VŠ: Masarykova univerzita

Rozvojový projekt na rok 2021

Formulář pro centralizované rozvojové projekty

Tematické zaměření: (vyberte pouze jedno)	**f) plnění požadavků stanovených obecně závaznými právními předpisy nebo pokyny orgánů státní správy**

Název projektu:

Zvýšení úrovně kybernetické bezpečnosti v prostředí VVŠ

Období řešení projektu:	**Od: 1.1.2021**	**Do: 31.12.2021**

Požadavek na dotaci ze státního rozpočtu v roce 2021 ukazatel I (v tis. Kč):

	Celkem:	**V tom běžné finanční prostředky:**	**V tom kapitálové finanční prostředky:**
Na celý projekt (vyplní pouze koordinátor)	15 700	15 700	0
Na dílčí část předkládající VŠ	2 700	2 700	0

ZÁKLADNÍ INFORMACE

Koordinátor celého projektu

Jméno	**RNDr. Miroslav Bartošek, CSc.**
VŠ	**Masarykova univerzita**

Zúčastněné VŠ:	01 Akademie múzických umění v Praze (AMU) 02 Akademie výtvarných umění v Praze (AVU) 03 Česká zemědělská univerzita v Praze (ČZU) 04 České vysoké učení technické v Praze (ČVUT) 05 Janáčkova akademie múzických umění v Brně (JAMU) 06 Jihočeská univerzita v Českých Budějovicích (JU) 07 Masarykova univerzita (MU) 08 Mendelova univerzita v Brně (MENDELU) 09 Ostravská univerzita (OU) 10 Slezská univerzita v Opavě (SU) 11 Technická univerzita v Liberci (TUL) 12 Univerzita Hradec Králové (UHK) 13 Univerzita J. E. Purkyně v Ústí nad Labem (UJEP)	14 Univerzita Karlova (UK) 15 Univerzita Palackého v Olomouci (UP) 16 Univerzita Pardubice (UPa) 17 Univerzita Tomáše Bati ve Zlíně (UTB) 18 Veterinární a farmaceutická univerzita Brno (VFU) 19 VŠB – Technická univerzita Ostrava (VŠB-TUO) 20 Vysoká škola ekonomická v Praze (VŠE) 21 Vysoká škola chemicko-technologická v Praze (VŠCHT) 22 Vysoká škola polytechnická Jihlava (VŠPJ) 23 Vysoká škola Technická a ekonomická v Českých Budějovicích (VŠTE) 24 Vysoké učení technické v Brně (VUT) 25 Západočeská univerzita v Plzni (ZČU)

	Řešitel předkládané dílčí části	**Kontaktní osoba**
Jméno:	RNDr. Miroslav Bartošek, CSc.	Mgr. Zuzana Řepišová
VŠ:	Masarykova univerzita	
Adresa/Web:	Žerotínovo nám. 9, 601 77 Brno; https://www.muni.cz	
Telefon:	549 49 2109	549 49 6456
E-mail:	bartosek@ics.muni.cz	repisova@ics.muni.cz

Vyplní pouze koordinátor projektu

<table>
<tr><td></td><td colspan="2">CHARAKTERISTIKA CELÉHO PROJEKTU</td></tr>
<tr><td>Anotace a popis celého projektu
(max. 1 800 znaků vč. mezer)</td><td colspan="2">Projekt je zaměřen na podporu nastavení a zvýšení úrovně kybernetické bezpečnosti (KB) na 25 veřejných vysokých školách. Tato vysoce aktuální potřeba je naléhavá v souvislosti s trvalým růstem KB hrozeb obecně, a ve zranitelných dobách souvisejících s celosvětovou pandemií zvláště. Nastavení kyberochrany je podmínkou pro širší elektronizaci a nasazení postupů pro distanční fungování vysoké školy. S výjimkou několika málo univerzit, které mají ustanoveny KB-týmy a základní procesy, je většina VVŠ v této oblasti na tom bídně. Cílem projektu je využít zkušeností a odborných kapacit vyspělejších univerzit, aby připravily metodiky a doporučení pro VVŠ různých velikostí, které umožní všem, i těm méně připraveným, zásadním způsobem zvýšit úroveň jejich kybernetické bezpečnosti. Vedle zlepšení situace v kyberochraně je neméně důležitým úkolem připravit vysoké školy na plnění zákonných povinnosti, které jim ukládá Zákon o kybernetické bezpečnosti (dále jen ZoKB), zejména co se týká významných informačních systémů orgánů veřejné moci. Je přirozeným požadavkem, aby vysoké školy postupovaly v tomto ohledu jednotným a synchronizovaným způsobem, ať už se to týká výkladů, rozsahu závazků a povinností (které by neměly být pro VVŠ nadměrně extenzivní a zatěžující), tak i harmonogramu potřebných kroků (který by měl být zvladatelný i pro nezkušené). Po věcné stránce se řešení projektu zaměřuje do 4 oblastí, pro které budou ustanoveny odborné pracovní skupiny pod vedením zkušených expertů: nastavení bezpečného kyberprostředí univerzity, významné informační systémy v prostředí VVŠ, osvěta uživatelů a systematické institucionální vzdělávání zaměstnanců, právní aspekty KB.</td></tr>
<tr><td>Přehled o řešení projektu v roce 2020</td><td colspan="2">Nejedná se o projekt pokračující z roku 2020</td></tr>
<tr><td></td><td>Cíle stanovené v návrhu projektu</td><td>Plnění plánovaných cílů a kontrolovatelných výstupů k datu předání této žádosti</td></tr>
<tr><td></td><td>Cíl</td><td></td></tr>
<tr><td></td><td>Cíl</td><td></td></tr>
<tr><td></td><td>Přehled čerpání finančních prostředků k datu předání této žádosti</td><td>Projekt financován od</td></tr>
<tr><td></td><td colspan="2">n/a</td></tr>
<tr><td>Zdůvodnění projektu/ analýza potřeb/ popis současného stavu oblasti, na kterou je projekt zaměřen.</td><td colspan="2">Trendy posledních let ukazují prudký nárůst kyberbezpečnostních hrozeb, které ohrožují stále více spolehlivou funkci, dostupnost, integritu, důvěryhodnost a bezpečnost infrastruktury, informačních systémů a datových zdrojů všech organizací, vysoké školy nevyjímaje. Jen Masarykova univerzita řešila v roce 2019 celkem 546 závažných kyberbezpečnostních incidentů vyžadujících manuální zásah členů kyberbezpečnostního týmu CSIRT-MU (vedle toho detekovala přes 100 tisíc dalších pokusů o kybernetický útok, které byly řešeny pomocí automatizovaných nástrojů/automatickou ochranou). Tyto neblahé trendy byly ještě umocněny v obzvláště zranitelném období koronavirové krize v první polovině letošního roku, jak o tom svědčí mj. masivní kybernetické útoky na nemocnice a další zařízení jak v ČR, tak i po celém světě. Jasně se ukazuje, že schopnost vysokých škol aktivně čelit těmto hrozbám je klíčová pro zajištění jejich dalšího fungování. Rychlý průzkum provedený předkladateli projektu dokládá, že jen malá část univerzit má vybudovány potřebné kapacity, postupy a zkušenosti pro zajištění své kyberbezpečnosti. Většina VVŠ zatím není na nebezpečí v této oblasti dostatečně připravena a často se tato problematika nedostala ani do centra pozornosti vedení. Současná legislativa řadí univerzity mezi orgány veřejné moci, a na základě určujících kritérií ve vyhlášce č. 360/2020 Sb. (o významných informačních systémech a jejich určujících kritériích) mezi povinné subjekty dle zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti, ZoKB). To klade na vysoké školy řadu povinností, se kterými se budou muset vypořádat. Dalším důležitým aspektem projektu jsou nové výzvy související s bezpečným přechodem škol na distanční vzdělávání a provoz, který urychlila koronavirová pandemie. V souvislosti se zajištěním kybernetické bezpečnosti tak stojí vysoké školy před celou řadou problémů a výzev, které je třeba efektivně řešit.</td></tr>
<tr><td>Cíl projektu.
Popis cílového stavu, kterého má být řešením projektu dosaženo.</td><td colspan="2">Cílem projektu je vytvořit metodiky a postupy pro zvýšení úrovně kybernetické bezpečnosti na veřejných vysokých školách v ČR, které budou reflektovat potřeby a možnosti jednotlivých škol. Součástí toho bude také příprava na plnění povinností pro provozovatele a správce významných informačních systémů podle ZoKB, vytvoření systému pro osvětu a vzdělávání zaměstnanců a studentů v oblasti kyberbezpečnosti. Vzhledem k různorodosti VVŠ budou připravena variantní řešení umožňující nasazení doporučených postupů a metodik podle potřeb jednotlivých VVŠ.</td></tr>
</table>

