IRIS UHK

Manuál institucionální bezpečnosti

Identifikace, prevence a řízení rizik v mezinárodní spolupráci

Univerzita Hradec Králové

Prorektorka pro vědu, výzkum a transfer znalostí

ve spolupráci s prorektorkou pro zahraniční vztahy

Verze: 1.1 | Rok: 2026

1. Úvod a účel manuálu

Manuál IRIS UHK (Institucionální a vědecká odolnost, integrita a síťová ochrana) je závazným provozním dokumentem Univerzity Hradec Králové pro oblast institucionální bezpečnosti. Poskytuje zaměstnancům, vedoucím pracovišť a pracovníkům institucionální bezpečnosti (IB) srozumitelný rámec pro identifikaci, hodnocení a řízení rizik spojených s mezinárodní spoluprací.

Manuál navazuje na Pokyn prorektorek č. 7/2026 k povinným konzultacím u rizikových mezinárodních aktivit a na metodická doporučení Ministerstva školství, mládeže a tělovýchovy (MŠMT) k bezpečnosti výzkumu.

Proč je to důležité?

Mezinárodní spolupráce je pro UHK klíčová — zároveň však může přinášet rizika, která nejsou vždy zjevná: nelegitimní přenos technologií, reputační poškození, narušení akademické svobody nebo porušení sankčních předpisů. Cílem tohoto manuálu je pomoci tato rizika včas identifikovat a zvládnout — nikoli bránit spolupráci.

1.1 Klíčové pojmy

Pojem	Vysvětlení
IRIS UHK	Systém institucionální bezpečnosti UHK — zahrnuje procesy, nástroje a odpovědnosti pro ochranu integrity výzkumu a spolupráce.
Mezinárodní aktivita	Výzkumná/výuková spolupráce, projekty, smlouvy, MoU, mobility, hostování, sdílení dat/know-how, dary, sponzoring se zahraničním prvkem.
Riziková aktivita	Mezinárodní aktivita naplňující alespoň jeden rizikový indikátor dle aktuálního checklistu na webu UHK.
Due diligence (DD)	Systematické posouzení důvěryhodnosti partnera a podmínek spolupráce, včetně sankčních, reputačních a bezpečnostních aspektů.
Konzultace	Povinné posouzení záměru a nastavení podmínek realizace dle Pokynu prorektorky 7/2026.
Checklist IRIS	Online nástroj (formulář) pro ověření rizikovosti záměru — vyplňuje žadatel před konzultací.
Dual-use	Technologie nebo znalosti s možným vojenským nebo jiným rizikovým využitím nad rámec deklarovaného civilního účelu.
Sankční seznam	Seznam entit/osob, se kterými je spolupráce zakázána nebo omezena (EU, OSN, US OFAC a další).

2. Organizace a odpovědnosti

Efektivní institucionální bezpečnost předpokládá jasné vymezení rolí. Níže jsou uvedeny klíčové role a jejich odpovědnosti v rámci IRIS UHK.

Role	Hlavní odpovědnosti v IRIS
Prorektorka pro vědu, výzkum a transfer znalostí	Správce systému IRIS; přijímá a posuzuje konzultace; odpovídá za vedení evidence; vydává stanoviska.
Prorektorka pro zahraniční vztahy	Spolu-konzultant u mezinárodních aktivit; koordinace s mezinárodním odd.
Vedoucí pracovišť / prodekani	Odpovídají za informování podřízených; zajišťují podmínky pro plnění Pokynu; dbají na včasné podání konzultací.
Hlavní řešitel / garant aktivity	Přímá odpovědnost za vyplnění checklistu a podání konzultace před zahájením přípravy závazného ujednání.
Pracovník IB / Compliance manager	Provádí due diligence (prověřování partnerů); vede evidenci případů; podporuje ostatní role.
Právní agenda	Posouzení smluvní dokumentace, IP, exportní kontroly; součinnost při konzultaci.
DPO / GDPR agenda	Posouzení předávání osobních údajů, DPIA; součinnost při citlivých aktivitách.
IT/kyber bezpečnost	Posouzení přístupů do systémů a infrastruktury; nastavení bezpečnostního režimu pro hosty.

3. Rizikové oblasti a indikátory

Rizikové indikátory jsou podrobně definovány v aktuálním checklistu zveřejněném na webové stránce institucionální bezpečnosti UHK. Níže jsou uvedeny hlavní kategorie rizik s příklady.

3.1 Partner a jeho původ

- Partner pochází z tzv. rizikovějších jurisdikcí (např. Rusko, Čína, Írán, Severní Korea, Bělorusko a další dle aktuálních doporučení MŠMT/EU).
- Partner je státní institucí nebo má nejasnou vlastnickou strukturu s vazbou na státní subjekty rizikovějšího státu.
- Zjištěny negativní reputační informace, sankční zápisy nebo vazby na nestandardní financování.
- Nedostatečná transparentnost — nelze ověřit identitu, sídlo nebo právní status partnera.

