ZÁKLADNÍ SHRNUTÍ

Níže jsou sepsána základní pravidla dotační výzvy IROP zaměřené na podporu kyberbezpečnosti (https://irop.gov.cz/cs/vyzvy-2021-2027/vyzvy/4vyzvairop).

Kybernetická bezpečnost – SC 1.1 (120. výzva)

Druh výzvy:	Financování:
Průběžná	**Ex post**
Harmonogram:	Alokace výzvy:
Příjem žádosti od 03/26 až 06/26	**2 142 857 Kč**

Místo realizace:

4.2 4. výzva IROP – PR (přechodové regiony)

Místem realizace projektu je území **přechodových regionů (PR)**, konkrétně:

- Středočeský kraj
- Jihočeský kraj
- Plzeňský kraj
- Jihomoravský kraj
- Kraj Vysočina

V případě projektů Středočeského kraje a jím zřizovaných nebo zakládaných organizací je jako místo realizace přípustné také **hlavní město Praha**.

Oprávnění žadatelé:

5.2 3. výzva IROP – MRR a 4. výzva IROP – PR

Oprávněnými žadateli jsou:

- organizační složky státu (OSS),
- příspěvkové organizace OSS,
- státní organizace,
- kraje,
- obce,
- organizace zřizované nebo zakládané kraji nebo obcemi,
- státní podniky,
- nestátní neziskové organizace zakládané výše uvedenými subjekty,
- subjekty poskytující veřejnou službu v oblasti zdravotní péče dle zákona č. 372/2011 Sb.

Financování

100% pro stát a státní organizace

85% pro kraje, obce a organizace zřizované

70% pro nemocnice, organizace zakládané a státní podniky

6.2 Paušální sazba na nepřímé náklady

Nepřímé náklady jsou hrazeny paušální sazbou ve výši 7 % z celkových způsobilých přímých výdajů projektu.

Podporované aktivity:

7.1 Obecné vymezení podporovaných aktivit

Podpora je určena na technická bezpečnostní opatření vztahující se k:

- kritické informační infrastruktuře (KII),
- významným informačním systémům (VIS),

- informačním systémům základních služeb (ISZS),
- ostatním informačním a komunikačním systémům (IS, KS).

Projekt může zahrnovat:

- zabezpečení jednoho nebo více informačních systémů,
- sdílená technická opatření pro více systémů současně.

7.2 Přehled podporovaných technických bezpečnostních opatření

Podporována jsou zejména tato technická bezpečnostní opatření:

- fyzická bezpečnost (např. zabezpečení serveroven),
- řízení přístupů a identit,
- ověřování identity uživatelů,
- ochrana proti škodlivému kódu,
- detekce a vyhodnocování kybernetických bezpečnostních událostí,
- zaznamenávání činností systémů a uživatelů,
- aplikační bezpečnost,
- kryptografické prostředky,
- zajištění dostupnosti informací,
- bezpečnost průmyslových a řídicích systémů.

Jedno technické opatření může být využito pro více informačních systémů, pro účely finančních limitů se však **započítává pouze jednou**.

Pro projekt stačí jedno technické opatření, ale maximální způsobilé náklady pak budou 20mil Kč.
Maximální počet opatření je 12.

7.3 Omezení podporovaných aktivit

Podpora **není určena** na:

- organizační, procesní a personální opatření (např. školení, směrnice),
- technická opatření realizovaná primárně pro systémy určené k ochraně utajovaných informací (ISOUI),
- aktivity, které nesouvisejí přímo se zabezpečením IS/KS uvedených v projektu.

V případě sdílení technických opatření mezi způsobilými systémy a ISOUI musí být tato skutečnost **jasně popsána ve studii proveditelnosti** a způsobilá část nákladů jednoznačně oddělena.

Podrobněji viz pravidla Výzvy.

Specifická kritéria a podmínky:

Projekty předkládané do Kybernetická bezpečnost musí splňovat **soubor specifických kritérií a podmínek**, které vyplývají ze Specifických pravidel pro žadatele a příjemce. Nesplnění těchto podmínek vede k **vyřazení projektu z dalšího hodnocení**.

8.1 Zaměření projektu

Projekt musí být zaměřen **výhradně na technická bezpečnostní opatření** dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Není přípustné, aby byl projekt zaměřen primárně na:

- organizační opatření,
- procesní opatření,
- personální opatření,
- vzdělávání nebo školení.

Technická opatření musí být **hlavním a jednoznačně identifikovatelným výstupem projektu**.

8.2 Vazba na informační systémy

Projekt musí jasně definovat:

- **konkrétní informační a komunikační systémy**, které jsou projektem zabezpečovány,
- jejich zařazení (KII / VIS / ISZS / IS / KS),
- vazbu jednotlivých technických opatření na tyto systémy.