Popis cílové skupiny. Uveďte a popište cílovou skupiny (příp. cílové skupiny), pro kterou je projekt určen.	Výstupy projektu se dotknou v té či oné míře všech cílových skupin na vysoké škole. Zejména pak: - Kyberbezpečnostních týmů a manažerů kybernetické bezpečnosti VVŠ - Vedení VVŠ - Správců a provozovatelů infrastruktury a informačních systémů - Zaměstnanců - Studentů

Výstupy celého projektu		
Definujte konkrétní a měřitelné výstupy projektu, které budou výsledkem projektu.	č.	**Výstup projektu** (přidejte řádky podle potřeby)
	1	Analýza stavu KB na VVŠ
	2	Metodiky, personální a procesní rámec pro KB na VVŠ
	3	Nastavení základní úrovně bezpečnosti kyberprostředí na jednotlivých VVŠ
	4	Identifikace, kategorizace a analýza významných informačních systémů (VIS) v prostředí VVŠ
	5	Doporučení a postupy k naplnění povinnosti správce a provozovatele VIS
	6	Metodika analýzy dopadů
	7	Příprava prostředí VVŠ pro splnění zákonných opatření plynoucích ze ZoKB
	8	Osvětové materiály pro KB
	9	Nastavení systematické KB osvěty na jednotlivých VVŠ
	10	Kurzy KB pro školení zaměstnanců
	11	Implementace KB-kurzů do systému vzdělávání zaměstnanců jednotlivých VVŠ
	12	Workshopy pro klíčové oblasti řešení
	13	Závěrečná zpráva řešení projektu za rok 2021, včetně návrhu dalšího postupu pro rok 2022

Popis činností projektu					
Pro každý výstup identifikujte hlavní činnosti, které povedou k jeho naplnění v harmonogramu.	č.	**Hlavní činnosti** (přidejte řádky podle potřeby)	**Termín zahájení**	**Termín ukončení**	**Číslo výstupu**
	1	Příprava metodik a nástrojů pro analýzy aktuálního stavu KB ve VŠ prostředí (analýza personálního a procesního nastavení KB na VVŠ, analýzy osvěty a vzdělávání zaměstnanců v KB)	1.1.	31.1.	1
	2	Průzkum aktuálního stavu na jednotlivých VVŠ; zpracování souhrnných analýz jako východisek pro další opatření; kategorizace VVŠ z pohledu možností a potřeb nastavení základní úrovně KB	1.2.	31.3.	1
	3	Příprava manuálu pro vznik KB týmu VVŠ a definice jeho základních služeb; definice základních procesů pro identifikaci, řešení a komunikaci KB incidentů; vytvoření vzorů legislativních opatření pro nastavení základní úrovně KB v prostředí VVŠ; definice vzorové struktury Bezpečnostní dokumentace	1.1.	30.6.	2
	4	Vytvoření a legislativní ustanovení KB týmů na VVŠ, kde toto dosud neproběhlo	1.3.	30.6.	3
	5	Implementace základních procesů a opatření: univerzitní kyberbezpečnostní směrnice; identifikace, řešení a komunikace incidentů, a dalších	1.5.	31.12.	3
	6	Zpracování právních analýz povinností VVŠ dle ZoKB, včetně analýz k určování významných informačních systémů dle současné legislativy	1.1.	31.12.	2-7

7	Příprava metodiky pro jednotnou identifikaci VISů v prostředí VVŠ; konzultace s NÚKIB	1.1.	31.3.	4
8	Identifikace a zpracování soupisů VISů na jednotlivých VVŠ	1.1.	30.10.	4
9	Doporučení na stanovení rozsahu SŘBI – pro malou, střední a velkou univerzitu; metodika identifikace, hodnocení a evidence aktiv; vzorový katalog hrozeb a zranitelností pro VVŠ; metodika provádění analýzy rizik; zpracování dalších doporučení a vzorů	1.1.	30.9.	5
10	Vytvoření metodiky pro analýzu dopadů (BIA) pro VVŠ; dotazníkový průzkum mezi VVŠ k analýze dopadů a jeho zpracování	1.3.	30.6.	6
11	Konzultace a workshopy k podpoře VVŠ při přípravě prostředí pro splnění zákonných opatření plynoucích ze ZoKB	1.4.	31.12.	7
12	Specifikace cílových skupin pro KB osvětu a identifikace jejich potřeb; příprava vzdělávacích materiálů pro jednotlivé cílové skupiny; zpracování osvětových článků a podpůrných materiálů na vybraná témata. Zpracování metodiky pro zavádění systematické osvěty a návrhu vzorových procesů zajištění rozvoje KB povědomí	1.1.	30.6.	8
13	Nastavení procesů KB osvěty jednotlivých VVŠ; disseminace vytvořených materiálů; adaptace generických osvětových článků a jejich zveřejnění ve vybraných publikačních kanálech VVŠ s širokým dopadem	1.6.	31.12.	9
14	Příprava vzorového kurzu KB v podobě adaptovatelné pro různé vzdělávací platformy	1.1.	30.5.	10
15	Adaptace vzorového kurzu pro lokální prostředí a potřeby jednotlivých VVŠ (obsah, platforma); doplnění specifických informací a odkazů na konkrétní vnitřní předpisy, procesy a informační systémy. Implementace konkrétních kroků pro zavedení periodického školení zaměstnanců v KB dle aktuálních možností a potřeb dané organizace	1.6.	31.12.	11
16	Pořádání interních workshopů k implementaci doporučení a metodik připravených jednotlivými pracovními skupinami do prostředí VVŠ a výměně zkušeností; osvětové workshopy za účasti zástupců NÚKIB	1.1.	31.12.	12
17	Zpracování závěrečné zprávy projektu, zhodnocení průběhu řešení a naplnění plánovaných výstupů; vize další spolupráce VVŠ v roce 2022	1.10.	31.12.	13

Vztah projektu k prioritám Strategickému záměru ministerstva a Plánu realizace Strategického záměru pro rok 2021	Zajištění důvěrnosti, integrity a dostupnosti informací a dat v elektronické podobě je nezbytnou podmínkou pro spolehlivé fungování informační a komunikační infrastruktury vysokých škol a jejich informačních systémů. Z tohoto pohledu je kybernetická bezpečnost klíčové průřezové téma pro všechny prioritní oblasti využívající IT podporu, a to jak v oblasti vzdělávání, tak při zajištění provozu vysokých škol. Speciální pozornost zasluhuje ochrana a bezpečnost infrastruktury, systémů a nástrojů vysokých škol pro rozvoj flexibilních forem vzdělávání stejně jako provozních činností zajišťovaných distančními metodami – ať již jako reakce na akutní potřeby v době pandemie nebo všeobecný trend k vyšší efektivitě ve vzdělávacích, administrativních a provozních činnostech.
Zdůvodnění řešení projektu ve spolupráci zapojených VŠ. Popis synergického efektu společného řešení.	Problematika zajištění kyberbezpečnosti v tak složitém prostředí, jaké představuje vysoká škola (rozsáhlá infrastruktura, vysoký počet a různorodost typů uživatelů, počet, rozsah a významnost informačních systémů) je výzvou, kterou většina VVŠ není schopna plně obsáhnout jen vlastními silami. Přitom navzdory různorodosti škol má většina problémů stejnou povahu, takže spojení sil a synergie ze společného řešení je přirozeným a nutným východiskem pro dosažení maximálního efektu s omezenými dostupnými zdroji. Řešení a nastavování kyberbezpečnosti není jednorázovou záležitostí, jedná se o trvalý a repetitivní úkol, který bude i do budoucna vyžadovat součinnost a spolupráci vysokých škol. Náročnost tohoto úkolu podtrhuje také dynamika vývoje a permanentně vznikající nové typy hrozeb související s rychlým vývojem technologií a sofistikovaností útočníků. Předkladatelé projektu mají velmi pozitivní zkušenost s obdobným projektem CRP 2018 na zavádění GDPR na VVŠ (č. C11-2018), odkud mohou čerpat osvědčené postupy a zkušenosti.