3.2 Předmět spolupráce

- Spolupráce se týká kritických technologií EU (AI, kvantové technologie, biotechnologie, pokročilé materiály, polovodiče, kosmické technologie, energie).
- Riziko dvojího užití (dual-use) — výsledky výzkumu by mohly mít vojenské nebo bezpečnostní aplikace.
- Přenos citlivých dat, know-how nebo duševního vlastnictví mimo EU bez adekvátního smluvního rámce.
- Provádění výzkumu ve vojensky nebo bezpečnostně citlivých oblastech.

3.3 Financování

- Financování z nejasného nebo anonymního zdroje; dary bez jasného účelu.
- Neobvyklá výše příspěvku (nepřiměřená poskytnutému plnění).
- Podmíněné financování s omezeními výzkumu, publikování nebo sdílení výsledků.
- Sponzoring nebo dar, který by mohl zakládat střet zájmů nebo vliv na výzkumné závěry.

3.4 Smluvní a procesní aspekty

- Návrh smlouvy obsahuje neobvyklé mlčenlivostní doložky, omezení publikování nebo předkupní práva na výsledky.
- Partner požaduje přístup k datům nebo infrastruktuře UHK nad rámec deklarovaného účelu.
- Aktivita je navrhována v neobvyklé rychlosti nebo s tlakem na vynechání standardních schvalovacích kroků.

3.5 Reputační a etická rizika

- Spolupráce s partnerem, který je spojen s porušováním lidských práv nebo akademických svobod.
- Výzkum s potenciálním dopadem na zranitelné skupiny bez etického schválení.
- Mediální nebo veřejný zájem, který by mohl poškodit dobré jméno UHK.

⚠ Pravidlo konzervativního přístupu

Pokud si nejste jisti, zda váš záměr naplňuje některý z rizikových indikátorů — vyplňte checklist a konzultaci si vyžádejte. Je lepší provést konzultaci zbytečně, než zanedbat potenciální riziko.

4. Proces konzultace — krok za krokem

Povinná konzultace probíhá ve třech fázích: příprava podkladů, podání a posouzení, výstup a evidence.

Fáze 1 – Zjistit (Žadatel)

Krok 1: Vyplňte Checklist IRIS

Odkaz: Checklist rizikovosti mezinárodní aktivity (IRIS_UHK) — formulář na webu UHK

Checklist vyplňuje žadatel (vedoucí pracoviště / hlavní řešitel) vždy před zahájením přípravy závazného ujednání. Výsledek checklistu je součástí podkladů pro konzultaci.

Pokud checklist nevyhodnotí žádný rizikový indikátor jako ANO, konzultace není povinná — doporučujeme ji však i tak zvážit u nejasných případů.

Fáze 2 – Podat (Žadatel)

Krok 2: Podejte konzultaci s povinými podklady

Minimální podklady pro konzultaci:

1. Popis záměru a přínosu pro UHK
2. Identifikace partnera(ů) a zdroje financování
3. Výsledek checklistu (označené rizikové indikátory)
4. Návrh smlouvy / MoU nebo klíčové body (pokud existují)
5. Návrh mitigací / podmínek (co je již zajištěno)

Podání probíhá elektronicky prostřednictvím formuláře na webové stránce IRIS UHK.
Lhůta pro vyřízení: standardně 10 pracovních dní od doručení úplných podkladů.

Fáze 3 – Posouzení a výstup (Prorektorky + součinnost útvarů)

Prorektorky posoudí záměr a podle povahy případu přizvou k součinnosti: právní agendu, GDPR/DPO, IT/kyber, zahraniční agendu, ekonomiku.

Výstup konzultace	Co to znamená pro žadatele
✅ **Bez výhrad**	Záměr lze realizovat. Doporučujeme uschovat stanovisko jako součást projektové dokumentace.
⚠️ **S podmínkami**	Záměr lze realizovat po splnění stanovených podmínek a mitigačních opatření. Podmínky jsou závazné a jejich plnění se eviduje.
❌ **Nedoporučeno**	Záměr nelze realizovat v navrhované podobě. Prorektorky navrhnou alternativy nebo podmínky pro přepracování.

5. Due diligence — prověřování partnera

Due diligence (DD) je systematický proces ověřování důvěryhodnosti a rizikovosti zahraničního partnera. Provádí ji pracovník IB nebo pověřená osoba, zpravidla jako součást konzultačního procesu.

