COLLECTION OF DECISIONS AND ORDINANCES OF THE UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

Number: R 632 Date: 9 March 2026

Rector's Ordinance to strengthen resistance to illegitimate influence at the University of South Bohemia in České Budějovice

Article 1

Introductory provisions

1. International cooperation in the field of research, development and innovation is primarily based on a common understanding and respect for fundamental values and principles such as academic rights and freedoms, research ethics, research integrity and the principles of open science. However, as a result of these fundamental values and principles, higher education and research institutions are particularly vulnerable to illegitimate influence.

2. Higher education and research institutions are directly responsible for the management and development of their international cooperation, in accordance with academic freedoms and their autonomy. At the same time, these institutions are fully aware of their role and responsibility towards society and their task of protecting democratic and academic values.

3. The aim of this ordinance is to establish internal processes and binding procedures at the University of South Bohemia in České Budějovice (hereinafter also referred to as 'USB') in order to strengthen USB's resilience to illegitimate influence (hereinafter also referred to as 'institutional resilience'). In particular, it emphasises the need to raise awareness of this issue across USB, the need for proper education of its employees and students, and the awareness of the personal responsibility of each of them.

4. In the case of higher education and research institutions, institutional resilience should be understood as the ability to implement a system of measures to strengthen research security against illegitimate influence and to protect their reputation, consisting in particular of secure international research and academic cooperation, including compliance with binding sanctions, in intellectual property management and risk management, particularly in areas of research with significant transformative potential for knowledge and technology, in areas related to dual-use

technologies and military equipment, but also in managing the risk of misuse of knowledge or technology to violate human rights and freedoms.

5. In strengthening its resilience to illegitimate influence, USB draws primarily on generally applicable legal regulations[1] and public methodological materials related to this area.[2]

6. For the sake of simplicity, this ordinance uses the generic masculine form in its text.

Article 2

Basic concepts

1. 'Illegitimate influence' is a term used to describe undesirable influence on people, decision-making or processes. It includes the influence of foreign powers but also criminal (e.g. corrupt) behaviour and undesirable lobbying. These are usually activities that are hidden, deceptive, coercive or corrupt, and which the originator of the illegitimate influence (foreign power, corruption, lobbying in violation of the law or generally accepted social ethical rules) performs directly or through a third party and which threaten or harm the interests of higher education and research institutions.

2. According to the Council Recommendation on strengthening research security,[3] the following are considered to be illegitimate influence in the field of research, development and innovation:

   a) Undesirable transfer of critical knowledge, know-how and technologies that may affect the security of the EU and its Member States, for example if used for military or intelligence purposes in third countries;
   b) Misuse of research activities to spread disinformation based on influence from third countries/parties;
   c) Incitement of self-censorship among students and researchers, leading to the undermining of institutional autonomy;
   d) Violations of scientific ethics or research integrity, resulting in the misuse of knowledge and technology to suppress or undermine fundamental democratic values.

3. 'Foreign power' means a foreign state or its body, or a supranational or international organisation or its body, as well as any other natural persons, regardless of their nationality, and legal persons, regardless of their registered office or place of business, if they participate, even partially, in promoting the interests of a foreign state or organisation through illegitimate influence.

4. The term 'due diligence' means the appropriate care taken to eliminate or reduce the risks of illegitimate influence on higher education and research institutions resulting from cooperation with third parties.

5. The term 'balanced openness' refers to the balance between developing open cooperation with international partners on the one hand and strengthening research security on the other.

Article 3

USB Security Manager

1. The USB Security Manager is responsible for the USB's resilience to illegitimate influence.

2. The USB Security Manager reports directly to the USB Rector and is part of the Rector's Office within the organisational structure of the USB Rectorate.