Stručná charakteristika	**Název VŠ (zkratka)**	**Popis zapojení**

zapojení jednotlivých VŠ do řešení projektu (přidejte řádky dle počtu zapojených VŠ)	AMU	V projektu budeme řešit základní zpracování požadavků v oblasti nastavení kyberbezpečnosti na AMU. Provedeme analýzu stavu a identifikaci významných informačních systémů a s tím související přípravu pro splnění požadavků stanovených obecně závaznými právními předpisy nebo pokyny orgánů státní správy. Zahájíme kyberbezpečnostní osvětu a vzdělávání zaměstnanců a studentů. Navazovat bude zpracování popisu změny procesů, inovace vnitřní legislativy a školení zainteresovaných zaměstnanců.
	AVU	AVU byla v roce 2020 objektem cíleného hackerského útoku – a jak se ukázalo, nebyla na takovou situaci připravena. Cílem našeho zapojení je tedy nastavit systém řízení kybernetické bezpečnosti na AVU včetně jejích přidružených pracovišť, který bude reflektovat specifika malé umělecké VŠ a nové trendy v zajištění výuky, zejména rozšíření distanční výuky. Pro AVU bude klíčové efektivní nastavení cílů, procesů, rolí a odpovědností v systému outsourcingu významné části správy IS AVU. AVU se musí současně zaměřit na zvládání kybernetické bezpečnosti v systému malého IT oddělení.
	ČZU	V projektu se Česká zemědělská univerzita v Praze zaměří na analýzu a nastavení oblasti kybernetické bezpečnosti a vlastní aplikování v prostředí univerzity. Základem je analyzovat současný stav v rámci personálního, procesního a legislativního nastavení. Hlavním cílem bude realizace minimálních požadavků podle Zákona o kybernetické bezpečnosti v průniku s ISMS. Důležitá bude aktualizace vlastních směrnic a nastavení online kurzů a osvěty pro zaměstnance univerzity.
	ČVUT	ČVUT jako partner s bohatými zkušenostmi se zaváděním ISO standardů v oblasti kyberbezpečnosti bude koordinovat přípravu a nasazování doporučení a metodik v rámci pracovní skupiny PS-2, se speciálním důrazem na oblast významných informačních systémů v prostředí VVŠ.
	JAMU	JAMU patří v rámci ČR k menším VVŠ, její kapacity pro tvorbu vlastních analýz, řešení či zapojení do řešitelských týmů jsou velmi omezené. Náš přínos k celkovému výstupu z projektu proto spatřujeme především v testování, konzultacích a výměně zkušeností na poli využití aplikací z prostředí O365 v distanční výuce i běžné praxi a sdílení poznatků nabytých školením správců v uvedených oblastech.
	JU	Jihočeská univerzita v Českých Budějovicích se v rámci projektu zaměří na zpracování soupisu významných infomačních systémů školy, analýzu aktuálního stavu kyberbezpečnosti na univerzitě a zavedení opatření pro zvýšení kyberbezpečnosti. Chceme se zaměřit hlavně na osvětu a pravidelné školení zaměstnanců, protože lidský faktor je určitě významný zdroj bezpečnostních rizik. Vývoj a úpravy software a jeho následná implementace bude řešena dodavatelsky.
	MU	MU je koordinující školou tohoto projektu se zodpovědností za průběh řešení a naplnění plánovaných cílů a výstupů. Vedle toho je vedoucím tří ze sedmi pracovních skupin projektu (viz níže, Organizace a řízení projektu), a to konkrétně PS-1, PS-3 a PS-7. Díky svým rozsáhlým expertním zkušenostem na poli kyberbezpečnosti (sahajícím až do roku 2007, CSIRT-MU od roku 2009, Kybernetický Polygon od 2013, první certifikovaný bezpečnostní tým v ČR v roce 2016, dlouhodobá spolupráce s NÚKIB) bude připravovat nebo koordinovat většinu společných výstupů a sdílení dobré praxe s ostatními účastníky projektu. Přímo uvnitř MU se chceme zaměřit mj. na implementaci systematického školení zaměstnanců v KB včetně jeho podpory v interní legislativě a dopracování, resp. zefektivnění systému provozní kyberbezpečnosti. Specifickým úkolem bude také zvýšení zabezpečení prostředí O365.
	MENDELU	Mendelova univerzita v Brně potřebuje aktivně zvýšit povědomí o kyberbezpečnosti napříč jednotlivými skupinami uživatelů ICT. V projektu si vytyčila cíle zmapovat aktuální situaci na jednotlivých součástech univerzity, navrhnout a implementovat základní legislativu, vytvořit a implementovat systém vzdělávání v oblasti kybernetické bezpečnosti pro zaměstnance. Jedním z nástrojů pro získání analýzy stavu jsou penetrační testy, které by univerzita v rámci projektu chtěla realizovat. Aktivně přispět bychom chtěli v oblasti školení a vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti.
	OU	Ostravská univerzita chce především nabídnout zapojeným vysokým školám vlastní zkušenosti se zajišťováním kyberbezpečnosti – příkladem budiž vybudování vlastního CSIRT týmu a jeho úspěšného zapojení do TF-CSIRT. Dále se budeme aktivně podílet na právních analýzách relevantní legislativy (zejména ZoKB a souvisejících vyhlášek) i na hledání nejschůdnějších způsobů, jak dostát zákonným povinnostem, proto je členem realizačního týmu právník a zároveň pověřenec pro ochranu osobních údajů OU. Na vnitrouniverzitní úrovni se zaměříme na dobudování a vylepšení nastavení interních kyberbezpečnostních procesů a přípravu na plnění povinností ze ZoKB.
	SU	Slezská univerzita v Opavě má za cíl zvýšit úroveň své kybernetické bezpečnosti. S podporou tohoto projektu provedeme nejprve detailní analýzu současného stavu na několika úrovních. Kromě vyhodnocení nastavení systémových prostředků budeme řešit také úroveň vnitřní legislativní podpory a usilovat o zvýšení osvěty mezi uživateli, zejména pak vzděláváním zaměstnanců. Důležitou součástí řešení bude mj. nastavení procesů pro identifikaci, odstranění a komunikaci bezpečnostních incidentů, soupis významných informačních systémů a k nim související opatření pro splnění zákonných povinností.