5.1 Typy due diligence

Typ DD	Kdy se používá / co zahrnuje
Základní DD	Běžné partnerství bez příznaků zvýšeného rizika. Zahrnuje: ověření identity a právního statusu, vyhledání v sankčních seznamech, základní mediální rešerši, ověření webu a referencí.
Rozšířená DD	Partner ze zvýšeného rizika, citlivá oblast (dual-use, kritické technologie), varovné signály při základní DD. Zahrnuje vše výše + doplňkové databáze (UNODC, OpenSanctions), analýzu vlastnické struktury, geopolitické a etické faktory.

🔑 Vždy Rozšířená DD

Citlivé oblasti jako AI, kvantové technologie, biotechnologie, pokročilé materiály a polovodiče vždy vyžadují Rozšířenou DD — bez ohledu na zemi původu partnera.

5.2 Postup základní DD — přehled zdrojů

Co ověřujete	Kde hledáte
Identita a právní status partnera	Veřejné rejstříky (obchodní, spolkový…), web partnera, akademické profily (ORCID, Scopus, ROR)
Sankční seznamy	EU Sanctions Map (eeas.europa.eu), OpenSanctions.org, OFAC SDN List, UN sanctions
Reputace a mediální rešerše	Google (jméno + instituce + 'scandal' / 'fraud' / 'sanctions'), lokální média, investigativní portály
Akademická integrita	Retraction Watch, PubPeer, Predatory journal databases
Vlastnická struktura	OpenCorporates, národní obchodní rejstříky, ICIJ Offshore Leaks DB
Geopolitické vazby	MŠMT rizikové země, EU Country Risk, Freedom House Index

5.3 OSINT zásady

- Zásada legality — sbírejte pouze veřejně dostupné informace, nepořizujte osobní údaje nad rámec účelu DD.
- Zásada ověřitelnosti — každé zjištění musí být doloženo zdrojem (URL, screenshot, datum přístupu).
- Zásada OPSEC — při prověřování nepracujte pod vlastní identitou; používejte pracovní zařízení určené pro IB, VPN.
- Zásada minimalizace — dokumentujte pouze to, co je relevantní pro posouzení rizika.

6. Eskalační schéma a reakce na incidenty

Zjistíte-li v průběhu due diligence nebo realizace aktivity varovný signál nebo bezpečnostní incident, postupujte dle následujícího eskalačního schématu.

Úroveň / Situace	Co dělám / Kdo rozhoduje
🟢 **Nízké riziko — bez varovných signálů**	Základní DD je dostatečná. Záměr lze realizovat. Dokumentujte výsledek DD a uložte spolu s projektovými materiály.
🟡 **Střední riziko — varovné signály, nejasnosti**	Přecházíte na Rozšířenou DD. Konzultujete s pracovníkem IB / Compliance managerem. Prorektorka informována.
🔴 **Vysoké riziko — závažné nálezy, sankce, varovné signály**	Okamžitě eskalujte na Prorektorku pro vědu a výzkum + právní agendu. Záměr se pozastavuje do vyjasnění. Zvažte konzultaci s MŠMT / FAÚ.
🚨 **Bezpečnostní incident (úniky dat, neoprávněný přístup, podezření z ovlivňování)**	Okamžitě informujte IT/kyber + Prorektorku + při podezření na trestný čin zvažte oznámení orgánům činným v trestním řízení. Aktivujte krizový komunikační plán.

Oznamovací kanály IRIS UHK
➢ Konzultace a podání: https://www.uhk.cz/cs/univerzita-hradec-kralove/veda-a-vyzkum/nelegitimni-ovlivnovani ➢ Pracovník IB / Compliance: hana.tomaskova@uhk.cz ➢ Prorektorka pro vědu, výzkum a TZ: hana.tomaskova@uhk.cz ➢ Anonymní oznamovací kanál (whistleblowing): https://www.uhk.cz/cs/univerzita-hradec-kralove/uhk/uredni-deska/verejne-informace/whistleblowing ➢ Právní agenda: pravnioddeleni@uhk.cz ➢ GDPR / DPO: gdpr@uhk.cz ➢ IT/kyber bezpečnost: https://helpdesk-it.uhk.cz/

7. Citlivé oblasti a dual-use

Výzkum v citlivých oblastech nebo s potenciálem dual-use podléhá zpřísněnému režimu posouzení. Identifikace takových témat je odpovědností každého výzkumníka i vedoucího pracoviště.

7.1 Kritické technologie EU — přehled

Oblast	Příklady technologií / témat
Umělá inteligence	Systémy strojového učení s aplikacemi v bezpečnosti, rozpoznávání obličejů, autonomní systémy
Kvantové technologie	Kvantová kryptografie, kvantové výpočty, kvantové senzory
Biotechnologie	Syntetická biologie, genomika, CRISPR, bioinformatika s vojenským potenciálem
Pokročilé materiály	Nanomaterialy, kompozity pro letecký/vojenský průmysl
Polovodiče a mikroelektronika	Výroba čipů, pokročilé procesory, exportně kontrolované součástky
Kosmické technologie	Satelitní navigace, vzdálené snímání, pohonné systémy
Energetika	Jaderná energetika, technologie pro ukládání energie s vojenským potenciálem

Výčet není vyčerpávající. Při pochybnostech se vždy poraďte s pracovníkem IB nebo prorektorkou.

