Annexe No. 1 Rector's Ordinance R 632

Illegitimate influence at USB and its reporting

Purpose and context

International cooperation, openness and academic freedom are fundamental elements of excellent research, development and innovation. However, it is precisely these elements that can make the academic environment (i.e. primarily higher education and research institutions) particularly vulnerable to illegitimate influence. With growing international tensions and the increasing geopolitical importance of research, development and research, academic institutions today increasingly face risks associated with **illegitimate influence** in their international cooperation.

What is illegitimate influence and institutional resilience?

Undue influence is **the undesirable influence on people, decision-making or processes**. It includes the influence of foreign powers, but also criminal (e.g. corrupt) behaviour and undesirable or illegal lobbying. **These are usually activities that are hidden, deceptive, coercive or corrupt.** These activities can threaten and damage not only the interests of the University of South Bohemia, the higher education and research environment, but also **the broader protected interests of the CR** (e.g. security, defence, economic or political interests).

Institutional resilience to illegitimate influence refers to the ability of an academic institution to establish and implement **a system of measures to strengthen research security** against illegitimate influence and to protect its reputation. This system consists primarily of responsible international cooperation, which includes compliance with binding sanctions and appropriate screening of foreign partners, good 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 or military technologies, but also in research involving the risk of misuse of personal data or knowledge or technology to violate human rights and freedoms.

Illegitimate influence can pose significant operational, security, legal, financial and reputational risks for USB. It can lead to **disruption of decision-making and internal processes** or **interference with intellectual property, know-how and sensitive information** (e.g. research results, non-public contractual information and personal data). In extreme cases, it may result in **a breach of legal obligations** (e.g. binding sanctions regimes), which may lead to disputes and the threat of financial losses. We must also not overlook the considerable **reputational risks**, including threats to cooperation with reliable foreign partners, threats to academic freedom and openness of research, and threats to trust in the institution's results and data. Reputational risk activities also include patronage or participation in various events that appear to be professional but in fact have a hidden agenda or are organised by an entity that poses a reputational risk. The risks of influencing instruction, especially in the social sciences, cannot be overlooked either. It is also important to realise that financial risks are not necessarily linked only to violations of sanctions that are legally binding in the CR, but also to those that are not binding, e.g. through the loss of the opportunity to participate in a prestigious grant financed from abroad because the foreign provider must comply with sanctions that are legally binding for them but are not legally binding in the CR.

Strengthening institutional resilience means **building this resilience and increasing vigilance**. The ability to recognise risks in a timely manner and identify suspicious behaviour is key. A functional system is therefore a combination of institutional safeguards (internal regulations, processes, risk description and management, training of employees and students) and the personal responsibility of each individual. **Our awareness and attentiveness are therefore fundamental prerequisites** for being able to deal with potential threats effectively and in a timely manner.

Who could be a target?

Who can be the target of influence activities? Potentially, all of us, both members of the academic community and those outside it. **Anyone who comes into contact with an academic institution** is potentially of interest – students, interns, staff members in higher education and research, other employees, and even other people involved in the activities of an academic institution. This is because, **as employees of an academic institution, we have access to a wide range of sensitive information that could be misused against the protected interests of the institution, the academic environment, or the entire CR**. In addition, **some of us can influence important processes or individuals, which may be of interest to foreign powers**. In some cases, you may become 'just' **a tool** for an attacker **to influence someone else**.

It is **our access to sensitive information, research or other internal processes, or other individuals that makes us interesting to attackers**.

Recognising suspicious situations

How do I know that I have become the target of illegitimate influence? In the vast majority of existing cases, it was obvious to those who became the targets of illegitimate influence or their immediate surroundings that something was wrong – that **'something was wrong' or 'different' from what is normal in similar situations**. For example**,** they received **offers that seemed too good to be true** and often concealed malicious intent. Or they received **offers that they were pressed to consider quickly.**

This strategy by the attacker relies on creating pressure to make quick decisions, thereby reducing vigilance and careful consideration of the whole matter. A complete description of illegitimate influence techniques can be found in Chapter 6 of the Anti-Influence Manual for the HEI sector. Some specific scenarios of illegitimate influence are also demonstrated in a series of videos on the Trusted Research – Implementation Scenario Videos page.

It should also be noted that a security incident does not have to occur only on USB premises; you may also be approached on business trips or private trips, at social events, during chance encounters, or in other situations outside the work environment. Typical situations that subsequently lead or may lead to being approached for cooperation include, for example, direct approaches for cooperation, staged incidents, informal meetings under special circumstances, gifts or other advantageous invitations. Not only professional or courtesy visits abroad on USB premises, but also exchange programmes, conferences and other international meetings are often used as a starting point for approaching individual academics and for enabling or facilitating foreign trips and stays in the CR by foreign nationals posing as academics or members of their accompanying staff.

Reporting incidents

What should I do **if something like this happens to me** or I notice it happening to someone else?