	TUL	Pro TUL je řešení kyberbezpečnostní ochrany prioritním úkolem, potřebujeme řešit všechny oblasti plánované v projektu. Budeme se podílet v rámci našich kapacit ne činnosti pracovních skupin a následné adaptaci jejich výstupů pro nasazení v podmínkách naší univerzity.
	UHK	V současnosti Univerzita Hradec Králové obdobně jako ostatní VVŠ, denně řeší nové formy sofistikovaných útoků na informační systémy i provozovanou infrastrukturu. Jelikož aktuálně nemáme pro oblast kybernetické bezpečnosti vyčleněného specialistu a velikost celoškolského Oddělení informačních technologií UHK nemá dostatečnou kapacitu na tvorbu vzdělávacích materiálů a individuální školení uživatelů, vítáme inciativu sdílení dobré praxe a sdílení osvětových a vzdělávacích materiálů vytvořených v projektu a uvedené následně aktivně využijeme v prostředí Univerzity Hradec Králové.
	UJEP	Pro UJEP je klíčové z důvodu absence právnické fakulty převzetí dobré praxe z univerzit, které mají specializované právnické analytické kapacity, aby vystupovala jednotně s ostatními univerzitami v České republice v oblasti kybernetické bezpečnosti. Začlenění požadavků týkajících se kyberbezpečnosti do struktur univerzity po stránkách organizačních, procesních a provozních. Vytvoření směrnice a metodiky pro práci v oblasti kyberbezpečnosti pro organizační začlenění s definováním potřebných procesů pro zpracování chodu kyberbezpečnosti, tak zadefinování použitelných nástrojů pro provozní dohled nad infrastuktrurou a informačními systémy univerzity, zjišťování incidentů, logování událostí.
	UK	UK jako největší česká VVŠ s největší uživatelskou základnou a spektrem informačních systémů je přirozeným atraktorem pro kyberbezpečnostní útoky. Aktuální stav ochrany není zdaleka optimální, takže potřebujeme řešit na UK všechny body projektu. Aktivně se chceme zapojit do řešení společných částí projektu zejména v rámci pracovních skupin PS-1 a PS-3.
	UP	UP se bude podílet formou konzultací, připomínkování a přebírání příkladů dobré praxe pro zdokonalení nastavení kyberbezpečnostní ochrany na univerzitě. V rámci výstupu č. 3 předpokládá UP provedení penetračních testů infrastruktury.
	UPa	UPa se aktivně zúčastní na jednotlivých činnostech projektu. V úvodu řešení projektu se zaměří na analýzu stavu kyberbezpečnostního prostředí na UPa, dále zpracuje soupis svých VIS a ve spolupráci s ostatními VVŠ se zaměří na nastavení procesů dle ZoKB. Velkým přínosem projektu pro UPa bude vytvoření vzdělávacích materiálů a nastavení periodických online školení všech zaměstnanců UPa.
	UTB	UTB plánuje zapojení svého řešitelského týmu do všech pracovních skupin projektu s cílem řešit splnění minimálních zákonných povinností na UTB podle ZoKB pro oblast významných informačních systémů, nastavit interní procesy, připravit odpovídající vnitřní normy a vzdělávací materiály pro všechny cílové skupiny na univerzitě.
	VFU	VFU Brno počítá v rámci projektu s analýzou stávajícího stavu KB na naší univerzitě, a to vč. analýzy používání IS a forem distanční výuky ve vztahu ke KB, počítáme s nastavením KB v našem prostření, seznámení zaměstnanců s KB, a dále – a to je velmi důležité – sdílení těchto poznatků s ostatními VŠ, protože prostředí VŠ a jejich specifika sebou přináší i specifická řešení.
	VŠB-TUO	Vysoká škola báňská – Technická univerzita Ostrava se zapojí do velké části projektu, především v oblastech týkajících se analýzy stavu bezpečnosti, nastavení prostředí odpovídají požadavkům ZoKB, včetně identifikace významných informačních systémů dle tohoto zákona. Bude se podílet na tvorbě kurzů pro bezpečností osvětu a vzdělávání zaměstnanců. Aktivně bude vést pracovní sekci týkající se návrhu postupů a pravidel při Analýze rizik a následném sestavování bezpečnostních plánů.
	VŠE	Zapojení do analytických prací (stav kyberbezpečnosti, identifikace VIS a jejich analýzy); vytváření bezpečnostní dokumentace včetně směrnic; testování uživatelů pomocí simulovaných phisingových útoků; adaptace a převzetí doporučení a dalších výstupů projektu do prostředí VŠE; vytvoření kontrolního seznamu úkolů pro dosažení souladu se ZoKB pro VIS na škole a jeho postupné naplňování. Zavedení systematické osvěty a vzdělávání v KB.
	VŠCHT	Projekt se zaměří na vylepšení stávající úrovně bezpečnosti kyberprostředí na VŠCHT. Mezi stěžejní oblasti řešení bude patřit mj. oblast vzdělávání v kyberbezpečnosti (včetně testování vytvořených generických kurzů a jejich přizpůsobení do lokálních podmínek školy), vytvoření a legislativní ustanovení KB týmu, adaptace a implementace doporučení pracovních skupin projektu. Do společných výstupů budeme přispívat vlastními analýzami ve vybraných oblastech.
	VŠPJ	Na VSPJ chceme v rámci dílčího projektu provést implementaci výstupů z hlavních částí projektu a zpřístupnit vytvořené výukové materiály. Také chceme provést externí bezpečnostní analýzu k vyhledání KB zranitelností a v reakci na tuto analýzu provést zlepšení bezpečnosti. Ze zbývajících finančních prostředků bychom chtěli zajistit školení pro realizační tým ke zvýšení odbornosti v oblasti KB.

	VŠTE	VŠTE se v projektu zaměří především na analyzování současného stavu kybernetické bezpečnosti v prostředí školy a její prevenci. Dále v rámci projektu dojde k vytvoření vzdělávacího modulu v mobilní aplikaci, která je v prostředí VŠTE významným komunikačním nástrojem. Modul aplikace bude sloužit jako nástroj pro zvyšování znalostí a gramotnosti zaměstnanců a studentů v oblasti kyberbezpečnosti. Modul se po implementaci kurzu o KB stane i součástí proškolování zaměstnanců při vstupu do pracovního poměru u pozic, jenž práci na PC předpokládá. Skrze aplikaci také dojde k nastavení systematické osvěty na prostředí VŠTE. Dalším krokem bude procesní nastavení a implementace minimální úrovně zabezpečení dle ZoKB.
	VUT	VUT jako jedna z mála VŠ s praktickými zkušenostmi s provozováním vlastního CSIRT týmu bude v projektu spolupracovat zejména na úkolech PS-1 a PS-3; zaměřit se chceme i na efektivní využívání dostupných systémů pro automatickou detekci kyberbezpečnostních zranitelností.
	ZČU	ZČU v rámci aktivit projektu provede revizi a vylepšení procesů a interní legislativy v oblasti kybernetické bezpečnosti včetně klasifikace informačních systémů univerzity z hlediska ZoKB a z toho plynoucích povinností správce a provozovatele. Kromě popsaných společných aktivit se v projektu chceme zvláště zaměřit na návrh optimálního systému pro organizaci elektronického vzdělávání zaměstnanců. Získané výstupy využijí i ostatní členové projektu pro zlepšení svých systémů vzdělávání zaměstnanců.

Organizace a řízení projektu
Charakterizujte řízení projektu, rozdělení kompetencí, případně role jednotlivých partnerů, mechanismy průběžné kontroly realizace projektu.

Realizace projektu bude probíhat v rámci řídicí skupiny zodpovídající za celkový průběh projektu a pracovních skupin garantující řešení a výstupy projektu ve stanovených oblastech.

Řídicí skupina:
Zodpovídá za celkový průběh, směrování a koordinaci projektu, kontroluje plnění stanovených cílů a výstupů, sleduje naplňování harmonogramu a provádí jeho případné korekce. Vedle koordinátora celého projektu jsou v řídicí skupině zastoupeni vedoucí jednotlivých pracovních skupin a řešitelé všech dílčích projektů (zastupujících jednotlivé VVŠ zapojené v projektu). Schází se obvykle jednou za čtvrtletí. Zodpovídá za výstupy 12 a 13.

Pracovní skupiny projektu:

- **PS-1: Nastavení bezpečného kyberprostředí**
  Koordinuje MU. Zodpovídá za výstupy 1, 2, 3
- **PS-2: Významné informační systémy v prostředí VVŠ**
  Koordinuje ČVUT. Zodpovídá za výstupy 4, 5, 6, 7
- **PS-3: Osvěta a vzdělávání uživatelů**
  Koordinuje MU. Zodpovídá za výstupy 8, 9, 10, 11
- **PS-7: Právní aspekty KB v prostředí VVŠ**
  Koordinuje MU. Zpracovává právní analýzy a právní podporu pro potřeby Řídicí skupiny a pracovních skupin 1-3

Partneři koordinující pracovní skupiny mají dlouholeté odborné i praktické zkušenosti se svěřenou oblastí a disponují interní týmy s potřebnými expertními znalostmi. Na MU a také ČVUT působí již řadu let kyberbezpečnostní týmy CSIRT/CERT zajišťující klíčové činnosti v oblasti kyberbezpečnosti. Partneři, kteří nekoordinují přímo některou pracovní skupinu se zapojují do činnosti PS podle svých kompetencí a účastní se workshopů.

Realizační tým			
Uveďte plán personálního zajištění	**č.**	**Jména klíčových lidí** (přidejte řádky podle potřeby)	**Činnosti**
	1	RNDr. Miroslav Bartošek, CSc. – MU	Koordinátor projektu. Celkové řízení projektu, plnění cílů, koordinace činností a výstupů. Řešitel dílčí části za MU.
	2	Bc. Tomáš Plesník – MU	Koordinátor pracovní skupiny PS-3. Jako vedoucí CSIRT-MU s bohatými expertními i provozními zkušenostmi bude garantovat odbornou kvalitu a věcnou správnost řešení projektu, a také návaznosti mezi jednotlivými odbornými PS.
	3	RNDr. Michal Javorník, Ph.D. – MU	Koordinátor PS-1: řízení pracovní skupiny, koordinace a garance plánovaných výstupů.
	4	RNDr. Michal Růžička. Ph.D. – MU	Analýzy a doporučení v oblasti bezpečnostních technologií.
	5	Mgr. Zuzana Řepišová – MU	Administrativa celého projektu.

