INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

Seminář pro žadatele

10. výzva eGovernment a kybernetická bezpečnost – SC 1.1 (VRR)

Řídicí orgán IROP, MS Teams, 1. 11. 2022

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Program

12:30 – 13:00	Prezence účastníků
13:00 – 13:15	Zahájení, představení IROP a rozdílů mezi IROP 2014+ a IROP 2021+
13:15 – 14:00	Představení 10. výzvy IROP – eGovernment a kybernetická bezpečnost – SC 1.1 (VRR)
14:00 – 14:45	Systém hodnocení projektů a další administrace projektů, dotazy
14:45 – 15:00	Přestávka
15:00 – 15:30	Postup pro podání žádosti o podporu v MS2021+, dotazy
15:30 – 16:00	Výběrová a zadávací řízení, dotazy
16:00	Závěr

Zahájení, představení IROP a rozdílů mezi IROP 2014+ a IROP 2021+

PhDr. Aleš Pekárek, ŘO IROP

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

IROP 2021-2027

- **Alokace: 4,8 mld. EUR = 117 mld. Kč**
- Financování: Evropský fond pro regionální rozvoj
- Kofinancování: podle kategorií regionů 70 % nebo 85 % z EFRR (v Praze 40 %) a státní rozpočet podle Pravidel spolufinancování 0 - 30 %
- Projekty realizované prostřednictvím CLLD: 80 % nebo 95 % z EFRR

Role MMR a Centra

- **Ministerstvo pro místní rozvoj ČR = Řídicí orgán IROP (ŘO IROP)**
  - řízení programu
  - příprava výzev a pravidel pro žadatele a příjemce
  - poskytovatel dotace
- **Centrum pro regionální rozvoj ČR (Centrum) = Zprostředkující subjekt IROP**
  - Konzultační servis, konzultace
  - příjem a hodnocení žádostí o podporu
  - administrace změn, kontroly projektů, kontroly žádostí o platbu

Pravidla pro žadatele a příjemce

Obecná pravidla

závazná pro všechny specifické cíle a typy příjemců

http://www.irop.mmr.cz/cs/

Specifická pravidla (SPPŽP)

společná pro každou dvojvýzvu / trojvýzvu

http://www.irop.mmr.cz/cs/

podporované aktivity, způsobilé výdaje, povinné přílohy, hodnoticí kritéria

Změny v IROP 2021-2027

- **Konzultační servis Centra** - zřízen Konzultační servis Centra, ve kterém probíhá komunikace mezi žadateli a Centrem k projektům před předložením žádosti o podporu
- **Výzvy** - všechny výzvy v IROP jsou průběžné
- **Integrované nástroje** - žadatel předkládá žádost přímo do výzvy ŘO pro ITI/CLLD
- **Hodnocení v integrovaných výzvách** - žádosti se budou hodnotit pouze na Centru
- **MS2021+** - Postup pro podání žádosti o podporu v MS2021+ a Příručka pro práci v MS2021+ jsou na dokumenty IROP 2021-2027
- **Registrace uživatele v MS2021+** - nově přes Národní identitní autoritu

Změny v IROP 2021-2027

- **Kategorie regionů** - tři kategorie regionů s max. mírou spolufinancování z EU pro méně rozvinuté regiony 85 %, pro přechodové regiony 70 %, pro rozvinutější regiony 40 %

Projekty VRR	40 %
Projekty PR	70 %
Projekty MRR	85 %

Změny v IROP 2021-2027

- **Zjednodušené metody vykazování** - v některých výzvách - paušální sazba ve výši 7 %
- **Poskytnuté údaje veřejné správě** - nepožadujeme předložení již jednou veřejné správě poskytnutých údajů, např. výpis z Obchodního rejstříku / z katastru nemovitostí
- **eCBA a sledování příjmů v projektu** - zrušena povinnost eCBA a sledování příjmů
- **Nevyčerpané prostředky** - mezi sledovanými obdobími se přesouvají automaticky, ~~ŽoZ~~
- **Lhůty pro splnění** - zpravidla jsou navázány na datum doručení dokumentu či depeše
- **Kontrola formálních náležitostí a přijatelnosti** - v případě potřeby po dvou výzvách k doplnění žádosti vyzýváno ještě k opravě zjevných formálních chyb