3. The USB Security Manager, in particular:
   a) Sets up and continuously adjusts the USB's system of resistance to illegitimate influence;
   b) Monitors current developments and continuously educates themselves in the area of resilience to illegitimate influence in the higher education and R&D environment;
   c) Continuously informs the Rector or the Rector's Board about changes and the current situation in the area of resilience to illegitimate influence in the higher education and R&D environment;
   d) Regularly assesses the risks associated with institutional resilience, including the identification of sensitive areas of education and research at USB[4] (degree programmes, research teams, projects, instruments, equipment or technologies, scientific outputs including research data),
   e) Sets up a system and schedule for training USB employees and students to increase institutional resilience,
   f) Provides USB employees and students with consultations and advice on institutional resilience,
   g) Receives, evaluates and keeps records of reports pursuant to Article 6 of this ordinance and records of risk assessments processed by partners pursuant to Article 8 of this ordinance, including related documents;
   h) Communicates with other higher education institutions, state authorities, security forces, representative offices, international organisations and other relevant actors in the field of institutional resilience.

4. The USB Security Manager cooperates:
   a) With faculties and other parts of USB in the area of institutional resilience through institutional security officers;
   b) With the USB Cyber Security Manager in the area of information and cyber security;
   c) With the Head of the USB Technology Transfer Office in the area of intellectual property protection and technology and knowledge transfer;
   d) With the USB Bursar in the area of assessing restrictions imposed due to international sanctions or control regimes and in the area of screening foreign investments;
   e) With the USB Ethics Committee in the area of ethics and integrity of research at USB;

f) With the Occupational Health and Safety (OHS) and Fire Protection (FP) Officer at USB in the area of physical security;
g) With the USB Open Science Manager, particularly in the area of research data management at USB.

Article 4

Institutional Resilience Officers

1. Institutional resilience officers have been appointed for individual remits relating to research safety at USB:
   a) Financial remit – Bursar;
   b) Personnel remit – Head of the Rectorate Human Resources Office;
   c) Project remit – Vice-Rector for Development and External Relations;
   d) Internationalisation remit – Vice-Rector for International Relations;
   e) Science and research remit – Vice-Rector for Research;
   f) Studies remit – Vice-Rector for Student Affairs.

2. Institutional resilience officers, in particular:
   a) Cooperate with the USB Security Manager and follow his instructions and recommendations;
   b) Methodically manage their remits and cooperate with the relevant persons at the faculties (secretaries, heads of human resources offices, vice-deans with relevant remits) or directors of other constituent parts of USB (hereinafter referred to as 'responsible persons at the constituent parts');
   c) Undergo regular training in the field of institutional resilience;
   d) Provide employees and students with consultations and advice on institutional resilience in their remits;
   f) In cooperation with the responsible persons at the constituent parts, regularly evaluate and identify risky degree programmes, areas of education, scientific fields, and specific research teams, projects, instruments, equipment, and technologies at the given constituent part.

Article 5

Obligations of employees and students

1. Employees and students of USB are obliged to behave in such a way as to prevent the possibility of foreign influence being exerted on USB and to prevent violations of regulations relating to international control and sanctions regimes.

2. If attempts to exert foreign influence or violate the regulations under paragraph 1 occur, employees and students are obliged to report these incidents without undue delay (Article 6 of the ordinance).
3. Before entering into a contractual relationship with an external partner, employees are required to assess the risks of cooperation with the relevant contracting party (Article 8 of the ordinance). This also applies to the conclusion of memoranda and declarations of cooperation.
4. When concluding agreements or memoranda and other documents relating to cooperation in R&D and education, their content should include security criteria and related key conditions, as well as the establishment of rules applicable to foreign relations in the context of receiving delegations or travelling abroad.
5. Employees are required to undergo training on institutional resilience and to renew their training regularly. Selected employees who, particularly in view of their managerial positions, scientific field or area of education in which they work, are more likely to be the target of influence, shall undergo training to an extended extent.
6. Students are required to undergo training on institutional resilience if the USB Security Manager so decides.
7. Violation of the obligations under paragraphs 1 to 5 will be considered a serious violation of the obligations arising from the legal regulations relating to the work performed by employees within the meaning of Section 52(g) of Act No. 262/2006, the Labour Code.
8. Violation of the obligations under paragraphs 1 to 2 and 6 shall be considered a violation of the obligations established by legal regulations or internal regulations of the University within the meaning of Section 64 of Act No. 111/1998, on Higher Education Institutions and on Amendments and Supplements to Other Acts (Higher Education Act).