	6	JUDr. Mgr. Jakub Harašta, Ph.D. – MU	Vedení a koordinace PS-7, zpracování právních analýz a doporučení, právní konzultace všem PS, legislativní otázky.
	7	RNDr. Martin Laštovička – MU	Odborný pracovník Skupiny reakce na incidenty CSIRT-MU. Příprava metodik a doporučení v rámci PS-1. Podpora kyberbezpečnostním týmům partnerů projektu.
	8	Mgr. Richard Kalinec – MU	Odborný pracovník Skupiny reakce na incidenty CSIRT-MU. Příprava metodik a doporučení v rámci PS-1. Podpora kyberbezpečnostním týmům partnerů projektu.
	9	Mgr. Tomáš Marek – MU	Příprava osvětových materiálů a plánů jejich disseminace v rámci PS-3.
	10	Mgr. Břetislav Regner – MU	Analytické práce a doporučení pro oblast zvýšení zabezpečení prostředí O365.
	11	Jan Izydorzcyk – MU	Analytické práce a doporučení pro oblast bezpečnosti distančních nástrojů se zaměřením na nástroje O365.
	12	Další pracovníci CSIRT-MU	Analytické práce, příprava metodik a doporučení.
	13	Ing. Václav Obadálek – AMU	Řízení dílčí části projektu, příprava pro splnění zákonných opatření plynoucích za ZoKB.
	14	Bc. Tomáš Jungwirth – AMU	Analýza aktuálního stavu, nastavení úrovně bezpečnosti kyberprostředí, identifikace a analýza VIS.
	15	Jiří Krčmář – AMU	Implementace kurzu pro kyberbezpečnostní vzdělávání zaměstnanců.
	16	Tomáš Holý – AMU	Nastavení kyberbezpečnostní osvěty, doporučení pro nasazení nástrojů pro distanční vzdělávání.
	17	Evžen Mrázek – AVU	Řízení dílčího projektu.
	18	Tomáš Kuchař – AVU	Koordinátor za hlavní činnosti 1-9, řešitel 1-9.
	19	Jozef Tamók – AVU	Řešitel dílčích výstupů 1,3,6.
	20	Ing. Jiří Richter – ČVUT	Řízení dílčí části projektu, dílčí práce na přípravě metodik, doporučení a vzorů, konzultace s NÚKIB. Implementace bezpečnostních opatření, identifikace a hodnocení VISů.
	21	Ing. Radek Holý, Ph.D. – ČVUT	Zpracování podkladů pro analýzu aktuálního stavu KB. Konzultace a workshopy k podpoře VVŠ, příprava metodik. Zpracování hodnocení VISů.
	22	Ing. Radek Trousílek – ČVUT	Zpracování podkladů pro analýzu aktuálního stavu KB. Dílčí práce na přípravě doporučení a vzorů, konzultace a workshopy. Identifikace VISů.
	23	Ing. Robert Schindler, MSc. – ČVUT	Odborné práce na přípravě metodik, doporučení a vzorů, konzultace s NÚKIB.
	24	Ing. Jan Borák Ph.D. – ČZU	Řízení dílčí části projektu.
	25	Ing. Petr Hanzlík Ph.D. – ČZU	Spolupráce na projektu.
	26	Ing. Petr Vlachynský – ČZU	Spolupráce na projektu.
	27	Ing. Vlastislav Tůma – ČZU	Spolupráce na projektu.
	28	Ing. Marek Kokeš – JAMU	Řízení dílčí části projektu.
	29	Libor Spáčil – JAMU	Kontaktní osoba projektu, koordinace projektových činností, administrace projektu.
	30	Jaromír Albrecht – JAMU	Analytické činnosti, řešení technického zázemí a komunikace s dodavateli.
	31	David Vávra – JAMU	Dílčí technická řešení, komunikace s uživateli uvnitř JAMU.
	32	RNDr. Ludmila Bulánová – JU	Řízení dílčí části projektu, koordinace zpracování podkladů pro analýzu aktuálního stavu, adaptace doporučení k bezpečnému využívání nástrojů.

	33	Bc. Eduard Krlín – JU	Zpracování podkladů pro analýzu aktuálního stavu v KB a adaptace doporučení k nasazení v rámci univerzity.
	34	RNDr. Josef Milota – JU	Zpracování soupisu významných informačních systémů školy (VIS) podle jednotné metodiky připravené v projektu. Příprava směrnic a postupů.
	35	Ing. Jan Marek – JU	Zpracování podkladů pro analýzu aktuálního stavu, příprava směrnic a postupů.
	36	Ing. Stratos Zerdaloglu – MENDELU	Řízení dílčí části projektu.
	37	Ing. Jiří Passinger – MENDELU	Odpovědná osoba za oblast bezpečnosti infrastruktury.
	38	Ing. Martina Bednářová, Ph.D. – MENDELU	Odpovědná osoba za implementaci školení a vzdělávání uživatelů v oblasti bezpečnosti.
	39	Ing. Pavel Pomezný – OU	Analýzy technické připravenosti na plnění povinností dle ZoKB, analýzy VIS a jiných informačních systémů, příprava vzdělávání (kurzů) o kyberbezpečnosti, koordinace dílčí části CRP projektu.
	40	Mgr. Bc. Jan Humpolík – OU	Analýzy ZoKB a souvisejících předpisů; návrhy způsobů splnění povinností uložených ZoKB, zejména návrhy vnitřních předpisů; poskytování stanovisek k dílčím problémům plnění ZoKB.
	41	RNDr. Matej Zuzčák, Ph.D. – OU	Příprava metodiky pro vytvoření CSIRT týmu na menší (střední) univerzitě a jeho zapojení do TI-CSIRT, příprava vzdělávání (kurzů) o kyberbezpečnosti, analýzy bezpečnostních hrozeb.
	42	Mgr. Monika Šumberová – OU	Implementace vnitřních předpisů, zajištění vzdělávání (zejména zaměstnanců) ohledně kyberbezpečnosti, komunikace s vedením OU.
	43	Jan Rous – TUL	Řízení dílčí části projektu, analýzy, implementace výsledků projektu, školení, vnitřní legislativa.
	44	Petr Adamec – TUL	Analýzy, implementace KB, školení, vnitřní legislativa.
	45	Radek Melzer – TUL	Analýzy, programování, vnitřní legislativa.
	46	Václav Bernt – TUL	Školení, adaptace vzorových kurzů, příprava výukových materiálů.
	47	Mgr. Michal Zámečník – UHK	Řízení dílčí části projektu, koordinace projektových činností.
	48	Ing. Radek Mrkus – UHK	Analytické práce v rozsahu projektu.
	49	Bc. Aleš Herman – UHK	Analytické práce v rozsahu projektu.
	50	Bc. Libor Filip – UHK	Realizace projektových úkolů, koordinace projektových činností.
	51	Ing. Roman Vaibar Ph.D., MBA – UJEP	Řízení dílčí části projektu, koordinace výstupů projektu směrem k orgánům univerzity.
	52	JUDr. Ing. Eva Severová – UJEP	Příprava univerzitní směrnice pro oblast kyberbezpečnosti.
	53	Ing. Pavel Poláček – UJEP	Analytická část pro potřeby kyberbezpečnosti a technické zpracování při nasazování jednotlivých nástrojů sloužící k podchycení incidentů, logování aj.
	54	Bc. Daniel Tschunko – UJEP	Analytická část pro potřeby kyberbezpečnosti a technické zpracování při nasazování jednotlivých nástrojů sloužící k podchycení incidentů, logování aj.
	55	Ing. Vladimír Horák – UK	Řízení dílčí části projektu, kyberbezpečnostní tým.
	56	Mgr. Michal Voců – UK	Významné informační systémy.
	57	PhDr. Jan Víšek – UK	Kyberbezpečnost, zabezpečení nástrojů pro distanční výuku.
	58	MUDr. Petr Kajzar – UK	Osvěta uživatelů, školení zaměstnanců.