Priority IROP 2021-2027

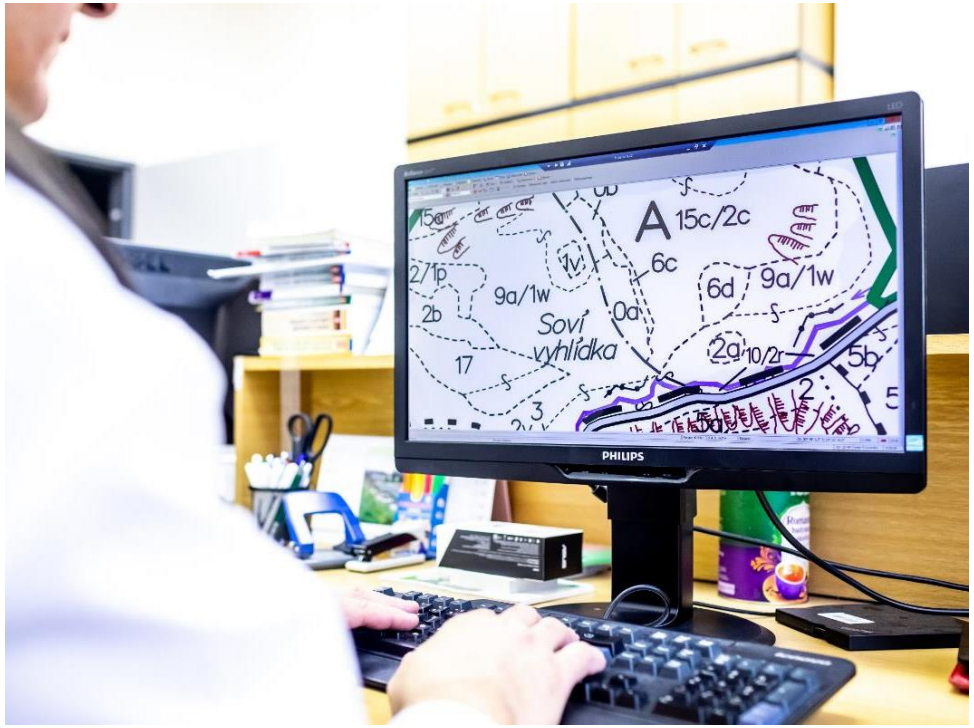
Číslo priority	Název priority
Priorita 1	**Zlepšení výkonu veřejné správy**
Priorita 2	Zelená infrastruktura měst a obcí a ochrana obyvatelstva
Priorita 3	Rozvoj dopravní infrastruktury
Priorita 4	Zlepšení kvality a dostupnosti sociálních a zdravotních služeb, vzdělávací infrastruktury a rozvoj kulturního dědictví
Priorita 5	Komunitně vedený místní rozvoj
Priorita 6	Rozvoj městské mobility

IROP 2021-2027: specifický cíl 1.1

Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány

Celkem **12,4 mld. Kč z EFRR**

Kybernetická bezpečnost – 3,6 mld. Kč (EFRR) | **30 %**
eGovernment – 6,4 mld. Kč (EFRR) | **50 %**
eHealth - 2,4 mld. Kč (EFRR) | **20 %**



Další výzvy v SC 1.1 IROP

2023

- Rozvoj neveřejné síťové infrastruktury veřejné správy (MRR, PR, ČR)
- eHealth (MRR, PR, ČR)
- Standardizace územních plánů (MRR, PR)
- Kybernetická bezpečnost (NÚKIB)

Další výzvy v SC 1.1 IROP

ITI výzva eGovernment a kybernetická bezpečnost – výzva č. 29, vyhlášení 10. listopadu 2022

V čem se liší výzvy pro integrované nástroje?