Article 6

Reporting security incidents

1. If an employee or student suspects that foreign influence is being exerted or attempted, or if a situation of illegitimate influence is observed in cooperation with third parties, or if such a situation or suspicion arises retrospectively, they shall immediately report these facts to the USB Security Manager via the email address protivliv@jcu.cz (Article 4 of the ordinance).
2. The report referred to in (1) must clearly state who is making it and what it concerns. A template for such a report is attached as an annexe to this ordinance.

3. The USB Security Manager shall evaluate the report within a reasonable time, taking into account the circumstances and the seriousness of its content, provide feedback and, if necessary, recommend further action. To this end, they may request consultation with the responsible person at the constituent parts of USB and the relevant institutional resilience officer. Where necessary or appropriate, the USB Security Manager shall report the facts to the state administration authorities or security services or consult with them on the situation.

4. Serious security incidents shall be reported by the USB Security Manager to the USB Rector or Dean, together with his or her recommendation. In such cases, the USB Rector or Dean shall decide on further action, usually after discussion with his or her colleagues on the USB Rector's Board.

Article 7

Mandatory reporting relating to international sanctions and control regimes

1. In cases where there is a suspicion that an applicant for studies, an applicant for employment or a potential partner collaborating on a research or educational project is from a country against which international sanctions[5] prohibiting technical assistance have been imposed, the student affairs office of the faculty, the human resources office of the constituent part or the project team concerned shall report this without undue delay to the USB Security Manager via the email address protivliv@jcu.cz

2. The report referred to in (1) must clearly state who is making it and what it concerns. The USB Security Manager may issue a template for such a report.

3. The USB Security Manager, in cooperation with the responsible person at the constituent part or the institutional resilience officer, shall recommend to the USB Rector or Dean, according to their authority in the matter, further action, in particular whether it is possible to continue with the admission procedure, selection procedure or project preparation, and under what conditions. This recommendation shall be based on the individual circumstances of the case, the degree programme, the field of education or the scientific discipline to which the case relates. The Security Manager is obliged to comply with all generally binding legal regulations, including informing or obtaining an opinion or permission from state authorities. The Rector or Dean shall decide on the further course of action, usually after discussion with their colleagues on the Rector's Board.

4. If there is a change in any of the international sanctions regimes that could affect the area of education or scientific research, the USB Security Manager shall inform the institutional resilience officer and the responsible persons at the constituent parts. The relevant institutional resilience officers shall then assess whether further action is necessary in relation to applicants for studies,

students, job applicants, employees or contractual or research partners. If such action is necessary, they shall inform the USB Security Manager. (3) shall apply analogously.

Article 8

Risk assessment of partners (due diligence)

1. Cooperation with third parties is an integral part of the activities of every higher education and research institution. Most of this cooperation is beneficial and poses no or only minimal risks of illegitimate influence. At the same time, however, there are areas of cooperation between higher education and research institutions and third parties that carry risks of undue influence to such an extent that it is highly desirable for higher education and research institutions to attempt to mitigate these risks as far as possible.

2. Due diligence is divided into basic and detailed. Basic due diligence[6] should be applied as widely as possible, ideally whenever a higher education or research institution establishes a relationship with a new partner, changes its relationship with an existing partner, or repeatedly during long-term cooperation. Detailed due diligence[7] should be used in particular in cases where basic due diligence reveals information indicating that the cooperation under review carries increased risks.

3. Before entering into a contractual relationship with an external partner, in particular a partnership agreement, research agreement or memorandum and declaration of mutual cooperation, employees responsible for preparing such an agreement or memorandum are obliged to assess the risks of cooperation with the other contracting party. Before commencing specific cooperation, it is also advisable to verify what internal rules and procedures are applied by the potential partner institution for cooperation with third parties.