If:

- You feel that someone is trying **to influence you or put pressure on you** (in a situation where they behave or act inappropriately towards you, for example, asking excessive questions about your research, internal processes, etc.);
- **You have received conspicuously advantageous offers of cooperation** (invitations to events, disproportionate gifts, paid trips abroad and training);
- Someone has tried to obtain or has obtained **unauthorised access to confidential information** through you or your colleagues;
- **You are unsure whether a certain unusual situation** that has happened to you or your colleagues, and which may unduly interfere with internal processes or decision-making at the faculty or USB, is **an attempt at illegitimate influence** and foreign interference,

inform the USB Security Manager.

Contact address:protivliv@jcu.cz

Briefly describe the situation, when and where it occurred, and who was involved (who was present, who contacted you).

The USB Security Manager will then ask you for a meeting and fill out **a Security Incident Report form** with you**, which is available in a separate annexe to the ordinance.** Alternatively, you can fill in this form directly and send it to the address provided (the USB Security Manager will still contact you and discuss the whole situation with you in person).

It is important not **to keep information about a possible ongoing attempt at illegitimate influence to yourself** and to report the incident. Similarly, you can contact the USB Security Manager in situations where you anticipate risks, e.g. before a business or private trip to a risky country (see also the following annexe), before signing a contract in which you find certain passages questionable, when preparing joint research projects with risky partners, or during the admission process for a person to study or work who may pose a risk. One of the main goals of building institutional resilience is not only to deal with actual or perceived incidents/anomalies that have already occurred, but also to reach a state where the majority of the USB academic community thinks about risks in advance and consults on them. The ultimate goal is to enable risky collaborations to take place, but in a way that is safer for both USB and the members of its academic community.

Summary of basic principles

The basis for increasing the resilience of an academic institution to illegitimate influence is the awareness that anyone can become a target of illegitimate influence or threats to research security. It is also crucial that everyone must take responsibility for their actions in such a situation. In short, it can be summarised as follows:

- **Everyone is interesting.** Everyone may have access to a certain amount of sensitive information (or decision-making powers).
- **Everyone is vulnerable.** Anyone who has access to sensitive information (or decision-making powers) can become a target of illegitimate influence, and whether this happens is beyond their control.
- **Everyone can ask for help.** If someone has already become the target of illegitimate influence, they have the option of resolving the situation with the help of others. Early reporting can be the most effective way to prevent damage.

Thanks to your responsible approach, USB will become more resistant to illegitimate influence and a safer environment overall, not only for research. Such resilience will enable us to better respond to risky situations, prevent them and minimise any consequences. Your behaviour can be **a good example and inspiration** for your colleagues and other institutions.

Annexe No. 2 Rector's Ordinance R 632

Rules of conduct on foreign trips

Participation in international conferences, as well as visits to foreign colleagues at their workplaces, is an integral part of the professional activities of academics and researchers. With growing international tensions and the increasing geopolitical importance of research and innovation, there is a growing need to thoroughly assess the risks of such trips, especially when they involve countries whose democratic and ethical values differ from ours, not only before they take place but also after returning.

This text aims to briefly outline the possible risks and threats of travelling abroad and to provide basic advice and recommendations on how to deal with such potential challenges. It concerns in particular:

- Participation in conferences and other scientific meetings
- Teaching
- Visits to academic and research institutions
- Visits to non-academic partners, such as business or industrial partners

These rules apply in particular to **short-term stays (business trips) fully funded by USB**. They do not primarily apply to longer-term research-related stays, such as fieldwork or internships, or stays (partially) funded by a third party – these will be dealt with separately (although many of the recommendations described below may also be useful for longer stays as well).

What to consider before travelling?

Before travelling abroad, it is important to remember that in different countries there may be differences in:

- Understanding of democracy and ethical principles
- Understanding of academic freedom (the degree of protection of academic freedoms in a given country is quantified by the Academic Freedom Index)
- Rules restricting cooperation established by sanctions imposed by the CR, the EU, the UN, etc., or arising from the rules of the country in question
- Cultural and legal environment

Before every trip abroad related to science and research (but also teaching), we should consider this in connection with the reason for our trip. We should therefore ask ourselves:

- What is the level of protection of academic freedoms in the country concerned?
- Is the country subject to binding relevant sanctions?
- Could our research be sensitive in relation to the country in question?

- Could our professional focus or activities in the country in question pose a risk to us? For example, if they could be perceived as contrary to the traditions, rules or even laws of the country.

It is therefore necessary to prepare carefully for every trip abroad. In addition to standard matters such as having an approved travel order, the correct type of visa (if required) and adequate insurance, a number of other aspects need to be considered:

- Do you need to take all your research with you that you have on your laptop or is it accessible from your laptop without protection? In some countries, the authorities have the right to access your laptop and copy all its contents, but sometimes they can do so without your knowledge (see also other recommendations below).
- Is the topic you want to discuss, even informally, restricted in any way by USB regulations (e.g. sensitive research or protected intellectual property) or USB contracts with third parties (e.g. contractual research, where you can only present the topic with the express consent of the third party)?