- žadatel předkládá žádost přímo do výzvy ŘO IROP pro ITI
- podmínkou je kladné vyjádření ŘV nositele ITI
- u integrovaných výzev nebudou limity min./max. celkových způsobilých výdajů

Představení výzvy

10. výzva IROP – eGovernment a kybernetická bezpečnost – SC 1.1 (VRR)

Ing. Jan Mazanik, ŘO IROP

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

Odkazy na výzvu

Texty výzev, obecná a specifická pravidla včetně příloh, postup pro podání žádosti v MS2021+:

https://irop.mmr.cz/cs/vyzvy-2021-2027

Kontrolní listy k hodnocení:

https://www.crr.cz/irop/projekt-a-kontrola/kontrolni-listy/

Parametry výzvy

Datum vyhlášení výzvy **Datum zpřístupnění MS2021+** **Datum zahájení příjmu žádostí**	17. 10. 2022, 14:00
Ukončení příjmu žádostí	31. 8. 2023
Nejzazší datum ukončení realizace projektu	31.12. 2027
Min/max. výše CZV	1-70 mil. Kč
Způsobilost výdajů	1. 1. 2021 do doby ukončení realizace

Parametry výzvy

Typ regionu - místo realizace	území hl. m. Prahy
Oprávnění žadatelé	• hlavní město Praha; • městské části hl. m. Prahy; • organizace zřizované nebo zakládané hl. m. Prahou / městskými částmi hl. m. Prahy
Alokace (EFRR)	245 mil. Kč

Parametry výzvy

Veřejná podpora	Pro aktivity „eGovernment“ Budou podpořeny pouze projekty nezakládající veřejnou podporu ve smyslu čl. 107 odst. 1 SFEU. Pro aktivitu Kybernetická bezpečnost Budou podpořeny projekty: • nezakládající veřejnou podporu ve smyslu čl. 107 odst. 1 SFEU; • žadatelů o podporu, kteří jsou poskytovatelé služeb obecného hospodářského zájmu dle Rozhodnutí 2012/21/EU (model A); • žadatelů o podporu, kteří nejsou poskytovatelé služeb obecného hospodářského zájmu dle Rozhodnutí 2012/21/EU (model B).

Parametry výzev - spolufinancofání (VRR)

Typ	EFRR	Státní rozpočet	Vlastní zdroje žadatele
hlavní město Praha;	40 %	10 %	50 %
městské části hl. m. Prahy;	40 %	10 %	50 %
organizace zřizované hl. m. Prahou / městskými částmi hl. m. Prahy	40 %	10 %	50 %
organizace zakládané hl. m. Prahou / městskými částmi hl. m. Prahy	40 %	0 %	60 %

Parametry výzvy

Ve výzvě není omezen počet žádostí o podporu předložených jedním žadatelem.

Podporované aktivity

„eGovernment“ a kybernetická bezpečnost

Podporované aktivity
(„eGovernment“)

- Elektronizace vybraných služeb veřejné správy
- Rozšíření propojeného datového fondu
- Integrace elektronických služeb veřejné správy a informací o službách veřejné správy na portál gov.cz
- Opatření vedoucí k intenzivnímu využívání existujících bezpečných systémů elektronické identifikace
- Publikace dat veřejné správy jako OpenData

Podporované aktivity
(„eGovernment“)

- Transakční portálová řešení s využitím zaručené elektronické identity
- Automatizace zpracování digitálních dat (robotizace)
- Centralizace, standardizace a sdílení elektronických služeb veřejné správy

Podporované aktivity
(kybernetická bezpečnost)

- **Kybernetická bezpečnost**

Nejsou podporovány aktivity

- **v souvislosti s elektronizací zdravotnictví (eHealth)**. V případě, že budou součástí projektu nástroje a služby využívající informační a komunikační technologie ke zlepšení prevence, diagnostiky, léčby a monitorování a řízení zdraví a životního stylu, bude se jednat o výdaje, které nelze zahrnout mezi přímé výdaje;
- **v souvislosti se standardizaci územních plánů**, tj. převodu stávajícího územního plánu, který ve stávajícím stavu není zpracován v jednotném standardu, do jednotného standardu stanoveného účinnou legislativní úpravou.