	59	Ing. Olga Klápšťová – UPa	Řízení dílčí části projektu, spolupráce na výstupech 1-6.
	60	Ing. Petr Švec – UPa	Garant výstupu 1, spolupráce na výstupech 2,4,5,6.
	61	Jakub Jelínek – UPa	Garant výstupu 2, spolupráce na výstupech 1,3.
	62	Tomáš Martínek – UPa	Garant výstupu 6, spolupráce na výstupech 1,5.
	63	RNDr. David Skoupil – UP	Řízení dílčí části projektu, koordinace realizačního týmu UP, zapracování výstupů pracovních skupin.
	64	PhDr. Rostislav Hladký, MBA – UP	Příprava koncepčních materiálů, tvorba a zpracování analýz, komunikace s partnery, komunikace s vedením UP a součástmi, disseminace osvětových materiálů.
	65	Mgr. Zuzana Čírtková – UP	Specialista kybernetické bezpečnosti, odborné vedení týmu, implementace technologickým opatření pro prevenci kybernetických hrozeb.
	66	Mgr. Leoš Jurásek, MBA – UP	Implementace procesů a opatření kybernetické bezpečnosti, řízení týmu správců sítí fakult a součástí, metodické vedení fakultních IT pracovníků, aplikace SŘBI.
	67	Ing. Petr Vojtek – UTB	Koordinátor dílčího projektu, zapojení v pracovní skupině Nastavení bezpečného kyberprostředí.
	68	Ing. Petr Skovajsa – UTB	Zapojení v pracovní skupině Nastavení bezpečného kyberprostředí.
	69	Mgr. Monika Hrabáková – UTB	Zapojení v pracovní skupině Významné informační systémy a Právní aspekty KB.
	70	Ing. Jozef Bambuch – UTB	Zapojení v pracovní skupině Významné informační systémy a nastavení O365.
	71	Ing. arch. Gabriela Chmelařová – VFU	Řešitel dílčí části projektu.
	72	Ing. Ladislav Žůrek – VFU	Technická podpora projektu.
	73	Mgr. Štěpán Richter	Právní podpora projektu.
	74	Ing. Michal Sláma – VŠB-TUO	Řízení dílčí části projektu, metodik odborné části.
	75	Ing. Martin Pustka, PhD. – VŠB-TUO	Kyberbezpečnostní aspekty řešení.
	76	Bc. Jakub Kalnik – VŠB-TUO	Člen bezpečnostního týmu, analytik zranitelností a hrozeb.
	77	Ing. Vitězslav Grygar	Člen bezpečnostního týmu, ICT specialista na protiopatření.
	78	Ing. Milan Nidl, MBA – VŠE	Řízení dílčí části projektu, koordinace činnosti v rámci školy.
	79	Ing. Luboš Pavlíček – VŠE	Analytické práce, příprava bezpečnostní dokumentace, navrhování procesů, školení.
	80	Ing. Jan Andraščík – VŠE	Školení, podpora vytváření dokumentace pro soulad se ZoKB.
	81	Ing. Pavel Härtel – VŠCHT	Řízení dílčí části projektu, informační bezpečnost.
	82	Antonín Mareš – VŠCHT	Správce serverů, informační bezpečnost – oblast serverů.
	83	Ing. Andrey Shchurov, Ph.D. – VŠCHT	Správce sítě, informační bezpečnost – oblast sítí.
	84	Ing. Vladimir Khlevnoy – VŠCHT	Správce Flowmon, SIEM – informační bezpečnost – oblast sítí.
	85	Bc. Marek Štark – VŠPJ	Řízení dílčí části projektu, IT technik – analýza a zlepšení KB.
	86	Ing. Martin Skoumal, DiS. – VŠPJ	Bezpečnostní manažer – adaptace a zpřístupnění vzdělávacích materiálu, zlepšení KB.
	87	Ondřej Chalupa, DiS. – VŠPJ	IT technik – analýza a zlepšení KB.
	88	Ing. Jaromír Vrbka, MBA, PhD. – VŠTE	Hlavní koordinátor činností na straně partnera projektu – zodpovídá za řádný průběh projektu.
	89	Ing. Jakub Uhlíř – VŠTE	Koordinátor odborných aktivit na straně partnera projektu.

	90	Jan Holba – VŠTE	Garant za plnění aktivit v oblasti IT – zodpovědný pracovník za činnosti spojené s nastavením kyberbezpečnostní osvěty v mobilní aplikaci.
	91	Ing. Jaromír Marušinec, Ph.D., MBA – VUT	Řízení dílčí části projektu.
	92	Ing. Tomáš Kreuzwieser – VUT	Implementace kybernetické bezpečnosti do infrastruktury.
	93	Ing. Tomáš Podermański – VUT	Nastavení procesů a systémů pro řešení bezpečnostních incidentů.
	94	Ing. Vít Baloun – VUT	Osvěta kybernetické bezpečnosti.
	95	Ing. Jiří Bořík – ZČU	Řízení dílčí části projektu, analytické činnosti v oblasti integrace vzdělávání zaměstnanců do informačních systémů univerzity.
	96	Ing. Jiří Čepák – ZČU	Zapracování zásad kybernetické bezpečnosti do existujících procesů univerzity, návrhy úprav vnitřní legislativy.
	97	Ing. Šárka Zuzjaková, Ph.D. – ZČU	Příprava a provedení průzkumů v oblasti vzdělávání zaměstnanců, aktualizace školících materiálů.
	98	Ing. Jan Krňoul – ZČU	Příprava náplně školení pro programátory a administrátory informačních systémů a jeho organizace.
	99	Bc. Martin Šebela – ZČU	Implementace zásad kybernetické bezpečnosti do školících materiálů pro zaměstnance.
	100	Mgr. Jan Nosek – SU	Koordinátor všech činností a plnění výstupů Řešitel dílčí části projektu.
	101	Ing. Jiří Sléžka, DiS. – SU	Kontaktní osoba dílčího projektu. Koordinátor aktivit v rámci PS-1 a PS-2.
	102	Mgr. Milan Študent – SU	Koordinátor pro oblast osvěty a vzdělávání v kyberbezpečnosti.
	103	Ing. Jakub Ježíšek – SU	Zpracování podkladů pro analýzu aktuálního stavu; implementace procesů a opatření v KB v rámci univerzity.
	104	Bc. Miroslav Pajr – SU	Činnosti související s identifikací a zabezpečením významných inf-systémů univerzity.
	105	Ing. Petr Korviny, Ph.D. – SU	Spoluřešitel činností v oblasti osvěty a vzdělávání v kyberbezpečnosti.

Přehled o pokračujícím projektu	Pokud se jedná o pokračující projekt, uveďte, kolik finančních prostředků bude čerpáno a jaké cíle a výstupy jsou plánovány do budoucna.		
	Rok realizace	**Čerpání finančních prostředků** (souhrnný údaj)	**Plánované cíle a výstupy**
	2022	25 mil Kč	Implementace vyššího stupně kyberzabezpečení a naplnění všech povinností pro správce a provozovatele VIS
	2023		
	2024		

Přehled o udržitelnosti investice/činnosti	Uveďte, jak bude z rozvojového projektu podpořená investice/činnost pokračovat a jakým způsobem bude finančně zabezpečena po ukončení rozvojového projektu.
	V rámci projektu nejsou plánovány žádné investice. Co se týče udržení nastartovaných činností: v rámci jednotlivých VVŠ je to nedílnou součástí nastavení kyberbezpečnostních postupů jako základní podmínky pro trvalou ochranu (jednorázová ochrana nedává zde žádný smysl). Na společné úrovni předpokládáme navázání dlouhodobé spolupráce kyberbezpečnostních týmů VVŠ s cílem jednak pokračovat v řešeních zahájených tímto projektem směrem k implementaci vyššího stupně kyberzabezpečení a praktické realizaci všech povinností pro správce a provozovatele významných informačních systémů, které budou identifikovány, popsány a projednány s NÚKIB.