Každé technické opatření musí být:

- věcně odůvodněno,
- popsáno ve studii proveditelnosti,
- přiřazeno ke konkrétnímu systému nebo skupině systémů.

8.3 Finanční limity technických opatření

Výše způsobilých výdajů projektu je **limitována počtem realizovaných technických bezpečnostních opatření**.

Jedno technické opatření se započítává **pouze jednou**, i v případě, že je využito pro více informačních systémů.

Překročení finančních limitů bez odpovídajícího navýšení počtu technických opatření je **nepřípustné**.

8.4 Vztah k systémům určeným k ochraně utajovaných informací (ISOUI)

Projekt **nesmí být zaměřen primárně** na zabezpečení systémů určených k ochraně utajovaných informací dle zákona č. 412/2005 Sb.

Pokud jsou technická opatření:

- **sdílena mezi ISOUI a ostatními IS/KS**,
  musí být:
- tato skutečnost popsána ve studii proveditelnosti,
- způsobilá část nákladů jednoznačně vymezena.

Způsobilost nákladů:

9.1 Celkové způsobilé výdaje (CZV)

Celkové způsobilé výdaje projektu jsou tvořeny:

CZV = přímé způsobilé výdaje + paušální sazba na nepřímé výdaje (7 %)

Výše CZV musí odpovídat:

- schválenému rozpočtu projektu,
- počtu realizovaných technických bezpečnostních opatření,
- finančním limitům stanoveným Specifickými pravidly.

9.2 Přímé způsobilé výdaje

Za přímé způsobilé výdaje jsou považovány zejména náklady přímo související s realizací technických bezpečnostních opatření, konkrétně:

- pořízení hardwaru a softwaru nezbytného k realizaci technických bezpečnostních opatření,
- pořízení licencí (časově omezených i trvalých, v souladu s pravidly IROP),
- dodávky a implementace bezpečnostních technologií,
- pořízení technologií pro:
  - řízení přístupů a identit,
  - detekci a vyhodnocování kybernetických bezpečnostních událostí,
  - ochranu proti škodlivému kódu,
  - kryptografickou ochranu,

    - aplikační bezpečnost,
    - zajištění dostupnosti informací,
    - bezpečnost průmyslových a řídicích systémů,
- nezbytné stavební úpravy související s instalací technologií (např. úpravy serveroven),
- DPH, pokud je pro příjemce **nezpůsobilá k odpočtu**.

Přímé způsobilé výdaje musí být:

- účelné,
- hospodárné,
- efektivní,
- přímo přiřaditelné ke konkrétním technickým opatřením.

9.3 Nepřímé výdaje (paušální sazba)

Nepřímé výdaje jsou hrazeny **paušální sazbou ve výši 7 %** z celkových způsobilých přímých výdajů projektu.
Nepřímé výdaje zahrnují zejména:

- administraci projektu,
- řízení projektu,
- režijní náklady,
- publicitu projektu,
- další podpůrné činnosti související s realizací projektu.

Nepřímé výdaje:

- **nejsou dokládány účetními doklady**,
- **nesmí být uplatněny zároveň jako přímé výdaje**.

9.4 Nezpůsobilé výdaje

Za nezpůsobilé výdaje jsou považovány zejména:

- náklady nesouvisející přímo s realizací projektu,
- organizační, procesní a personální opatření (např. školení, tvorba směrnic),
- výdaje na technická opatření realizovaná primárně pro systémy určené k ochraně utajovaných informací (ISOUI),
- úroky z úvěrů a půjček,
- pokuty, penále a sankce,
- výdaje vzniklé mimo období časové způsobilosti,
- DPH, pokud je nárok na její odpočet.

Podrobněji viz pravidla Výzvy.

Výčet povinných příloh (podrobně viz specifická pravidla výzvy):

1. **Plná moc**
2. **Zadávací a výběrová řízení**
3. **Doklad o právní subjektivitě žadatele**
4. **Studie proveditelnosti**
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**
8. **Znalecký posudek**
9. **Projektová dokumentace stavby**
10. **Rozpočet stavebních prací**

11. **Povinné přílohy prokazující vyhodnocení žadatele z pohledu podniku v obtížích**
12. **Podklady pro stanovení kategorií intervencí a kontrolu limitů**
13. **Smlouva o zřízení bankovního účtu**
14. **Souhlasné stanovisko odboru Hlavního architekta eGovernmentu (OHA) – stačí podání žádosti**
15. **Čestné prohlášení žadatele k souhlasnému stanovisku OHA**
16. **Čestné prohlášení žadatele k žádosti o souhlasné stanovisko OHA**
17. **Kontrolní list**
18. **Pověřovací akt**
19. **Doklad o stanovení KII / VIS / ISZS**
20. **Stanovení hodnoty indikátoru 304 002**
21. **Výpis z Evidence skutečných majitelů**

Podrobněji viz pravidla Výzvy.