Co je výstupem projektu? („eGovernment“)

Výstupem projektu musí být nově pořízený nebo modernizovaný **informační systém**.

- V jednom projektu je možné pořídit jeden nebo více IS.
- Pořízený informační systém musí zajišťovat **minimálně tři nové funkcionality**, pokud v modernizovaném informačním systému v době podání žádosti o podporu neexistují.
- Žadatel může uvést novou funkcionalitu, která není uvedená v seznamu. Funkcionalitu a její relevanci posoudí odbor Hlavního architekta eGovernmentu ve svém Stanovisku.

Co je výstupem projektu?
(kybernetická bezpečnost)

Realizace technických bezpečnostních opatření podle § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Podporována jsou technická bezpečnostní opatření:

- a) fyzická bezpečnost,
- b) nástroj pro ochranu integrity komunikačních sítí
- c) nástroj pro ověřování identity uživatelů,
- ...
- podle hlavy II, vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Co je výstupem projektu?

Projekt může být kombinací uvedeného.

Finanční limity

pro aktivity „eGgovernmentu“: nejsou

pro aktivitu Kybernetická bezpečnost: limit na jednotlivá technická opatření

Finanční limity

Na jednotlivá technická opatření jsou v projektu uplatňovány finanční limity:

projekt realizující 1 technické opatření: 1–20 mil. Kč celkových způsobilých výdajů,

projekt realizující 2 technická opatření: 1–26 mil. Kč celkových způsobilých výdajů,

projekt realizující 3 technická opatření: 1–32 mil. Kč celkových způsobilých výdajů,

projekt realizující 4 technická opatření: 1–38 mil. Kč celkových způsobilých výdajů.

Maximální počet technických opatření je 12 (písm. a až l, odst. 3, § 5 zákona č. 181/2021 Sb., o kybernetické bezpečnosti.

Od dvou technických opatření je nárůst celkových způsobilých výdajů vždy o 6 mil. Kč, **až do výše maximálních celkových způsobilých výdajů projektu**.

(tj. max. 70 mil. Kč)

Finanční limity

Celkový finanční limit na **jednotlivá technická opatření** je žadatel oprávněn **navýšit jednorázově o 30 mil. Kč**, pokud je součástí projektu zabezpečení jednoho nebo více **ISZS**.

Celkový finanční limit na jednotlivá technická opatření je žadatel oprávněn navýšit jednorázově o **10 mil. Kč**, pokud je součástí projektu zabezpečení jednoho nebo více **VIS**.

Celkový finanční limit na jednotlivá technická opatření je žadatel oprávněn navýšit jednorázově o **30 mil. Kč**, pokud je součástí projektu zabezpečení jedné nebo více **KII**.

Navýšení celkového finančního limitu **na jednotlivá technická opatření** v případě společného výsktu KII a/nebo VIS a/nebo ISZS je možné kumulovat.

Vždy platí minimální / maximální limit na projekt: 1 až 70 mil. Kč

Povinné přílohy k žádosti o podporu

1. Plná moc
2. Zadávací a výběrová řízení
3. Doklady k právní subjektivitě žadatele
4. **Studie proveditelnosti** - dle osnovy v příloze č. 2 SPPŽP
5. Doklad o prokázání právních vztahů k nemovitému majetku, který je předmětem projektu
6. Doklad prokazující povolení umístění stavby v území dle stavebního zákona
7. Doklad prokazující povolení k realizaci stavebního záměru dle stavebního zákona

4. PODROBNÝ POPIS PROJEKTU

4.1 PODROBNÝ POPIS VÝCHOZÍHO STAVU

Popište výchozí stav před zahájením realizace projektu, tj. výchozí situaci, problémy a nedostatky, které má projekt řešit.

4.2 POPIS JEDNOTLIVÝCH ČÁSTÍ PROJEKTU

UPOZORNĚNÍ

Žadatel dokládá souhlasné stanovisko odboru Hlavního architekta eGovernmentu (OHA), včetně Formuláře žádosti o stanovisko OHA typu A, případně vyjádření OHA o posouzení nerelevantnosti vydání stanoviska. Více viz příloha č. 9 Pravidla pro vydání souhlasného stanoviska odboru Hlavního architekta eGovernmentu.