4. If the conclusion of such a contractual relationship or memorandum poses a risk of damage to the reputation of USB or the employees or students involved, the exercise of foreign influence, the violation of restrictions arising from international control and sanction regimes, or the theft of intellectual property, the employee is obliged to contact the responsible person at the department, the institutional resilience officer or the USB Security Manager, who will assess the situation and recommend further action.

5. The USB Security Manager may designate selected constituent parts of USB, degree programmes, areas of education, scientific fields, scientific or educational projects, countries of origin of contractual partners or other characteristics of contractual relationships for which a written risk assessment must be prepared. The Security Manager of USB shall then submit this assessment, together with their recommendation, to the USB Rector or Dean, depending on their authority in

the matter. The USB Rector or Dean shall decide on the next steps, usually after discussion with their colleagues on the Rector's Board.

6. Cooperation is understood here in the broad sense of the term, including documents (contracts, memoranda, etc.), foreign trips, visits by third-party representatives, but also patronage, financing, gifts and attentions. The USB Security Manager may, through methodological recommendations for each of these activities, determine the requirements that such a risk assessment must meet.

Article 9

Binding procedures

1. Binding procedures related to strengthening the USB's institutional resilience to illegitimate influence are set out in the annexes to this ordinance.
2. The basic principles of illegitimate influence, its recognition and methods of reporting are described in Annexe 1 to this ordinance.
3. The form for reporting incidents related to illegitimate influence at USB is defined in Annexe 2 to this ordinance.
4. The rules of conduct on foreign business trips, especially on short-term trips to high-risk countries and fully funded by USB, are set out in Annexe 3 to this ordinance.
5. The list of high-risk countries from the perspective of USB is provided in Annexe 4 to this ordinance.

Article 10

Final provisions

1. The issue of research data protection during the preparation and conduct of research and its disclosure will be addressed in a separate ordinance by the Rector.
2. This ordinance repeals Rector's Ordinance R No. 566 of 21 November 2024.
3. This ordinance comes into force and takes effect on the date of its publication in the collection of decisions and ordinances of the USB Rector in the public section of the USB website.
4. The annexes to this ordinance shall be updated without the need to issue a new ordinance, always recording the number and date of the annexe version.

Prof. Ing. Pavel Kozák, Ph.D.
Rector

Prepared by: Vice-Rector for Research, Vice-Rector for International Relations

Distribution list: USB management, deans of USB faculties, directors of the other constituent parts of USB, USB Cyber Security Manager, Chair of the USB Ethics Committee, Occupational Health and Safety and Fire Protection Officer

Annexes:
1. Illegitimate influence at USB and its reporting
2. Rules of conduct on foreign trips
3. List of high-risk countries
4. Incident reporting

---

[1] In particular, Act No. 69/2006, on the implementation of international sanctions, Act No. 594/2004, implementing the European Communities' regime for the control of exports of dual-use goods and technologies, Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 establishing a Union regime for the control of exports, brokering and technical assistance (EU) 2021/821 of 20 May 2021 establishing a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

[2] In particular, methodological materials from MEYS:
- Strengthening resilience to illegitimate influence in higher education and research environments,
- Methodological recommendations for risk management in the area of research security at the institutional level;
- Methodological recommendations defining the minimum scope of due diligence and risk management in cooperation with third parties in the context of strengthening the resilience of the higher education and research environment to illegitimate influence (hereinafter referred to as 'Methodological recommendations for cooperation with third parties');
- Other materials referred to in these methodological materials.

[3] https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:C_202403510

[4] Article 6 of the Methodological Recommendations for Cooperation with Third Parties.

[5] Within the meaning of Section 2 of Act No. 69/2006, on the implementation of international sanctions.

[6] Article 7 of the Methodological Recommendation on Cooperation with Third Parties.

[7] Article 8 of the Methodological Recommendation on Cooperation with Third Parties.