Electronics and data

We all take our laptops and mobile phones with us (not only) on trips abroad. That is fine, and ultimately unavoidable. However, it is necessary to consider what work and personal information they contain and what the consequences would be for us and for USB if we lost any of it, if it were stolen, or if it were 'only' copied. Before each trip to a high-risk country (a list of these countries is provided below in Annexe 4), we therefore require you to consult with the USB Cybersecurity Manager about your trip and the electronics you intend to take with you. They will explain and recommend what risks you may encounter, how to secure your data, how to connect to USB securely from abroad, whether your technology will work at all on site, but will also offer you to take only clean devices with the most necessary content for your trip. The main recommendations include:

- Sometimes it is worth getting a local phone and phone plan.
- Keep your devices password-protected, ideally with a different password for each one.
- If any of your applications allow two-factor authentication, turn it on.
- If you are taking your own laptop, consider backing up and removing (i.e. transferring to another medium) data and information that you will not need or that is highly sensitive before you travel.
- Back up the contents of your mobile phone before you leave.
- Connect to USB primarily via VPN.

- Ensure that all your applications are up to date, your antivirus is enabled, automatic USB startup when inserted into your laptop is disabled, and your laptop does not automatically connect to Wi-Fi (the IT office will be happy to advise you on this).
- Never download applications from unofficial providers.
- Upon your return, contact the IT office, discuss the course of your trip with them, and hand over all your equipment for inspection.

If you are already in the country and no one is obviously following your around at the airport or hotel, you may easily get the feeling that no one is interested in you and that you are not in any danger. However, you should still carefully consider all your activities, whether related to the purpose of your visit (science, research, teaching) or your free time (smoking or drinking alcohol in public, inappropriate clothing, especially (but not only) for women, watching demonstrations or police or military equipment on the street, etc.). Could they expose you to any danger, external pressure, damage to your reputation, the reputation of USB or even the CR?

Behaviour when travelling abroad

We recommend:

- Be prepared to face unusual requests, e.g. you may be questioned or even pressured to share information about sensitive areas of your work. This will certainly put you in a very uncomfortable position. Always respond with a polite but firm refusal.
- Consider carefully what you will do with any gifts you receive and whether you need to declare any valuable gifts.
- Carefully consider what you are signing (whether, for example, you are giving up any rights or giving something to someone) and, if in doubt, contact the Legal Office of the USB Rectorate.
- Be aware that public and hotel Wi-Fi connections may not be secure, and consider what information you will share over these connections. In particular, avoid logging in with your USB account or using your internet/mobile banking. Using public Wi-Fi is risky in general, not only in relation to work activities, as it can compromise the device itself, regardless of whether it is used for work or private activities. At a minimum, it is always advisable to use a VPN.
- Be aware of unusual behaviour on your devices and do not share your laptop, phone or USB drive with anyone.
- Be careful with all IT gifts such as USB drives. It is safer to accept them, thank the giver, and discreetly dispose of them.
- Never connect your USB to another device, or a stranger's USB to yours.
- Always keep your electronics and sensitive materials with you. Even a hotel safe does not guarantee completely secure storage.

- Think about who you share information about yourself and your work with and what kind of information you share.
- Be wary if someone invites you to a free event or if an offer appears that seems too good to be true.

As always, if something unusual or suspicious happens, **inform your superiors and the USB Security Manager** (**see Illegitimate Influence at USB and its Reporting – Incident Reporting**) during your trip or after your return, depending on your assessment of the seriousness of the situation, and consider returning early.

Conferences and other scientific meetings are an excellent opportunity to exchange experiences and information, but also to establish new collaborations. However, it is always necessary, especially nowadays, to bear in mind the security risks associated with such trips. It is therefore highly desirable to be well prepared for every trip abroad in this respect.

You can also refer to the Trusted Research Countries and Conferences Guidance page.

Annexe No. 3 Rector's Ordinance R 632

List of high-risk countries

The following list includes countries with:

- Academic freedom index higher than 0.1 that are on the sanctions list – blue,
- Academic freedom index lower than 0.1 that are on the sanctions list – in red,
- Academic freedom index lower than 0.1 that are not on the sanctions list – in black.

Both the Academic Freedom Index and the sanctions list are subject to change over time. The USB Security Manager may decide to amend this list, particularly in view of the foreign security situation, after approval by the USB Rector's Board. The individual constituent parts of USB must be informed of this decision.

Haiti
Somalia
Democratic Republic of Congo
Central African Republic
Libya
Ukraine (occupied territories, including Crimea)
Sudan
Yemen
Zimbabwe
Russia
Venezuela
Syria
Iran
South Sudan
--- 0.1 (academic freedom index value)
Cuba
Egypt
Afghanistan
Tajikistan
Equatorial Guinea
Saudi Arabia
China
Turkmenistan
Rwanda
Belarus
Eritrea
Myanmar/Burma
North Korea
Nicaragua