Žadatel může kromě souhlasného stanoviska OHA / vyjádření OHA o posouzení nerelevantnosti vydání stanoviska doložit i jen potvrzení o přijetí žádosti o vydání stanoviska od OHA včetně Formuláře žádosti o stanovisko OHA typu A, vzor potvrzení je přílohou č. 8 Specifických pravidel. Souhlasné stanovisko OHA je následně žadatel povinen doložit prostřednictvím žádosti o změnu (viz kapitola 12 Obecných pravidel) nejpozději do 12 měsíců od registrace žádosti o podporu.

- Popis částí projektu
  - Uveďte a strukturovaně popište projektem pořizované informační systémy. Každý informační systém uveďte v samostatné tabulce. **Žadatel nevyplňuje, pokud je projekt zaměřen pouze na realizaci aktivity Kybernetické bezpečnosti**, tj. na realizaci technických bezpečnostních opatření podle § 5 odst. 3 zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále "ZKB") a mezinárodních standardů a norem v oblasti bezpečnosti informací.

Název pořizovaného IS	*Uveďte název*
ID IS	*Uveďte číselný identifikátor, který umožní tento IS jednoznačně identifikovat.*

Povinné přílohy k žádosti o podporu

8. Znalecký posudek
9. Projektová dokumentace stavby
10. Rozpočet stavebních prací
11. Povinné přílohy prokazující vyhodnocení žadatele o podporu z pohledu podniku v obtížích
12. Podklady pro stanovení kategorií intervencí a kontrolu limitů
13. Smlouva o zřízení bankovního účtu

Povinné přílohy k žádosti o podporu

14. **Souhlasné stanovisko odboru Hlavního architekta eGovernmentu**
15. **Čestné prohlášení žadatele k souhlasnému stanovisku odboru Hlavního architekta eGovernmentu**
16. **Čestné prohlášení žadatele k žádosti o souhlasné stanovisko odboru Hlavního architekta eGovernmentu**
17. **Kontrolní list**
18. Pověřovací akt

Povinné přílohy k žádosti o podporu

19. **Doklad o stanovení kritické informační infrastruktury, významného informačního systému nebo informačního systému základních služeb**
20. Stanovení hodnoty indikátoru 304 002
21. Výpis z Evidence skutečných majitelů

Souhlasné stanovisko odboru Hlavního architekta eGovernmentu

Povinnost doložení pro každý projekt!

Žadatel dokládá souhlasné stanovisko OHA včetně Formuláře žádosti o stanovisko OHA typu A, případně vyjádření OHA o posouzení nerelevantnosti vydání stanoviska.

Může doložit i jen **potvrzení** o přijetí žádosti o vydání stanoviska od OHA včetně Formuláře žádosti o stanovisko OHA typu A. Potvrzení musí být ve formě vzoru přílohy. Datum a čas příjmu žádosti o vydání stanoviska OHA musí předcházet datu a času registrace žádosti o podporu.

- Doložení podání žádosti o stanovisko OHA formou výpisu z datové schránky nebo jinou formou není relevantní přílohou a nebude akceptováno.
- Název projektu na doložené Žádosti o vydání stanovisko OHA a na výsledném stanovisku OHA musí být identický jako unikátní název projektu žadatele uvedený v systému MS2021+.
- Žádost o vydání souhlasného stanoviska odboru OHA může být podána na OHA až po datu a času vyhlášení příslušné výzvy, do které bude projekt předkládán, viz Příloha č. 9 Pravidla pro vydání souhlasného stan. OHA.

Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

Potvrzení o přijetí žádosti o vydání stanoviska odboru Hlavního architekta eGovernmentu

Odbor Hlavního architekta eGovernmentu potvrzuje přijetí žádosti o vydání stanoviska k projektu:

Název projektu:	
Název žadatele:	
Název výzvy Integrovaného regionálního operačního programu:	
Číslo jednací odboru Hlavního architekta eGovernmentu, pod kterým byla žádost o stanovisko zaevidována:	
Datum a čas příjmu žádosti o vydání stanoviska odboru Hlavního architekta eGovernmentu:	

Datum	
Jméno, funkce a podpis osoby oprávněné osoby k vydání potvrzení	

Čestné prohlášení žadatele k souhlasnému stanovisku odboru Hlavního architekta eGovernmentu

Povinnost doložení pro každý projekt, pro který je vydáno souhlasné stanovisko nebo stanovisko o posouzení nerelevatnosti.

Čestné prohlášení žadatele k žádosti o souhlasné stanovisko odboru Hlavního architekta eGovernmentu

Povinnost doložení pro každý projekt, u kterého je dodáno potvrzení o přijetí žádosti o vydání stanoviska OHA.

Kontrolní list

Kontrolní list se dokládá **u všech projektů v aktivitě Kybernetická bezpečnost**. Slouží k posouzení realizace technických bezpečnostních opatření podle VKB.

Pokud předmětem projektu není realizace aktivity Kybernetická bezpečnost, žadatel předloží namísto povinné přílohy dokument, ve kterém uvede, že je pro něj příloha se nerelevantní včetně dostatečného zdůvodnění pro toto tvrzení.

§	Název §	úroveň členění				Text § (pozn. Povinnou osobou se v tomto smyslu rozumí jakýkoliv příjemce IROP v oblasti kybernetické bezpečnosti)	jak/čím bude plněno (uveďte stručný strukturovaný popis, případně uveďte odkaz na příslušnou oblast studie proveditelnosti)	jak/čím je plněno (odkaz na přílohy s důkazy/popisem plnění - prinstcreeny, technická dokumentace, penetrační testy apod.)
						Povinná osoba v rámci fyzické bezpečnosti		
§ 17	Fyzická bezpečnost	a				předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování		
		b				stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a		
		c				u fyzického bezpečnostního perimetru stanoveného podle písmene b) přijme		
		c	1			k zamezení neoprávněnému vstupu,		
		c	2			k zamezení poškození a neoprávněným zásahům a		
		c	3			pro zajištění ochrany na úrovni objektů a v rámci objektů.		
						Povinná osoba pro ochranu bezpečnosti komunikační sítě zahrnuté v rozsahu		
§ 18	Bezpečnost komunikačních sítí	a				zajistí segmentaci komunikační sítě,		
		b				zajistí řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě,		
		c				pomocí kryptografie zajistí důvěrnost a integritu dat při vzdáleném přístupu,		
		d				aktivně blokuje nežádoucí komunikaci a		
		e				pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty		
		1				Povinná osoba používá nástroj pro správu a ověření identity uživatelů,		
		2				Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací zajišťuje		
		2	a			ověření identity před zahájením aktivit v informačním a komunikačním systému,		
		2	b			řízení počtu možných neúspěšných pokusů o přihlášení,		
		2	c			odolnost uložených nebo přenášených autentizačních údajů proti		
		2	d			ukládání autentizačních údajů ve formě odolné proti offline útokům,		
		2	e			opětovné ověření identity po určené době nečinnosti,		
		2	f			dodržení důvěrnosti autentizačních údajů při obnově přístupu a		
		2	g			centralizovanou správu identit.		
		3				Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru		
		4				Do doby splnění požadavku podle odstavce 3 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat autentizaci pomocí kryptografických		
		5				Do doby splnění požadavků podle odstavce 3 nebo 4 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci		
§ 19	Správa a ověřování identit	5	a			délky hesla alespoň		
		5	a	1		12 znaků u uživatelů a		
		5	a	2		17 znaků u administrátorů a aplikací,		
		5	b			umožňující zadat heslo o délce alespoň 64 znaků,		
		5	c			neomezující použití malých a velkých písmen, číslic a speciálních znaků,		
		5	d			umožňující uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla		
		5	e			neumožňující uživatelům a administrátorům		
		5	e	1		zvolit si nejčastěji používaná hesla,		
		5	e	2		tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího		
		5	e	3		opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel		
		5	f			pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto		

Doklad o stanovení kritické informační infrastruktury, významného informačního systému nebo informačního systému základních služeb

Pokud předmětem projektu není realizace aktivity Kybernetická bezpečnost, žadatel předloží namísto povinné přílohy dokument, ve kterém uvede, že je pro něj příloha se nerelevantní včetně dostatečného zdůvodnění pro toto tvrzení.