Vyplní pouze koordinátor:

ROZPOČET CELÉHO PROJEKTU		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	15 700
3.	**Celkem běžné a kapitálové finanční prostředky**	15 700

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (AMU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (AVU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (ČZU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (ČVUT)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	1 500
3.	**Celkem běžné a kapitálové finanční prostředky**	1 500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (JAMU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (JU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (MU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	2 700
3.	**Celkem běžné a kapitálové finanční prostředky**	2 700

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (MENDELU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (OU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (SU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (TUL)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UHK)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UJEP)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UK)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UP)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UPA)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500

3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (UTB)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VFU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VŠB-TUO)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VŠE)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VŠCHT)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VŠPJ)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0

2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VŠTE)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (VUT)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

ROZPOČET DÍLČÍCH ČÁSTÍ PROJEKTU (ZČU)		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
2.	**Běžné finanční prostředky**	500
3.	**Celkem běžné a kapitálové finanční prostředky**	500

Zdůvodnění způsobu rozdělení rozpočtu mezi jednotlivé VŠ.	Projekt bude realizován ve spolupráci a součinnosti všech 25 zapojených veřejných vysokých škol. Každá zapojená škola potřebuje řešit základní okruh problémů s nastavením, resp. vylepšením stavu své kyberbezpečnostní ochrany a přípravu svého vlastního prostředí na plnění povinností vyplývajících za ZoKB. Tyto okruhy problémů jsou obdobné pro všechny VVŠ, bez ohledu na jejich velikost, proto byla na tyto činnosti vyčleněna pro všechny VŠ v rozpočtu stejná částka ve výši 0,5 mil Kč, kterou jednotlivé školy podle potřeby doplní z dalších (obvykle vlastních) zdrojů pro řešení dalších úkolů nad rámec základního okruhu. Zvažovali jsem i možnost odstupňovat tuto základní částku úměrně podle velikosti VVŠ, ale po diskusi se všemi partnery jsme od toho ustoupili, neboť základní okruh práce je pro všechny školy stejný, navíc malé školy jsou handicapovány nižšími personálními kapacitami aktuálně vyčleněnými na kyberbezpečnost a potřebují tyto kapacity posílit. Kromě částky na základní okruh pak ty vysoké školy, které zajišťují realizaci společných činností a výstupů, získaly z rozpočtu příspěvek na zajištění těchto činností, v závislosti na jejich odhadované celkové náročnosti.	
Zdůvodnění výše požadovaných finančních prostředků jednotlivých VŠ zapojených do projektu	**Název VŠ (zkratka)**	**Zdůvodnění**
	AMU	Výše požadovaných finančních prostředků AMU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	AVU	Výše požadovaných finančních prostředků AVU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	ČZU	Výše požadovaných finančních prostředků ČZU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.

	ČVUT	Výše požadovaných finančních prostředků odpovídá jednak nákladům na implementaci potřebných výstupů v rámci školy, tak zejména realizaci výstupů a činností v rámci pracovní skupiny PS-2, za kterou převzala ČVUT zodpovědnost a která činí větší díl požadovaných prostředků.
	JAMU	Výše požadovaných finančních prostředků JAMU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	JU	Výše požadovaných finančních prostředků Jihočeské univerzity v Českých Budějovicích odpovídá činnostem popsaným v dílčím projektu a zapojení školy, která nemá v rámci IT vývojové oddělení. Vývoj a implementaci SW v oblasti uvedených výstupů realizuje univerzita dodavatelsky.
	MU	Výše požadovaných finančních prostředků odpovídá nákladům hlavního řešitele projektu v souvislosti jak s koordinací celého projektu, tak zejména s realizací velké části výstupů celého projektu poskytnutých ostatním partnerům projektu v rámci tří pracovních skupin projektu.
	MENDELU	Výše požadovaných finančních prostředků MENDELU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy.
	OU	Výše požadovaných finančních prostředků Ostravské univerzity odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy.
	SU	Výše požadovaných finančních prostředků SU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	TUL	Výše požadovaných finančních prostředků TUL odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UHK	Výše požadovaných finančních prostředků UHK odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UJEP	Výše požadovaných finančních prostředků UJEP odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UK	Výše požadovaných finančních prostředků UK odpovídá rozsahu vlastních činnosíi popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UP	Výše požadovaných finančních prostředků UK odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UPa	Výše požadovaných finančních prostředků UPa odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	UTB	Výše požadovaných finančních prostředků UTB odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VFU	Výše požadovaných finančních prostředků VFU odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VŠB-TUO	Výše požadovaných finančních prostředků VŠB-TUO odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.

	VŠE	Výše požadovaných finančních prostředků VŠE odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VŠCHT	Výše požadovaných finančních prostředků VŠCHT odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VŠPJ	Výše požadovaných finančních prostředků VŠPJ odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VŠTE	Výše požadovaných finančních prostředků VŠTE odpovídá rozsahu vlastních činností popsaných v rámci dílčího projektu při nastavení bezpečného kyberprostředí školy a charakteristice zapojení partnera popsané výše.
	VUT	Výše požadovaných finančních prostředků VUT odpovídá nákladům na implementaci potřebných výstupů v rámci školy.
	ZČU	Výše požadovaných finančních prostředků ZČU odpovídá nákladům na implementaci potřebných výstupů v rámci školy a realizaci činností popsaných v charakteristice zapojení partnera.

Poznámka: V případě, že potřebujete sdělit další doplňující informace, uveďte je v příloze.

Každá VŠ (včetně té, která je koordinující) uvede charakteristiku té části projektu, kterou řeší, v následující tabulce:

CHARAKTERISTIKA DÍLČÍ ČÁSTI PROJEKTU					
Přehled o řešení projektu v roce 2020	Nejedná se o pokračující projekt z roku 2020.				
	Cíle stanovené v návrhu projektu		**Plnění plánovaných cílů a kontrolovatelných výstupů k datu předání této žádosti**		
	Cíl				
	Cíl				
	Přehled čerpání finančních prostředků k datu předání této žádosti		**Projekt financován od**		
Výstupy dílčí části projektu					
Definujte konkrétní a měřitelné výstupy projektu, které budou výsledkem projektu.	**č.**	**Výstup dílčí části projektu** (přidejte řádky podle potřeby)			
	1	Analýza stavu KB na MU a ostatních VVŠ			
	2	Metodiky, personální a procesní rámec pro KB na VVŠ			
	3	Nastavení základní úrovně bezpečnosti kyberprostředí na jednotlivých VVŠ			
	4	Identifikace a analýza významných informačních systémů školy			
	5	Příprava pro splnění zákonných opatření plynoucích za ZoKB			
	6	Osvětové materiály pro KB			
	7	Nastavení systematické KB osvěty na jednotlivých VVŠ			
	8	Implementace kurzu pro kyberbezpečnostní vzdělávání zaměstnanců na MU			
	9	Doporučení pro zvýšení bezpečnosti v prostředí O365			
	10	Workshopy pro klíčové oblasti řešení			
	11	Závěrečná zpráva řešení projektu za rok 2021, včetně návrhu dalšího postupu pro rok 2022			
Popis dílčích činností projektu					
Pro každý výstup identifikujte hlavní činnosti, které povedou k jeho naplnění v harmonogramu.	**č.**	**Hlavní činnosti** (přidejte řádky podle potřeby)	**Termín zahájení**	**Termín ukončení**	**Číslo výstupu**
	1	Příprava metodik a nástrojů pro analýzy aktuálního stavu KB ve VŠ prostředí (analýza personálního a procesního nastavení KB na VVŠ, analýzy osvěty a vzdělávání zaměstnanců v KB)	1/2021	1/2021	1
	2	Průzkum aktuálního stavu na MU a ostatních VVŠ; zpracování souhrnných analýz jako východisek pro další opatření; kategorizace VVŠ z pohledu možností a potřeb nastavení základní úrovně KB	2/2021	3/2021	1
	3	Příprava manuálu pro vznik KB týmu VVŠ a definice jeho základních služeb; definice základních procesů pro identifikaci, řešení a komunikaci KB incidentů;	1/2021	6/2021	2

		vytvoření vzorů legislativních opatření pro nastavení základní úrovně KB v prostředí VVŠ; definice vzorové struktury Bezpečnostní dokumentace			
	4	Koordinace a podpora vytvoření a legislativního ustanovení KB týmů na VVŠ, kde toto dosud neproběhlo	3/2021	6/2021	3
	5	Pomoc partnerům projektu s implementací základních procesů a opatření: univerzitní kyberbezpečnostní směrnice; identifikace, řešení a komunikace incidentů, a dalších	5/2021	12/2021	3
	6	Zpracování soupisu významných informačních systémů školy (VIS) na MU podle jednotné metodiky připravené v rámci pracovní skupiny PS-2	1/2021	10/2021	4
	7	Dokončení příp. vylepšení procesů pro splnění minimálních zákonných povinností dle ZoKB v oblasti VIS a dalších podle metodik a doporučení připravených v projektu	6/2021	12/2021	5
	8	Soupis a analýza dostupných aktuálně dostupných materiálů a přístupů ke KB osvětě na VVŠ. Specifikace cílových skupin a identifikace jejich potřeb; příprava vzdělávacích materiálů pro jednotlivé cílové skupiny; zpracování osvětových článků a podpůrných materiálů na vybraná témata. Zpracování metodiky pro zavádění systematické osvěty a návrhu vzorových procesů zajištění rozvoje KB povědomí	1/2021	6/2021	6
	9	Pomoc a podpora partnerům s nastavení procesů KB osvěty a daptací + disseminací vytvořených materiálů	6/2021	12/2021	7
	10	Adaptace vzorových kurzů vytvořených v rámci projektu pro potřeby a prostředí MU	6/2021	9/2021	8
	11	Nastavení a implementace periodického (online) školení zaměstnanců v KB na MU	9/2021	12/2021	8
	12	Analýzy a doporučení ke zvýšení zabezpečení platformy 0365 na MU	3/2021	12/2021	9
	13	Koordinace případně pořádání interních workshopů pro partnery projektu k implementaci doporučení a metodik připravených jednotlivými pracovními skupinami, a k výměně praktických zkušeností; osvětové workshopy za účasti zástupců NÚKIB	1/2021	12/2021	10
	14	Zpracování závěrečné zprávy projektu, zhodnocení průběhu řešení a naplnění plánovaných výstupů; vize další spolupráce VVŠ v roce 2022	10/2021	12/2021	11

Realizační tým			
Uveďte plán personálních o zajištění	**č.**	**Jména klíčových lidí** (přidejte řádky podle potřeby)	**Činnosti**
	1	RNDr. Miroslav Bartošek, CSc.	Koordinátor projektu. Celkové řízení projektu, plnění cílů, koordinace činností a výstupů. Řešitel dílčí části za MU.
	2	Bc. Tomáš Plesník	Koordinátor pracovní skupiny PS-3. Jako vedoucí CSIRT-MU s bohatými expertními i provozními zkušenostmi bude garantovat odbornou kvalitu a věcnou správnost řešení projektu, a také návaznosti mezi jednotlivými odbornými PS.
	3	RNDr. Michal Javorník, Ph.D.	Koordinátor PS-1: řízení pracovní skupiny, koordinace a garance plánovaných výstupů.
	4	RNDr. Michal Růžička. Ph.D.	Analýzy a doporučení v oblasti bezpečnostních technologií.
	5	Mgr. Zuzana Řepišová	Administrativa celého projektu.
	6	JUDr. Mgr. Jakub Harašta, Ph.D.	Vedení a koordinace PS-7, zpracování právních analýz a doporučení, právní konzultace všem PS, legislativní otázky.

	7	RNDr. Martin Laštovička	Odborný pracovník Skupiny reakce na incidenty CSIRT-MU. Příprava metodik a doporučení v rámci PS-1. Podpora kyberbezpečnostním týmům partnerů projektu.
	8	Mgr. Tomáš Marek	Příprava osvětových materiálů a plánů jejich disseminace v rámci PS-3.
	9	Mgr. Břetislav Regner-	Koordinace analýz a doporučení pro zvýšení bezpečnosti platformy O365.
	10	Jan Izydorzcyk	Analytické práce a doporučení pro oblast bezpečnosti platformy O365.
	11	Další pracovníci CSIRT-MU	Analytické práce, příprava metodik a doporučení.

Přehled o pokračujícím projektu	Pokud se jedná o pokračující projekt, uveďte, kolik finančních prostředků bude čerpáno a jaké cíle a výstupy jsou plánovány do budoucna.		
	Rok realizace	**Čerpání finančních prostředků** (souhrnný údaj)	**Plánované cíle a výstupy**
	2022	25 mil Kč	Implementace vyššího stupně kyberzabezpečení a naplnění všech povinností pro správce a provozovatele VIS
	2023		
	2024		

Přehled o udržitelnosti investice/činnosti	Uveďte, jak bude z rozvojového projektu podpořená investice/činnost pokračovat a jakým způsobem bude finančně zabezpečena po ukončení rozvojového projektu.

Poznámka: V případě, že potřebujete sdělit další doplňující informace, uveďte je v příloze.

Každá VŠ (včetně té, která je koordinující) uvede samostatný rozpočet za tu část projektu, kterou řeší, v následující tabulce:

ROZPOČET DÍLČÍ ČÁSTI PROJEKTU		
		Požadavek na dotaci ze státního rozpočtu – ukazatel I (v tis. Kč)
1.	**Kapitálové finanční prostředky**	0
1.1	Dlouhodobý nehmotný majetek (SW, licence)	
1.2	Samostatné věci movité (stroje, zařízení)	
1.3	Ostatní technické zhodnocení	
2.	**Běžné finanční prostředky celkem**	2 700
	Osobní náklady:	
2.1	Mzdy (včetně pohyblivých složek)	1 490
2.2	Ostatní osobní náklady (odměny z dohod o pracovní činnosti, dohod o	380

	provedení práce, popř. i některé odměny hrazené na základě nepojmenovaných smluv uzavřených podle zákona § 1746 odst. 2 č. 89/2012 Sb., občanský zákoník)	
2.3	Odvody pojistného na veřejné zdravotní pojištění a pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti a příděly do sociálního fondu	668
	Ostatní:	
2.4	Materiální náklady (včetně drobného majetku)	32
2.5	Služby a náklady nevýrobní	120
2.6	Cestovní náhrady	10
2.7	Stipendia	0
3.	**Celkem běžné a kapitálové finanční prostředky**	2 700

Zdůvodnění požadavků v jednotlivých položkách (přidejte řádky podle potřeby)			
Číslo položky (viz předchozí tabulka**)**	**Název výdaje a jeho podrobné zdůvodnění**	**Výstup projektu** (uveďte výstup z tabulky „Výstupy dílčí části projektu““)	**Částka (v tis. Kč)**
2.1	Mzdy a odměny hlavního řešitel a administrátora za řízení, administrativu, zprávy, hodnocení a celkovou organizaci projektu	1-11	320
2.1	Mzdy a odměny odborným pracovníkům zajišťujícím řešení a výstupy v PS-1	1-5,9	670
2.1	Mzdy a odměny odborným pracovníkům zajišťujícím řešení a výstupy v PS-3	6-8	300
2.1	Mzdy a odměny právnímu týmu, PS-7	2-5	200
2.2	OON zejména pro studenty a externí pracovníky při obsahové, grafické a technické realizaci osvětových materiálů a článků	1-2, 6-7	380
2.3	Povinné zákonné zdravotní a sociální pojištění, příspěvek na sociální fond	1-11	668
2.4	Spotřební materiál a drobný majetek	1-11	32
2.5	Konzultační služby na nástroje a postupy v prostředí O365	9	100
2.5	Služby spojené s přípravou a organizací workshopů	10	20
2.6	Tuzemské cestovné (v závislosti na konkrétní epidemiologické situaci zejména ve 2. polovině roku 2021)	1-11	10

Předpokládané zdroje financování projektu	
Uveďte, jaké jsou předpokládané zdroje financování rozvojového projektu (dotace ze státního rozpočtu, vlastní zdroje VŠ – uveďte jaké atd.).	
Zdroj financování	**Částka (v tis. Kč)**
Dotace Centralizovaného rozvojového projektu 2021	2 700

Souvislost s ostatními podávanými projekty	Uveďte, zda je obsahově podobný projekt podáván současně v rámci centralizovaných rozvojových projektů na rok 2021.
	Částečná souvislost (nikoliv však překryv) se týká projektu zaměřeného na etické používání distančních nástrojů (projektu zabývajícího se distančním vzděláváním jako nástrojem rozvoje vysokých škol).

Počet studentů, kteří jsou do projektu zapojení/jichž se projekt týká	Uveďte, jaké je zapojení studentů v rámci projektu, ať již jako příjemci podpory a/nebo jestliže se podílí na řešení projektu (přidejte řádky dle potřeby).
	Do řešení projektu bude přímo zapojeno několik studentů zejména při redakčním zpracování osvětových materiálů. Svými dopady se projekt týká prakticky všech studentů zapojených VVŠ.