VREDNOTE

1. Opredelite države in partnerske institucije, kjer je akademska svoboda ogrožena

- Kot prvo orientacijsko točko si oglejte svetovni **indeks akademske svobode** (Academic Freedom Index **-** AFi).
- Nato opravite bolj podrobno **oceno znanstvenega, izobraževalnega in institucionalnega okolja** v državi ter pri specifični partnerski organizaciji.
- Naknadno **analizirajte** še **motive** zunanjega partnerja za krnitev akademske svobode in spremljajte njegove **zmožnosti** omejevanja in/ali instrumentalizacije evropskih raziskovalcev in organizacij.

2. Z namenom razumevanja zunanjih pritiskov na akademsko svobodo in integriteto opravite oceno ranljivosti vaše institucije

- Izvedite **oceno ranljivosti** za posamezno institucijo in/ali projekt.
- Preverite ali obstoječe sodelovanje z zunanjimi akterji vodi v morebitne **odvisnosti**.
- Potrdite, da obstoječi **partnerski** sporazumi ustrezno varujejo akademsko svobodo.
- Spremljajte **zunanja imenovanja** in častne nazive vaših raziskovalk in raziskovalcev.
- Zagotovite **usposabljanja** za vse, ki prihajajo v stik z institucijami, kjer se pojavlja grožnja akademski svobodi in univerzalnim vrednotam.
- Vzpostavite mehanizem **poročanja**, ki bo omogočal evidentiranje groženj akademski svobodi v instituciji.

3. Okrepite zavezanost akademski svobodi in integriteti na institucionalni in individualni ravni

- Obravnavajte **specifične oblike ranljivosti**, ko jih prepoznate.
- Zagotovite **usposabljanja** za vse, ki prihajajo v stik z institucijami, kjer se pojavlja grožnja akademski svobodi in univerzalnim vrednotam.
- Vključite teme akademske svobode in integritete v **temeljne vsebine** vseh akademskih izobraževalnih programov.

- **Pogosto javno** utrjujte pomen akademske svobode in integritete.
- **Ozaveščajte** študente in zaposlene (akademsko in administrativno osebje) o pomenu in varovanju temeljnih akademskih vrednot
- **Podprite** akademsko osebje, ki raziskuje teme, ki jih želijo zunanji akterji zatreti.
- Uvedite **specializiran program podpore** za gostujoče akademsko osebje in študente, ki prihajajo iz držav, kjer je ogrožena akademska svoboda.
- Pomagajte **varovati preganjano akademsko osebje** ali študente z zagotovitvijo (začasnega) zatočišča.
- Razmislite o podpisu **zaveze za demokracijo**.

4. Nadaljujte sodelovanje s partnerji v represivnih okoliščinah

- Izogibajte se **stigmatizaciji ali odtujevanju** študentov, akademskega osebja in institucij, ki delujejo v neliberalnih institucionalnih okolji.
- **Krepite zavedanje** in **razumevanje** o tem na kakšen način represivne okoliščine vplivajo na akademsko svobodo.
- **Preučite standardne etične postopke**, da zagotovite, da tvegane raziskave v represivnih okoliščinah ne bodo samodejno zavrnjene (in na takšen način zatrte) s strani odgovornih komisij in teles.
- Zagotovite smernice in prirejeno tehnično podporo za na področju **podatkovne** in **digitalne varnosti**, da prispevate k obvladovanju tveganj nadzora v represivnih okoliščinah.
- Vzpostavite **postopke za ravnanje v nujnih primerih** nadlegovanja, pridržanja ali izginotja.
- Zavežite se mehanizmom **transparentnosti** in **preverjanja**, prilagojenim obravnavi sodelovanja z represivnimi okolji.

UPRAVLJANJE

1. Objavite kodeks ravnanja za tuje vmešavanje

- **Naj zagotavlja zaščito**:

- akademske svobode;
- varnosti podatkov in intelektualne lastnine;
- odličnosti in **odprtosti pri raziskovanju, poučevanju** in podpori učenju;
- etike, integritete in zaupanja.

- **Vključuje naj postopke za**:

- prepoznavanje tujega vmešavanja (vključno s kršitvami podatkov in etično neprimernimi raziskavami);
- zaščito žvižgačev;
- obravnavanje notranjih navzkrižij interesov.

2. Ustanovite odbor za tuje vmešavanje

- **Vključen v obstoječo institucionalno strukturo in odgovoren za**:

- **ozaveščanje** z izobraževanjem in usposabljanjem;
- spremljanje morebitnih tveganj;
- upravljanje raziskovalnih podatkov in intelektualne lastnine v mednarodnih sodelovanjih ter svetovanje in podporo vključenim raziskovalnim skupinam;
- obvladovanje in zmanjševanje tveganj;
- **preiskovanje** tujega vmešavanja.

PARTNERSTVA

1. Razvoj splošnih pogojev za uvedbo sistema za obvladovanje tveganj

- Odbor za preiskovanje tujega vmešavanja mora zagotoviti, da sta varnost znanja in akademska integriteta zaščiteni v vseh partnerstvih, tako da **pregleda postopke** ter jih po **potrebi razširi** in **okrepi**.
- Povečati je potrebno splošno **ozaveščenost** o morebitnih tveganjih, povezanih s sodelovanjem v partnerstvu, in o načinih, kako jih institucija poskuša **omiliti**.
- Zagotoviti podporo **strategiji obvladovanja tveganj**.
- Krepiti ozaveščenost in znanje s področja zakonodaje o nadzoru izvoza in **preverjanja neposrednih tujih naložb (FDI)**.
- Opredelite in zaščitite **"kronske dragulje"** institucije ter krepite razumevanje morebitnih tehnoloških, varnostnih in gospodarskih interesov tretjih držav.
- Opredelite merila za poročanje o načrtih za partnerstvo odboru za tuje vmešavanje in določite, kdo je **odgovoren za spremljanje** poročanja.
- Opredelite **minimalne standarde skrbnosti** za različne vrste partnerstev.
- Odbor za tuja vmešavanja lahko ustanovi **pododbor ali delovno skupino** za **obvladovanje tveganj**.

2. Vzpostavitev zanesljivega postopka za pripravo trdnih sporazumov o partnerstvu

- Razviti **pozitivno naravnan program**: opredeliti varna ali nizko tvegana področja mednarodnega sodelovanja.
- **Pripravite se na partnerstvo**: zagotovite, da temelji na strateški viziji kot delu internacionalizacije.
- Razvite dobro poznavanje partnerske organizacije, njenega mesta v nacionalnem raziskovalnem sistemu njene države.
- Izvedite skrbni pregled: zberite informacije, ki osebju omogočajo **oceno morebitnih tveganj** v zvezi z varnostjo, vrednotami in ugledom.
- **Skrbno se pogajajte** o partnerskem sporazumu: zagotovite pregledno razmejitev odgovornosti, vključno s finančnimi obveznostmi, pravicami intelektualne lastnine, upravljanjem podatkov in odprto znanostjo.

- **Spremljajte izvajanje sporazuma**: osredotočite se na vprašanja, povezana z morebitnim tujim vmešavanjem.
- Ocenite rezultate sodelovanja in se naučite, kaj je treba storiti za prihodnje sodelovanje.

KIBERNETSKA VARNOST

1. Ozaveščanje o tveganjih za kibernetsko varnost

- Razvite usposabljanje in organizirajte seminarje o vseh razpoložljivih in uporabljenih **tehnologijah za varstvo podatkov**, vključno z zaupnim računalništvom.
- **Izvedite izobraževanje in usposabljanje** raziskovalcev, študentov ter administrativnega in podpornega osebja na področju **kibernetske higiene**, da bi prepoznali tveganja in se znali izogniti kibernetskim napadom ali se z njimi spopasti.
- Razvite in objavite **enostavno izvedljive postopke eskalacije** v primeru suma kibernetskih napadov ter zagotovite prepoznavnost enotne kontaktne točke za triažo prijavljenih incidentov.
- Vzdržujte in sporočajte **seznam 10 največjih tveganj** kibernetske varnosti
- Redno objavljajte informacije z **opisi najboljših praks in incidentov** na področju kibernetske varnosti.

2. Odkrivanje in preprečevanje kibernetskih napadov s strani akterjev tujega vmešavanja

- Vzpostavite in redno izvajajte preiskave **odprtokodnih obveščevalnih podatkov (OSINT)** ter vzpostavite zmogljivosti za opozarjanje na odstopajoče vedenje.
- Razvite **postopke preverjanja** za raziskovalce ter administrativno in podporno osebje.
- **Nabavite opremo, certificirano za kibernetsko varnost**, in vlagajte v razvoj rešitev za zaščito zaupnosti podatkovnih zbirk, vključno z zaupnimi računalniškimi podatki.
- Izvedite **nadzor fizičnega dostopa**, ki ustreza zahtevani ravni.

- Razvite za grozd pisarne/korporativne dejavnosti **centraliziran pristop upravljanja** operacijskih sistemov in nameščenih aplikacij ter onemogočite in odstranite lokalne upravne pravice (LAR).
- Omogočite **dvofaktorsko avtentikacijo (2FA)** za dostop do kritičnih storitev in repozitorijev ter vzdržujte in uveljavljajte **sezname blokad** za prepoved dostopa do znanih zlonamernih spletnih strani ali spletnih strani, ki kršijo avtorska prava.

3. Odziv na kibernetske napade, zaradi tujega vmešavanja in okrevanje po njih:

- Razvijajte **zmogljivosti situacijskega zavedanja** z izmenjavo pridobljenih izkušenj in posodabljanjem skupnih črnih list, sistemov ugleda in podatkovnih zbirk.
- Razvite **načrt za obravnavo incidentov**, ki vključuje jasne postopke, v katere so vključene tako prizadete strani kot tudi tisti, ki se morajo odzvati. Prevzemite prakse in elemente iz modelov za obvladovanje incidentov, kot je **model za obvladovanje varnostnih incidentov (Security Incident Managament Maturity Model - SIM3)**.
- Krepite zmogljivosti **forenzične pripravljenosti**, da skrajšate čas za odziv.
- Sprejmite **disciplinske ukrepe** za osebje, ki je storilo prekršek, in pri tem vključite dokaze **iz digitalne preiskave**.
- V incidente vključite ustrezne **organe pregona**, **nacionalne obveščevalne** in **varnostne agencije**, **urade za intelektualno lastnino** in **organe za varstvo podatkov**.