Přímé výdaje

- pořízení drobného hmotného majetku – HW s výjimkou koncových HW zařízení;
- pořízení drobného nehmotného majetku – SW;
- pořízení dlouhodobého hmotného majetku – HW s výjimkou koncových HW zařízení;
- pořízení dlouhodobého nehmotného majetku – SW;
- cloudová řešení - do doby ukončení realizace projektu;
- výdaje na nákup a pořízení dat;
- nákup vybudovaných komunikačních tras - optických vláken;

Přímé výdaje

- výdaje na koncová zařízení nezbytná pro realizaci technických bezpečnostních opatření;
- výdaje na stavební úpravy a stavební práce na realizaci bezpečnostních technických opatření, zejména opatření fyzické bezpečnosti nebo omezení přístupu k zařízením průmyslových řídicích systémů (zejména stavební úpravy serverovny a související infrastruktury např. za účelem instalace a montáže protipožárního systému, přístupového a zabezpečovacího systému, instalace elektrických rozvodů a zařízení včetně elektrocentrály instalace a montáže klimatizace a vzduchotechniky a s tím související kompletační a dokončovací práce);
- penetrační testy související s pořízeným technickým bezpečnostním opatřením;
- DPH

Nepřímé výdaje

Náklady, které nelze při použití paušální sazby 7 % zahrnout mezi přímé výdaje

- Dokumentace žádosti o podporu – žádost, SP, znalecké posudky, zakázky, ..
- Projektová dokumentace a dokumentace pro realizaci projektu – BOZP, audity, ..
- Administrativní kapacity a řízení projektu – externí služby, účetnictví, archivace,..
- Poplatky – pojištění majetku, ..
- Režijní, provozní a jiné náklady – nájemné, energie, úklid,..
- Publicita projektu
- Další náklady související s projektem – výdaje na koncová zařízení, ostatní náklady související s projektem a nespadající pod přímé výdaje nebo do nezpůsobilých výdajů

Indikátory

- celkem **6** indikátorů
- žadatel vybírá podle realizovaných aktivit
- informace k jednotlivým indikátorům jsou uvedeny v příloze č. 1 Metodické listy indikátorů, která obsahuje:
    - podrobnou specifikaci jednotlivých indikátorů
    - způsob stanovení výchozích a cílových hodnot
    - konkrétní postup výpočtu
    - termíny vykazování dosažených hodnot
    - způsob doložení dosažené hodnoty indikátoru
    - tolerance, ve kterých se indikátory považují za naplněné
    - vazební matici pro výběr indikátorů k jednotlivým aktivitám

Indikátory

305 002 - Počet pořízených informačních systémů

(počet IS)

Indikátor je povinný k výběru a naplnění pro všechny žádosti o podporu, v rámci kterých je realizována aktivita „eGovernment“.

Indikátory

305 150 - Nová funkcionalita informačního systému

(funkcionality)

Indikátor je povinný k výběru a naplnění pro všechny žádosti o podporu, v rámci kterých je realizována aktivita „eGovernment“.

Každý pořízený (nový nebo inovovaný) informační systém musí mít projektem zavedeny minimálně tři nové funkcionality, vybrané z definice indikátoru, popř. uvede vlastní funkcionalitu a ve studii proveditelnosti ji zdůvodní. Novou funkcionalitu a její relevanci posoudí ve svém stanovisku odbor Hlavního architekta eGovernmentu.

Minimální počet tří nových funkcionalit se vztahuje na každý informační systém odděleně.

Indikátory

309 401 - Veřejné instituce podpořené pro účely vývoje digitálních služeb, produktů a procesů

(veřejné instituce)

Indikátor je povinný k výběru a naplnění pro všechny projekty výzvy, v rámci kterých dochází k pořízení informačního systému orgánů územní samosprávy, ostatních orgánů veřejné moci mimo městské podniky a veřejné vysoké školy nebo výzkumné ústavy.

