting conditions for terminating the collaboration.
- **Addressing information security in relationships with suppliers of** equipment, resources, and services related to research activities, as well as goods and services for the operational needs of academic institutions.
- Managing Reputational Risks (both to the institution and its workers): This involves:
  - Assessing the risk of damage to the institution's reputation, teams, and staff due to research and diplomatic collaboration with countries with heightened security risks and setting rules for managing such collaborations or transferring decision-making on such collaborations to a higher level.
  - Assessing the risk of damage to the institution's reputation, teams, and staff due to scientific and non-scientific collaboration with the private sector, such as in the establishment of spin-offs, transfer of intangible assets, involvement in or participation in legal entities, including associations, and setting rules for managing such collaborations or transferring decision-making on such collaborations to a higher level.
  - Managing the provision of sponsorships for scientific and social projects, conferences, and other events, including renting institutional spaces.
- Setting rules for **organising scientific conferences, educational events, diplomatic and social meetings**, and visits where the participation of unaccredited public or the presence of individuals from countries with heightened security risks is expected, or where discussions involve sensitive areas of research and education. This should align, e.g., with the rules outlined in the **Methodological Recommendation for Cooperation with Third Parties**.
- **Compliance with Legal Obligations:** Ensuring compliance with procedures stipulated by mandatory legal regulations concerning public procurement, GDPR, whistleblower protection, and depending on the institution's main activities and current projects, also considering international sanctions, control regimes, foreign investment screening, and other mandatory rules for protection against security threats and risks.

- Incident Management Procedures: **Establishing procedures for resolving specific security incidents**, particularly for reporting observed or suspected events, implementing corrective measures necessary to eliminate causes, and setting up a system for evaluating the effectiveness of security measures and implementing their changes.
- **Management of Documented Data and Information**: This involves a system for creating and updating documents (identification, format, and medium of the document), ensuring their storage, accessibility for authorised access, and disposal.
- **Internal Communication**: Implementing appropriate internal communication to support the institutional resilience agenda and establishing protective measures concerning **media communication**, particularly focusing on access to sensitive data and decision-making regarding its use.



HUMAN RESOURCES MEASURES

Human resources measures will primarily involve HR personnel, but their implementation will impact all levels of management, as security considerations should be integrated into management activities at all levels.

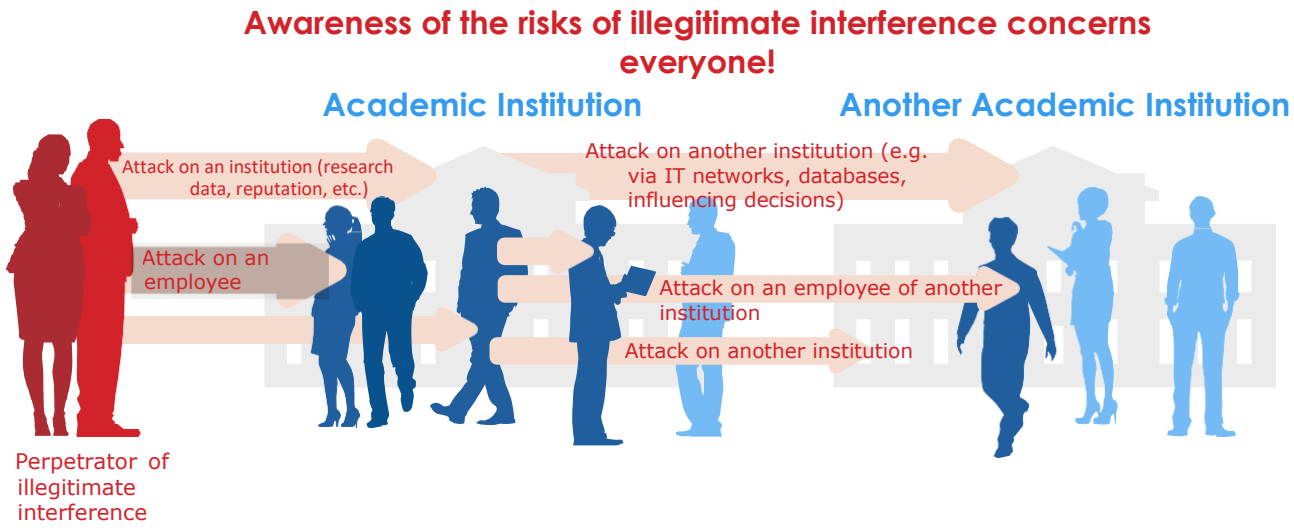
The measures will include:

- Evaluation during Recruitment, Changes, and Termination: **When recruiting new employees or collaborators, as well as during changes and terminations of employment**, the resilience of the institution should be considered. These procedures should be reflected in internal HR policies.
- Incorporating Responsibility for Information Security into **Employment Contracts**: This includes the use of confidentiality agreements to ensure employees are aware of their responsibilities regarding information security.
- Security Measures for Remote Work: Implementing security measures to protect information during the processing and storage of data when **working remotely**.
- Regulating Employee Conduct in Public Spaces, Including Cyberspace: Evaluating the need and possibilities for legally regulating employees' actions **in public spaces (including cyberspace)**, such as the disclosure of work-related information on social media or activities in online posts. The use of confidentiality clauses is recommended.
- Setting Rules for Foreign **Travel to High-Risk Destinations**: Establishing guidelines for employee travel to high-risk destinations in accordance with the **Methodological Recommendation for Cooperation with Third Parties**.

- Incorporating Research Protection Requirements into **Ethical Codes**: Integrating requirements for protecting research from security threats into the ethical codes of academic institutions. This should especially concern the respect for fundamental human rights, the protection of impartiality and independence from ideological and political pressures or interests, and the support of trusted research.
- **Developing Training Programmes: Creating training programmes for** security managers, HR personnel, and other relevant staff. This should include education on institutional resilience for new employees, tailored to their specific roles and responsibilities.

- Raising Awareness: Enhancing awareness of research security and the impact of illegitimate interference on the institution's reputation and that of its research staff. This aims to foster an understanding of the **personal responsibility each member of the academic institution holds**, considering that:
  - **Every person has access to sensitive information** that could be a target of illegitimate interest from third parties, as information that might seem insignificant to one person could be of great value to another.
  - **Every person can become a subject of interest** (illegitimate interference), and the decision by a third party to target a specific employee is beyond the control of the individual.
  - **Every person can defend themselves**, as tools are available to recognise illegitimate interference, understand how to respond, and know whom to contact for support.

Consequences of Poor Decision-Making: Employees must understand that poor decisions can not only damage their own reputation but also harm the good name of their home institution or other academic institutions and/or individuals.



PHYSICAL SECURITY MEASURES

Measures in the area of physical security will involve actions that may already be in place within the framework of building management and fire safety, but these will need to be reassessed from the perspective of institutional resilience, particularly to ensure the protection of sensitive data and information.

In the context of physical security, examples of measures include:

- Implementing controls for **physical access to secured areas** (departments, laboratories, etc.) and for work conducted within these areas.
- Establishing access controls to equipment and facilities used in sensitive areas of research and education.
- Ensuring the **physical security of offices and equipment**, including protection against physical threats to infrastructure.
- Implementing measures to **protect soft targets**, including the use of technological solutions for **warning and information** dissemination systems.
- Setting rules for **handling information carriers**.
- Protecting institutional equipment outside of the workplace according to rules for the use and storage of entrusted property.
- Implementing additional measures based on recommendations from experts on building soft target protection.

TECHNOLOGICAL MEASURES

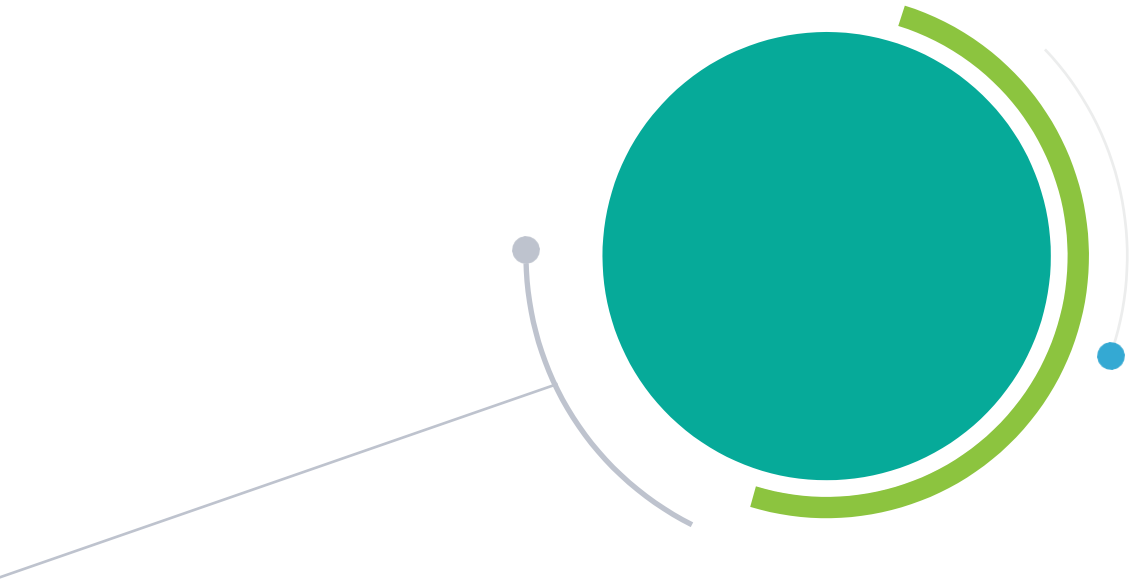
Technological measures are or will be implemented within the competencies of IT departments of academic institutions or based on IT supply and service provisions related to cybersecurity.

According to international standards for information security systems, cybersecurity is a narrower subset of information security as it pertains to the protection of information in cyberspace. Implementing new measures for ensuring cybersecurity does not always or only mean the implementation of new ICT devices and systems but also involves the need for organisational, HR, and/or physical protection measures for buildings and facilities.

Cybersecurity measures will need to be reassessed and supplemented from the perspective of protecting institutions against illegitimate interference and strengthening research security, particularly through the introduction of the following:

- **Managing authorisations and access** to sensitive and protected electronic data in line with organisational measures, managing the allocation and use of access rights, and ensuring secure authentication.
- **Ensuring data integrity** (preservation and accessibility), including data masking, in accordance with organisational measures concerning access to information.

- **Securing trustworthy ICT services and supplies**.
- **Securing user endpoints**, managing the use of removable media.
- **Enhancing cybersecurity measures,** and addressing technical vulnerabilities, whether based on the mandatory implementation of European NIS2 legislation, including:
  - Access to source codes.
  - Protection against malicious software, managing software installations.
  - Securing network services.
  - Managing technical vulnerabilities.
  - Secure programming and development.
  - Use of cryptography.
  - Conducting cybersecurity audits.
- Continuously evaluating the effectiveness of relevant measures for specific institutions or research projects,
- and other actions as recommended by cybersecurity experts.



CONCLUSION

For a system of measures to strengthen research security to achieve the intended results and help reinforce the credibility of research and higher education and research institutions in the Czech Republic, the implementation of effective measures will require adequate financial and capacity resources.

In the **Proposal for a Council Recommendation on enhancing research security, the European Commission calls on** Member States, national authorities, and individual academic institutions to mobilise existing financial resources to strengthen their research security. It is also expected that the criterion of research security will become an integral part of the schemes supporting international research collaboration in the future.

Given this, the agenda of institutional resilience will need to be integrated into the operations of higher education and research institutions. Initially, the implementation of this agenda will require increased attention, but it will eventually become a routine part of the work of research and administrative staff, without representing a significant additional burden in terms of personnel or financial resources. On the contrary, it should provide assurances for stable development and create space for trustworthy collaboration.