7.2 Exportní kontrola a licence

- Výzkum nebo transfer technologií s potenciálem dual-use může podléhat exportní kontrole dle nařízení EU č. 821/2021.
- V případě pochybností kontaktujte právní agendu pro posouzení nutnosti licence Ministerstva průmyslu a obchodu (MPO).
- Nehmotný přenos technologií (e-mail, cloud, vzdálená spolupráce) rovněž může podléhat exportní kontrole.

8. Smluvní ochrana a doporučené mitigace

Při identifikaci rizikových indikátorů nebo po konzultaci s podmínkami je nezbytné zajistit odpovídající smluvní ochranu a mitigační opatření.

A) Partner a financování

- Doplnění informací o vlastnické struktuře a konečném příjemci (beneficial owner).
- Ověření transparentnosti financování a smluvních plateb.
- Prověření sankčních aspektů v součinnosti s IRIS/compliance.

B) Smluvní ujednání

- Jasná pravidla publikování a nakládání s výsledky — žádné neodůvodněné omezení.
- Vyvážené nastavení IP a mlčenlivosti; omezení exkluzivity.
- Doložka o souladu s interními pravidly UHK a možnost ukončení při zjištění rizika.

C) Data, IT a kybernetická bezpečnost

- Minimalizace přístupů (need-to-know), oddělené účty, časově omezený přístup.
- Posouzení GDPR/DPIA; pravidla předávání dat mimo EU; smluvní zajištění (standardní smluvní doložky).
- Bezpečné ukládání dat; evidence přístupů.

D) Dual-use / citlivá témata

- Odborné posouzení rizika dvojího užití; omezení sdílení detailů v rané fázi výzkumu.
- Interní schválení publikace u citlivých výstupů (procesně, nikoli obsahově — ochrana akademické svobody).

E) Reputace a komunikace

- Koordinace s vedením UHK; sjednocené veřejné odpovědi.
- Předem dohodnutý komunikační plán pro případ mediálního zájmu.

9. Vzdělávání a šíření povědomí

Institucionální bezpečnost je sdílenou odpovědností — každý zaměstnanec, student i člen vedení je spoluzodpovědný za odolnost UHK.

Minimální osnova školení (dle Přílohy 5 Pokynu prorektorek)

- Principy institucionální odolnosti, prevence a odpovědnost jednotlivců.
- Typické rizikové scénáře v mezinárodní spolupráci (partnerství, financování, dary, MoU).
- Due diligence minimum: reputace, vlastnická struktura, zákonnost, sankční aspekty.
- Data / IT bezpečnost a řízení přístupů.
- Střet zájmů, etika, dokumentace.
- Postup oznamování a ochrana oznamovatelů.

Školení se organizuje alespoň 1× ročně pro vedoucí pracovišť a pracovníky zapojené do mezinárodní spolupráce. Nově příchozí zaměstnanci procházejí vstupním školením v rámci onboardingu.

10. Právní a metodický rámec

Dokument / Předpis	Relevance pro IRIS UHK
Pokyn prorektorky č. 7/2026	Závazný vnitřní předpis UHK pro povinné konzultace — základ celého systému IRIS.
Metodické doporučení MŠMT k bezpečnosti výzkumu (2024)	Doporučení k due diligence a řízení rizik spolupráce pro české VŠ.
Nařízení EU 2021/821 (exportní kontrola dual-use)	Pravidla pro vývoz zboží a technologií s možným vojenským využitím.
GDPR (Nařízení EU 2016/679)	Ochrana osobních údajů; předávání dat mimo EU; DPIA.
Zákon č. 171/2023 Sb. (ochrana oznamovatelů)	Whistleblowing; povinný vnitřní oznamovací kanál.
Zákon č. 412/2005 Sb. (ochrana utajovaných informací)	Aplikuje se při spolupráci s citlivými informacemi.
Zákon č. 89/2021 Sb. (kybernetická bezpečnost)	Povinnosti v oblasti kybernetické bezpečnosti pro VŠ.
FAÚ — finanční analytický úřad	Posouzení podezřelých obchodních transakcí a protiprávního financování.

Aktuální seznam externích zdrojů a odkazů je průběžně aktualizován na webové stránce: https://www.uhk.cz/cs/univerzita-hradec-kralove/veda-a-vyzkum/nelegitimni-ovlivnovani

Tento manuál byl zpracován Prorektorkou pro vědu, výzkum a transfer znalostí UHK. Verze 1.1, 2026. Za aktualizaci a správu dokumentu odpovídá prorektorka pro vědu, výzkum a transfer znalostí.