Do indikátoru **nejsou** započítávány instituce, které jsou zakládány za účelem zisku, tj. kapitálové obchodní společnosti, a to akciové společnosti a společnosti s ručením omezeným a dále také nezahrnuje veřejné vysoké školy nebo výzkumné ústavy. Ostatní zapojené instituce se započítávají způsobem 1 IČ = jedna jednotka indikátoru

Indikátory

309 201 - Počet aktivních interních uživatelů systému

(unikátní uživatelé/rok)

Indikátor je povinný k výběru a naplnění pro všechny žádosti o podporu, jejichž součástí je informační systém využívaný interními uživateli. Za uživatele nejsou považováni správci a administrátoři IS.

Indikátory

309 301 - Počet aktivních externích uživatelů systému

(unikátní uživatelé/rok)

Žadatel uvede počet unikátních externích uživatelů z řad veřejnosti pořízených informačních systémů, tj. systémů, kterými je naplňován indikátor výstupu 305 002 - Počet pořízených informačních systémů, kteří systém použili během jednoho roku od ukončení realizace projektu.

Indikátory

304 002 - Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti

(prvek)

- Indikátor je povinný k výběru a naplnění pro všechny žádosti o podporu realizující aktivitu kybernetická bezpečnost.
- Prvkem je technické opatření podle § 5, odst. 3 ZKB

Každý prvek bude do hodnoty indikátoru započítán takto:

a)V případě VIS/ISZS/IS/KS bude každý prvek započítán pro každý systém zvlášť.

b)V případě KII bude prvek započítán pouze jednou pro každou infrastrukturu, bez ohledu na to, kolik jednotlivých systémů obsahuje.

Pokud bude technické opatření sdíleno více KII/VIS/ISZS/IS/KS, bude započítán tolikrát, kolika KII/VIS/ISZS/IS/KS bude sdílen.

Indikátory – vazební matice

Označení a popis aktivity	Možnost kombinace s jinými aktivitami výzvy	Povinnost vybrat indikátor v dané aktivitě	Povinné indikátory k výběru v příslušné aktivitě	Povinný k naplnění
Kybernetická bezpečnost	Ano	Ano	304 002 - Nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti	Ano

...

Indikátory – vazební matice

Označení a popis aktivity	Možnost kombinace s jinými aktivitami výzvy	Povinnost vybrat indikátor v dané aktivitě	Povinné indikátory k výběru v příslušné aktivitě	Povinný k naplnění
Elektronizace vybraných služeb veřejné správy; **Rozšíření propojeného datového fondu;** **Integrace elektronických služeb veřejné správy a informací o službách veřejné správy na portál gov.cz;** **Opatření vedoucí k intenzivnímu využívání existujících bezpečných systémů elektronické identifikace;** **Publikace dat veřejné správy jako OpenData;** **Transakční portálová řešení s využitím zaručené elektronické identity;** **Automatizace zpracování digitálních dat (robotizace);** **Centralizace, standardizace a sdílení elektronických služeb veřejné správy**	Ano	Ano	305 002 - Počet pořízených informačních systémů	Ano
		Pro projekty, v rámci kterých dochází k pořízení IS orgánů územní samosprávy, ostatních orgánů veřejné moci mimo městské podniky a veřejné vysoké školy nebo výzkumné ústavy.	309 401 - Veřejné instituce podpořené pro účely vývoje digitálních služeb, produktů a procesů	Ano
		Ano	305 150 - Nová funkcionalita informačního systému	Ano
		Pro projekty, jejichž součástí je IS využívaný interními uživateli. Za uživatele nejsou považováni správci a administrátoři IS.	309 201 - Počet aktivních interních uživatelů systému	Ano
		Pro projekty, jejichž součástí je informační systém, jehož uživatelé jsou z řad veřejnosti.	309 301 - Počet aktivních externích uživatelů systému	Ano

DĚKUJEME ZA POZORNOST

Řídicí orgán IROP

EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR