Úrad pre reguláciu elektronických komunikácií a poštových služieb, Továrenská 7,
P. O.BOX 40, 828 55 Bratislava

zadávanie podlimitnej zákazky postupom

verejná súťaž
podľa § 112 až 114 a § 116 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“) s využitím pravidla uvedeného v § 112 ods. 7 písm. b) ZVO

Súťažné podklady

"Implementácia technických opatrení a organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti"

Vypracoval: Mgr. Ľudovít Blázy, referent VO

V Bratislave, dňa 28. októbra 2022

A.1 Pokyny pre uchádzačov

Časť I.
Všeobecné informácie

1. Identifikácia verejného obstarávateľa

Verejný obstarávateľ

Názov organizácie: Úrad pre reguláciu elektronických komunikácií a poštových služieb
Adresa organizácie: Továrenská 7, P. O. BOX 40, 828 55 Bratislava, Slovenská republika
Zastúpený: Ing. Ivan Marták, predseda úradu
IČO: 42 355 818
DIČ: 2024003729
Adresa profilu verejného obstarávateľa: https://www.uvo.gov.sk/vyhladavanie-profilov/detail/15002
Právna forma: rozpočtová organizácia
Web organizácie (URL): www.teleoff.gov.sk
Kontaktná osoba: Mgr. Ľudovít Blázy, referent verejného obstarávania
Telefón: +421 2 57881352
E-mail: ludovit.blazy@teleoff.gov.sk

2.Predmet zákazky

2.1 Názov predmetu zákazky**: Implementácia technických opatrení a organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti**

2.2 Číselný kód pre hlavný predmet a doplňujúce predmety zákazky z Hlavného slovníka, prípadne alfanumerický kód z Doplnkového slovníka Spoločného slovníka obstarávania (CPV):
Hlavný predmet:
72220000-3 Systémové a technické poradenstvo

Doplňujúce predmety:
72250000-2 Služby týkajúce sa podpory systému
72263000-6 Implementácia softvéru
72260000-5 Služby súvisiace so softvérom

2.3 V zmysle § 3 ods. 5 zákona č. 343/2015 Z. z. o verejnom obstarávaní (ďalej len "zákon o verejnom obstarávaní") sa týmto obstarávaním zadáva civilná zákazka (ďalej len zákazka).

2.4 Predmet zákazky:
V rámci analýzy a implementácie technických opatrení v súlade so zákonom č.69/2018 Z. z. o kybernetickej bezpečnosti požaduje verejný obstarávateľ zabezpečenie vytvorenia analytických výstupov a súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu:
1.Analýza stavu a príprava pre log management + mapovanie zdrojov
2.Príprava zadaní a mapovanie zdrojov pre implementáciu SIEM, kontrola kvality
3.Analytická príprava a technické možnosti na dvojfaktorovú autentifikáciu pre vzdialene prístupy
4.Analýza a implementácia procesov riadenia zraniteľností - vulnerability manažment
5. Analytická príprava a možnosti pre mobile device management
6.Plánovanie kontinuity činností, vypracovanie návrhu Stratégie kontinuity a vytvorenie plánov kontinuity, Havarijné plánovanie, DRP disaster recovery plány
7.Integrácia na Vládny informačný systém kybernetickej bezpečnosti (VISKB).

V rámci implementácie organizačných opatrení v súlade so zákonom č.69/2018 Z. z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia interných smerníc ako i súvisiacej dokumentácie a to:
1. Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov
2. Inventarizácia, klasifikácia a kategorizácia informačných aktív
3. Vzdelávanie a príprava vzdelávacích materiálov pre IT aj neIT zamestnancov
4.Vykonanie analýzy rizík kybernetickej bezpečnosti a návrh na riadenie rizík
5.Analýza zmluvných vzťahov s tretími stranami z pohľadu KB, adaptácia odporúčaní do zmlúv
6.Plán kontrol, interných auditov, compliance management

Podrobné vymedzenie predmetu zákazky vrátane vypracovaných technických špecifikácií je uvedené v časti "B.1 Opis predmetu zákazky".

3. Rozdelenie predmetu zákazky

Predmet zákazky je rozdelený na časti : áno

Časť 1. : Implementácia technických opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

Časť 2: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

Uchádzači sú oprávnení predložiť ponuku súčasne na obe časti predmetu zákazky, prípadne len na jednu časť predmetu zákazky.

4. Variantné riešenie

4.1 Uchádzačom sa neumožňuje predložiť variantné riešenie vo vzťahu k žiadnej z častí predmetu zákazky.

4.2 Ak súčasťou ponuky bude aj variantné riešenie, na túto ponuku sa nebude prihliadať a takéto variantné riešenie nebude zaradené do vyhodnotenia ponúk.

5. Pôvod predmetu zákazky

Uchádzač, jeho prípadní subdodávatelia a ním ponúkané tovary musia spĺňať požiadavky na pôvod stanovené všeobecne záväznými právnymi aktmi Európskej únie, príslušnými medzinárodnými zmluvami a dohodami.

6. Miesto dodania predmetu zákazky a lehoty uskutočnenia

6.1 Miesto dodania predmetu zákazky: Úrad pre reguláciu elektronických komunikácií a poštových služieb, Továrenská 7, Bratislava, pokiaľ nie je v objednávke stanovené inak.

6.2 Lehota na dodanie predmetu zákazky: **6 mesiacov od účinnosti zmluvy** (platí pre každú časť predmetu zákazky)

7. Zdroj finančných prostriedkov a predpokladaná hodnota zákazky

7.1 Predmet zákazky bude financovaný v zmysle pravidiel operačného programu Integrovaná infraštruktúra v rámci projektu: 2021/11 Kybernetická bezpečnosť, podľa Zmluvy č. Z311071BQB8 o poskytnutí NFP.

7.2 Predpokladaná hodnota zákazky určená na základe zdokumentovaného prieskumu trhu je **109 980,-EUR bez DPH,** pričom

Pre Časť 1 zákazky: Implementácia technických opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti je PHZ vo výške 59 700,-EUR bez DPH.

Pre Časť 2 zákazky: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti je PHZ vo výške 50 280,-EUR bez DPH.

7.3 Vlastná platba bude realizovaná formou bezhotovostného platobného styku, na základe daňového dokladu - faktúry vystaveného úspešným uchádzačom, splatnosť ktorého je 60 dní odo dňa jeho doručenia verejnému obstarávateľovi.

8. Typ zákazky a zmluva

8.1 Zákazka na poskytnutie služieb podľa § 3 ods. 2 ZVO.

8.2 Výsledkom tejto súťaže bude zmluva v zmysle § 269 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov uzatvorená samostatne pre každú časť zákazky.

8.3 Podrobné vymedzenie zmluvných podmienok na dodanie požadovaného predmetu zákazky je uvedené v návrhu zmluvy ktorá tvorí Prílohu č. 5 týchto súťažných podkladov. Uchádzač je povinný akceptovať znenie navrhnutých obchodných podmienok, ktoré sú súčasťou súťažných podkladov.

9. Lehota viazanosti ponuky

9.1 Uchádzač je svojou ponukou viazaný počas lehoty viazanosti ponúk. Lehota viazanosti ponúk plynie od uplynutia lehoty na predkladanie ponúk do uplynutia lehoty viazanosti ponúk stanovenej verejným obstarávateľom.

9.2 Lehota viazanosti ponúk je stanovená do **31. 03. 2023.**

9.3 V prípade uplatnenia revíznych postupov v zmysle § 163 a nasl. ZVO alebo iných okolností, verejný obstarávateľ oznámi uchádzačom predpokladané predĺženie lehoty viazanosti ponúk.

9.4 Uchádzači sú svojou ponukou viazaní do uplynutia verejným obstarávateľom oznámenej, prípadne primerane predĺženej lehoty viazanosti ponúk.

9.5 Úrad pre reguláciu elektronických komunikácií a poštových služieb si vyhradzuje právo uzavrieť zmluvu v predĺženej lehote viazanosti ponúk.

Časť II.
Dorozumievanie a vysvetľovanie

10. Dorozumievanie medzi verejným obstarávateľom a záujemcami/uchádzačmi

10.1 V súlade § 20 ZVO sa bude elektronická komunikácia vrátanie doručovania v tejto verejnej súťaži uskutočňovať spôsobom určeným funkcionalitou elektronického prostriedku, prostredníctvom ktorého sa toto verejné obstarávanie realizuje, t. j. komunikácia a výmena informácií sa bude uskutočňovať v písomnej forme, výhradne prostredníctvom elektronického prostriedku informačného systému elektronického verejného obstarávania (ďalej len „IS EVO“) (https://www.uvo.gov.sk/portalsystemu-evo-5f5.html).

10.2 Postup záujemcu / uchádzača je upravený v príručkách pre záujemcu / uchádzača, ktoré sú zverejnené na stránke portálu IS EVO v položke menu Príručky (https://www.uvo.gov.sk/portal-systemu-evo5f7.html).

10.3 Komunikácia sa bude uskutočňovať výhradne v slovenskom jazyku prípadne v českom jazyku a to písomnou formou v elektronickej podobe prostredníctvom systému IS EVO.

10.4 Pri elektronickej komunikácii v IS EVO sa považuje elektronická správa/informácia/oznámenie/písomnosť/žiadosť o vysvetlenie (ďalej len „informácia“)za doručenú v okamihu jej odoslania verejným obstarávateľom v IS EVO. Odoslaním dochádza automaticky k doručeniu informácie záujemcovi/uchádzačovi na jeho používateľské konto. Doručenie informácie IS EVO vykonáva automaticky v danom okamihu odoslania, pričom IS EVO automaticky zasiela/generuje príjemcovi notifikačný e-mail o doručení informácie, čo je zaznamenané aj v auditnom zázname IS EVO.

10.5 Akákoľvek komunikácia so záujemcami, ktorí sú evidovaní na elektronickom liste záujemcov pri danej zákazke alebo s uchádzačmi, ktorá bude realizovaná prostredníctvom systému EVO, bude zasielaná na záujemcom/uchádzačom určený kontaktný email (zadaný pri registrácii do systému EVO).

10.6 Ak záujemca alebo uchádzač, zašle informáciu inými prostriedkami, napr. e-mailom, verejný obstarávateľ nebude na takúto formu komunikácie prihliadať.

10.7 V zmysle § 164 ods. 3 písm. a) ZVO uchádzač, záujemca alebo osoba, ktorej práva alebo právom chránené záujmy boli alebo mohli byť dotknuté postupom obstarávateľa môže podať žiadosť o nápravu prostredníctvom funkcionality IS EVO.

11. Vysvetľovanie a doplnenie súťažných podkladov

11.1 Záujemca môže požiadať verejného obstarávateľa o vysvetlenie súťažných podkladov, informatívneho dokumentu alebo inej sprievodnej dokumentácie a to v primeranej lehote v elektronickej podobe cez systém IS EVO.

11.2 O odoslaní vysvetlenia budú všetci záujemcovia zaregistrovaní v IS EVO upozornení notifikačným e-mailom IS EVO. Vysvetlenie alebo doplnenie dokumentov potrebných na vypracovanie ponuky a na preukázanie splnenia podmienok účasti budú zverejnené a sprístupnené v IS EVO.

11.3 Vysvetlenie každej žiadosti o vysvetlenie, predloženej podľa bodov 11.1, sa oznámi podľa bodu 11.2 bezodkladne s prihliadnutím na primeraný čas na kvalifikované vypracovanie vysvetlenia všetkým záujemcom, ktorým verejný obstarávateľ poskytol súťažné podklady najneskôr však **tri pracovné dní** pred uplynutím lehoty na predkladanie ponúk, za predpokladu, že o vysvetlenie sa požiada dostatočne vopred.

11.4. Za dostatočne vopred doručenú žiadosť záujemcu o vysvetlenie sa považuje žiadosť doručená v odporúčanej lehote do **11.11.2022** prostredníctvom IS EVO. V prípade, že záujemca požiada o vysvetlenie po uplynutí odporúčanej lehoty, verejný obstarávateľ poskytne vysvetlenie záujemcom, avšak dôrazne upozorňuje, že v takomto prípade nezaručuje, že záujemca bude mať doručené vysvetlenie do uplynutia lehoty na predkladanie ponúk, čím preberá záujemca na seba riziko, že nestihne poskytnuté vysvetlenie zapracovať do svojej ponuky. Verejný obstarávateľ v takom prípade nie je povinný predĺžiť lehotu na predkladanie ponúk.

12. Obhliadka miesta dodania predmetu zákazky

Obhliadka miesta dodania predmetu zákazky sa neuskutoční.

Časť III.
Príprava ponuky

13. Vyhotovenie ponuky

13.1. Ponuka musí byť vyhotovená a predložená v elektronickej podobe vo formáte, ktorá zabezpečí trvalé zachytenie jej obsahu a predložená prostredníctvom funkcionality IS EVO.

13.2. Dokumenty a doklady, ktoré tvoria ponuku uchádzača a ktoré neboli pôvodne vyhotovené v elektronickej forme, ale v listinnej, sa prostredníctvom systému IS EVO predkladajú zoskenované.

13.3. Dokumenty a doklady, ktoré tvoria ponuku uchádzača a ktoré boli pôvodne vyhotovené v elektronickej forme sa prostredníctvom systému IS EVO predkladajú v pôvodnej elektronickej podobe.

13.4 Verejný obstarávateľ alebo obstarávateľ môže kedykoľvek počas priebehu verejného obstarávania požiadať uchádzača o predloženie originálu príslušného dokumentu, úradne osvedčenej kópie originálu príslušného dokumentu alebo zaručenej konverzie, ak má pochybnosti o pravosti predloženého dokumentu alebo ak je to potrebné na zabezpečenie riadneho priebehu verejného obstarávania.

14. Jazyk ponuky

Ponuky, návrhy a ďalšie doklady a dokumenty vo verejnom obstarávaní sa predkladajú v štátnom jazyku a môžu sa predkladať aj v českom jazyku. Ak je doklad alebo dokument vyhotovený v inom ako štátnom jazyku alebo českom jazyku, predkladá sa spolu s jeho úradným prekladom do štátneho jazyka. Ak sa zistí rozdiel v obsahu dokladu alebo dokumentu predloženom podľa druhej vety, rozhodujúci je úradný preklad do štátneho jazyka.

15. Mena a ceny uvádzané v ponuke, mena finančného plnenia

15.1. Uchádzačom navrhované zmluvné ceny za požadovaný predmet zákazky budú vyjadrené v európskych menových jednotkách (ďalej len EUR) a stanovené podľa § 3 zákona NR SR č.18/1996 Z. z. o cenách v znení neskorších predpisov, vyhlášky MF SR č. 87/1996 Z. z., ktorou sa vykonáva zákon NR SR č. 18/1996 Z. z. o cenách. Zmluvné ceny nesmú byť viazané na inú menu alebo parameter.

15.2. Záujemca je pred predložením svojej ponuky povinný vziať do úvahy všetko, čo je nevyhnutné na úplné a riadne plnenie zmluvy, pričom do svojich cien zahrnie všetky náklady spojené s plnením predmetu zákazky. Uchádzač ku každej oceňovanej položke uvedie v navrhovanej zmluvnej cene aj jednotkovú cenu. Uchádzač musí vyplniť príslušnú tabuľku Návrhy na plnenie kritérií tak, aby každá požadovaná cenová položka mala uvedenú číselnú hodnotu.

15.3. Ak je uchádzač platiteľom dane z pridanej hodnoty (ďalej len „DPH“), t. j. zdaniteľnou osobou pre DPH v zmysle príslušných predpisov (ďalej len „zdaniteľná osoba“), navrhovanú zmluvnú cenu v štruktúrovanom rozpočte ceny zmluvy uvedie v zložení:

- navrhovaná zmluvná cena v EUR bez DPH,
- sadzba DPH v %,
- výška DPH v EUR,
- navrhovaná zmluvná cena v EUR vrátane DPH.

15.4. Ak uchádzač nie je zdaniteľnou osobou pre DPH, uvedie navrhovanú zmluvnú cenu, ako aj všetky ostatné ceny, ktoré sú v týchto súťažných podkladoch požadované uvádzať bez DPH ako celkovú konečnú cenu. Skutočnosť, že nie je zdaniteľnou osobou pre DPH, uchádzač uvedie v ponuke.

15.6. Všetky ceny uvádzané v ponuke uchádzača sú navrhovanými zmluvnými cenami a musia byť vypracované presne podľa časti A3. Kritériá hodnotenia týchto súťažných podkladov.

15.7. **Uchádzač uvedie cenu do formulára, ktorý tvorí Prílohu č. 5: Návrh na plnenie kritérií, týchto Súťažných podkladov a to samostatne pre každú časť zákazky pre ktorú predkladá ponuku.**

16. Zábezpeka ponuky

16.1. Zábezpeka sa nevyžaduje.

Časť IV.
Obsah ponuky

17. Obsah ponuky

17.1. Uchádzač môže predložiť iba jednu ponuku vyhotovenú podľa bodu 13. týchto súťažných podkladov, ktorá musí obsahovať:

i. Vyplnený „Formulár na predloženie ponuky“ uvedený v Prílohe č.1 týchto súťažných podkladov. Formulár bude podpísaný oprávnenou osobou za uchádzača. V prípade, že uchádzač predkladá ponuku pre obe časti predmetu zákazky, Formulár na predloženie ponuky stačí predložiť raz (x)

ii. potvrdenia, doklady a dokumenty, prostredníctvom ktorých uchádzač preukazuje splnenie podmienok účasti týkajúcich sa osobného postavenia a technickej a odbornej spôsobilosti požadovaných v oznámení o vyhlásení verejného obstarávania a v týchto súťažných podkladoch v časti A2; v prípade, že uchádzač využije možnosť predkladania konkrétnych dokladov na preukázanie splnenia podmienok účasti, je povinný originálne doklady alebo ich úradne overené kópie (vrátane úradných prekladov) naskenovať a vložiť ich do systému ako súčasť ponuky. V prípade, že sú doklady ktorými uchádzač preukazuje splnenie podmienok účasti vydávané orgánom verejnej správy (alebo inou povinnou inštitúciou) priamo v digitálnej podobe, môže uchádzač vložiť do systému tento digitálny doklad (vrátane jeho úradného prekladu),

iii. v prípade, ak sú dokumenty v ponuke podpísané osobou inou ako je štatutárny orgán alebo člen štatutárneho orgánu uchádzača, verejný obstarávateľ požaduje predložiť splnomocnenie pre zástupcu uchádzača, ktorý je oprávnený konať v mene uchádzača v záväzkových vzťahoch,

iv. v prípade skupiny dodávateľov podľa bodu 19.1 týchto súťažných podkladov, splnomocnenie pre člena skupiny dodávateľov, ktorý má právnu subjektivitu a spôsobilosť na právne úkony v plnom rozsahu, na uskutočňovanie všetkých právnych úkonov týkajúcich sa ponuky, ktorú táto skupina dodávateľov predloží v rámci tohto verejného obstarávania a týkajúcich sa účasti tejto skupiny dodávateľov v rámci tohto verejného obstarávania, podpísanú všetkými členmi skupiny alebo osobou/osobami oprávnenými konať v danej veci za každého člena skupiny (Vzor je uvedený v Prílohe č. 2.: Splnomocnenie pre osobu konajúcu za skupinu dodávateľov),

v. návrh Obchodných podmienok (zmluvy) na dodanie predmetu zákazky podľa Prílohy č. 4 týchto súťažných podkladov, podpísaný uchádzačom, jeho štatutárnym orgánom alebo členom štatutárneho orgánu alebo iným zástupcom uchádzača, ktorý je oprávnený konať v mene uchádzača, po doplnení údajov vyznačených v zmluve, a to samostatne pre každú časť predmetu zákazky, pre ktorú uchádzač predkladá ponuku

vi. vyplnený Návrh na plnenie kritérií, vypracovaný v súlade s týmito súťažnými podkladmi (Vzor návrhu je uvedený v Prílohe č. 5: Návrh na plnenie kritérií) a to samostatne pre každú časť predmetu zákazky, pre ktorú uchádzač predkladá ponuku

vii.

viii. uvedenie podielu zákazky, ktorú má uchádzač v úmysle zadať subdodávateľom, navrhovaných subdodávateľov a predmet subdodávok vypracovaný podľa Prílohy č. 3 - Vyhlásenie o subdodávateľoch, a to samostatne pre každú časť predmetu zákazky, pre ktorú uchádzač predkladá ponuku. Pri navrhovaných subdodávateľoch uvedie podiel zákazky (subdodávky) vo finančnom vyjadrení (EUR), názov/ obchodné meno/ meno a priezvisko, sídlo/ miesto podnikania/ adresa pobytu, IČO/ dátum narodenia ak nebolo IČO pridelené.

Časť V.
Predkladanie ponuky

18. Náklady na ponuku

18.1 Všetky náklady a výdavky spojené s prípravou a predložením ponuky znáša uchádzač bez finančného nároku voči verejnému obstarávateľovi, bez ohľadu na výsledok verejného obstarávania.

19. Uchádzač oprávnený predložiť ponuku

19.1. Uchádzačom môže byť aj skupina fyzických osôb/právnických osôb vystupujúcich voči verejnému obstarávateľovi spoločne. Skupina dodávateľov nemusí vytvoriť právne vzťahy, musí však stanoviť vedúceho člena (ďalej aj „lídra“) skupiny dodávateľov. Všetci členovia takejto skupiny dodávateľov utvorenej na dodanie predmetu zákazky musia udeliť plnú moc lídrovi skupiny, ktorý bude konať v mene ostatných členov skupiny v rámci tejto súťaže ako napr. prijímať pokyny v tomto verejnom obstarávaní ako aj konať v mene skupiny pre prípad prijatia ich ponuky, podpisu zmluvy a komunikácie/zodpovednosti v procese plnenia zmluvy. V prípade prijatia ponuky skupiny dodávateľov sa vyžaduje, aby skupina dodávateľov z dôvodu riadneho plnenia zmluvy uzatvorila a predložila verejnému obstarávateľovi zmluvu v súlade s platnými právnymi predpismi, ktorá bude zaväzovať zmluvné strany, aby ručili spoločne za záväzky voči verejnému obstarávateľovi vzniknuté pri realizácii predmetu zákazky.

19.2. Uchádzač môže predložiť iba jednu ponuku. Ak uchádzač v lehote na predkladanie ponúk predloží viac ponúk, verejný obstarávateľ alebo obstarávateľ prihliada len na ponuku, ktorá bola predložená ako posledná a na ostatné ponuky hľadí rovnako ako na ponuky, ktoré boli predložené po lehote na predkladanie ponúk.

20. Predloženie ponuky

20.1. Uchádzač predloží ponuku v lehote na predkladanie ponúk podľa bodu 22.1. tejto kapitoly súťažných podkladov v zmysle § 49 ods. 1 písm. a) ZVO elektronicky prostredníctvom IS EVO. Elektronická ponuka musí byť predložená prostredníctvom „Sprievodného listu“ vytvoreného IS EVO.

20.2 V prípade, že subjekt (uchádzač) ešte nie je zaregistrovaný v privátnej zóne na portáli www.uvo.gov.sk, pre účasť na elektronickom verejnom obstarávaní, resp. komunikáciu v IS EVO a pre elektronické predkladanie ponuky prostredníctvom IS EVO, je potrebné vykonať registráciu subjektu v privátnej zóne.

20.3 Pri predkladaní ponuky uchádzač postupuje podľa príručky zverejnenej na stránke portálu IS EVO v položke menu Príručky (https://www.uvo.gov.sk/viac-o-is-evo/prirucky-5f7.html).

20.4 Uchádzač môže predložiť iba jednu ponuku vyhotovenú podľa týchto súťažných podkladov. Ak uchádzač v lehote na predkladanie ponúk predloží viac ponúk, obstarávateľ prihliada len na ponuku, ktorá bola predložená ako posledná.

20.5. Funkcionalita IS EVO neumožňuje predložiť elektronickú ponuku po uplynutí lehoty na predkladanie ponúk uvedenej v bode 22.1.

20.6. Na zabezpečenie ochrany osobných údajov a dôverných informácií tvoriacich obsah ponuky, uchádzač elektronicky predloží aj kópiu časti ponuky podľa bodu 17.1 ii vo formáte Portable Document Format (.pdf) v takom vyhotovení, ktoré umožní nezverejnenie dôverných informácií alebo osobných údajov v zmysle noriem ochrany osobných údajov (napríklad s vynechaným textom tvoriacim dôverné informácie). Ak ide o dokumenty, ktoré sú podpísané alebo obsahujú odtlačok pečiatky, predkladajú sa v elektronickej podobe s uvedením mena a priezviska osôb, ktoré dokumenty podpísali a dátumu podpisu, bez uvedenia podpisu týchto osôb a odtlačku pečiatky.

21. Lehota na predkladanie ponuky

21.1. Lehotu na predkladanie ponúk verejný obstarávateľ stanovil nasledovne: **21. november 2022 do 12:00 hod.**

22. Doplnenie, zmena a odvolanie ponuky

22.1.Uchádzač môže predloženú ponuku stiahnuť, resp. vymazať prostredníctvom funkcionality webovej aplikácie EVO do uplynutia lehoty na predkladanie ponúk podľa bodu 21.3 tejto časti súťažných podkladov. Predloženie novej ponuky je možné vykonať prostredníctvom funkcionality webovej aplikácie EVO až po jej predchádzajúcom stiahnutí, resp. vymazaní (kliknutím na tlačidlo „Stiahnuť ponuku“ a predložením novej ponuky).

22.2 Pre doplnenie alebo zmenu elektronickej ponuky sú záväzné a určujúce aktuálne platné pokyny a príručky, voľne dostupné na portáli UVO: https://www.uvo.gov.sk/viac-o-is- evo/prirucky-5f7.html

Časť VI.
Vyhodnotenie ponuky

23. Otváranie ponúk

23.1. Otváranie ponúk sa uskutoční v jednej fáze.

23.2. Otváranie ponúk sa uskutoční dňa **21. novembra 2022 o 12:15 hod.**

23.3 Otváranie ponúk je prístupné iba uchádzačom, ktorí predložili ponuku v lehote na predkladanie ponúk. Prístupnosťou otvárania ponúk pre uchádzačov sa rozumie ich sprístupnenie prostredníctvom funkcionality IS EVO všetkým uchádzačom, ktorí predložili ponuku určeným spôsobom komunikácie. Otváranie ponúk sa vzhľadom na uvedené realizuje bez fyzickej prítomnosti uchádzačov.

23.4 Na otváraní ponúk sa zverejňuje iba počet predložených ponúk a návrhy na plnenie kritérií, ktoré sa dajú vyjadriť číslom. Ostatné údaje uvedené v ponuke vrátane obchodného mena alebo názvu, sídla, miesta podnikania alebo adresy pobytu všetkých uchádzačov sa nezverejňujú.

23.5 Verejný obstarávateľ najneskôr do piatich pracovných dní odo dňa otvárania ponúk pošle všetkým uchádzačom, ktorí predložili ponuky v lehote na predkladanie ponúk, zápisnicu z otvárania ponúk, ktorá obsahuje údaje zverejnené na otváraní ponúk podľa bodu 23.4 tejto časti súťažných podkladov.

24. Preskúmanie a hodnotenie ponúk

Verejný obstarávateľ vyhodnotí ponuky v súlade s § 112 ods. 7 písm. b) a § 55 ods. 1 ZVO, t. j. vyhodnotenie ponúk z hľadiska splnenia požiadaviek na predmet zákazky a vyhodnotenie splnenia podmienok účasti sa uskutoční až po vyhodnotení ponúk na základe kritérií na vyhodnotenie ponúk u uchádzača, ktorý sa umiestnil na prvom mieste (tzv. superreverzná súťaž). V prípade vylúčenia uchádzača umiestneného na prvom mieste v poradí postupuje obstarávateľ pri vyhodnocovaní ponúk uchádzača/uchádzačov umiestnených ako ďalších v

poradí, analogicky tak, že vždy vyhodnocuje ďalšieho uchádzača umiestneného ako prvého v poradí v novo zostavenom poradí.

25. Oprava chýb

25.1. Zrejmé matematické chyby zistené pri skúmaní ponúk sú:

25.1.1 Rozdiel medzi sumou uvedenou číslom a sumou uvedenou slovom,

25.1.2 Rozdiel medzi jednotkovou cenou a celkovou cenou, ak uvedená chyba vznikla dôsledkom nesprávneho násobenia jednotkovej ceny množstvom, platiť bude jednotková cena,

25.1.3 Nesprávne spočítaná suma vo vzájomnom súčte alebo v medzisúčte jednotlivých položiek; platiť bude správny súčet, resp. medzisúčet jednotlivých položiek a pod,

25.1.4 Iné zrejmé chyby v písaní a počítaní.

25.2. Komisia písomne požiada uchádzača o vysvetlenie ponuky s cieľom odstránenia zrejmých matematických chýb v ponuke zistených pri jej vyhodnocovaní.

25.3. Do procesu hodnotenia ponúk nebude zaradená a bude vylúčená ponuka uchádzača:

25.3.1 Ak uchádzač neakceptuje opravenú sumu vzniknutú zrejmou matematickou chybou.

25.3.2 Ak uchádzač nedoručí písomné vysvetlenie v lehote dvoch pracovných dní odo dňa odoslania žiadosti o vysvetlenie, pokiaľ komisia neurčila dlhšiu lehotu.

25.4. Uchádzač bude písomne upovedomený o vylúčení jeho ponuky podľa ustanovení bodu 26.3. týchto súťažných podkladov s uvedením dôvodu vylúčenia a lehoty, v ktorej môže byť podaná námietka.

26. Vyhodnocovanie ponúk

26.1. Komisia po zostavení poradia uchádzačov na základe nimi predložených kritérií na vyhodnotenie ponúk u uchádzača umiestneného na prvom mieste v poradí preskúma či ponuka uchádzača umiestneného na prvom mieste v poradí:

26.1.1. obsahuje všetky doklady a dokumenty určené v bode 17. tejto kapitoly súťažných podkladov,

26.1.2. zodpovedá pokynom a požiadavkám uvedeným vo Výzve na predkladanie ponúk a v týchto súťažných podkladoch.

26.2. Ak komisia identifikuje nezrovnalosti alebo nejasnosti v informáciách alebo dôkazoch, ktoré uchádzač poskytol, písomne požiada o vysvetlenie ponuky uchádzača umiestneného na prvom mieste v poradí podľa § 53 ods. 1 ZVO. Vysvetlením ponuky nemôže dôjsť k jej zmene. Za zmenu ponuky sa nepovažuje odstránenie zrejmých chýb v písaní a počítaní.

26.3 V prípade, ak sa javí ponuka uchádzača umiestneného na prvom mieste v poradí ako mimoriadne nízka vo vzťahu k predmetu zákazky, obstarávateľ písomne požiada uchádzača o vysvetlenie týkajúce sa tej časti ponuky, ktoré sú pre jej cenu podstatné v súlade s ustanoveniami § 53 ods. 2 a 6 ZVO.

26.4. Z procesu vyhodnocovania bude vylúčená ponuka uchádzača, ak bude naplnená niektorá z podmienok uvedených v ustanovení § 53 ods. 5 ZVO.

26.5. Uchádzač bude upovedomený o vylúčení jeho ponuky s uvedením dôvodu vylúčenia a v prípade, ak sa jedná o zákazku, v ktorej je možné podať námietku aj s uvedením lehoty, v ktorej môže byť podaná námietka.

26.6. Ak dôjde k vylúčeniu uchádzača umiestneného na prvom mieste v poradí alebo jeho ponuky, komisia zostaví nové poradie ponúk na základe kritéria na vyhodnotenie ponúk a komisia bude následne pri vyhodnocovaní postupovať tak ako je uvedené v bode 24. týchto súťažných pokladov.

27. Posúdenie splnenia podmienok účasti uchádzačov

27.1 Posúdenie splnenia podmienok účasti uchádzačov bude založené na posúdení splnenia podmienok týkajúcich sa:

27.1.1 osobného postavenia podľa § 32 ZVO,
271.2 technickej spôsobilosti alebo odbornej spôsobilosti podľa § 34 ZVO

27.2 Verejný obstarávateľ písomne požiada uchádzača alebo záujemcu o vysvetlenie alebo doplnenie predložených dokladov, ak z predložených dokladov nemožno posúdiť ich platnosť alebo splnenie podmienky účasti. Verejný obstarávateľ môže v súvislosti s dôvodom na vylúčenie podľa odseku bodu písomne požiadať uchádzača alebo záujemcu o vysvetlenie. Ak verejný obstarávateľ alebo obstarávateľ neurčí dlhšiu lehotu, uchádzač alebo záujemca doručí vysvetlenie alebo doplnenie predložených dokladov do dvoch pracovných dní odo dňa odoslania žiadosti, ak sa komunikácia uskutočňuje prostredníctvom elektronických prostriedkov.

27.3 Verejný obstarávateľ vylúči kedykoľvek počas verejného obstarávania uchádzača alebo záujemcu z dôvodov podľa § 40 ods. 6 ZVO. Uchádzačovi, ktorý nesplnil podmienky účasti, bude písomne oznámené jeho vylúčenie s uvedením dôvodu a lehoty, v ktorej môže byť podaná námietka podľa ZVO.

Časť VII.
Dôvernosť a etika vo verejnom obstarávaní

28. Dôvernosť procesu verejného obstarávania

28.1. Informácie, týkajúce sa preskúmavania, vysvetľovania, vyhodnocovania ponúk a odporúčaní na prijatie ponuky najúspešnejšieho uchádzača sú dôverné. Členovia komisie na vyhodnocovanie ponúk a zodpovedné osoby obstarávateľa nebudú počas prebiehajúceho procesu verejného obstarávania poskytovať alebo zverejňovať uvedené informácie o obsahu ponúk ani uchádzačom, ani žiadnym tretím osobám.

28.2. Informácie, ktoré uchádzač v ponuke označí za dôverné, nebudú zverejnené alebo inak použité bez predošlého súhlasu uchádzača, pokiaľ uvedené nebude v rozpore so zákonom o verejnom obstarávaní a inými všeobecne záväznými právnymi predpismi/ osobitnými predpismi (zákon č.211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov, zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, atď.).

28.3. Za dôverné informácie je možné označiť výhradne obchodné tajomstvo, technické riešenia a predlohy, návody, výkresy, projektové dokumentácie, modely, spôsob výpočtu jednotkových cien a ak sa neuvádzajú jednotkové ceny ale len cena, tak aj spôsob výpočtu ceny a vzory. Ako obchodné tajomstvo uchádzač nemôže označiť údaje, ktoré sú návrhmi na plnenie kritérií.

29. Revízne postupy

29.1. Uchádzač alebo osoba, ktorej práva alebo právom chránené záujmy boli alebo mohli byť dotknuté postupom verejného obstarávateľa môže podľa § 164 zákona o verejnom obstarávaní podať verejnému obstarávateľovi žiadosť o nápravu.

29.2. Uchádzač alebo osoba, ktorej práva alebo právom chránené záujmy boli alebo mohli byť dotknuté postupom verejného obstarávateľa môže podať podľa § 170 zákona o verejnom obstarávaní námietku proti postupu verejného obstarávateľa. V súlade s § 170 ods. 7 námietky nemožno podať pri:
a) zadávaní zákaziek na uskutočnenie stavebných prác, ak je predpokladaná hodnota zákazky rovná alebo nižšia ako 800 000 eur,
b) zadávaní podlimitných zákaziek verejným obstarávateľom na dodanie tovaru alebo poskytnutie služby,
c) zadávaní zákazky s nízkou hodnotou verejným obstarávateľom,
d) postupe zadávania podlimitnej koncesie,
e) zadávaní zákaziek na dodanie tovaru alebo poskytnutie služby v oblasti obrany a bezpečnosti, ak je predpokladaná hodnota zákazky rovná alebo nižšia ako finančný limit podľa §5 ods. 5 písm. a).

Časť VIII.
Prijatie ponuky

30. Informácia o výsledku vyhodnotenia ponúk

Každému dotknutému uchádzačovi bude zaslaný výsledok vyhodnotenia ponúk vrátane poradia uchádzačov. Dotknutým uchádzačom je uchádzač, ktorého ponuka sa vyhodnocovala, vylúčený uchádzač, ktorému plynie lehota na podanie námietok proti vylúčeniu, a uchádzač, ktorý podal námietky proti vylúčeniu, pričom úrad o námietkach zatiaľ právoplatne nerozhodol. Úspešnému uchádzačovi alebo uchádzačom oznámia, že jeho ponuku alebo ponuky prijímajú. Neúspešnému uchádzačovi oznámia, že neuspel a dôvody neprijatia jeho ponuky. Informácia o výsledku vyhodnotenia ponúk zasielaná dotknutým uchádzačom obsahuje najmä:
a) identifikáciu úspešného uchádzača alebo uchádzačov,
b) informáciu o charakteristikách a výhodách prijatej ponuky alebo ponúk,
c) výsledok vyhodnotenia splnenia podmienok účasti u úspešného uchádzača, ktorý obsahuje informácie preukazujúce splnenie podmienok účasti týkajúcich sa finančného a ekonomického postavenia a technickej spôsobilosti alebo odbornej spôsobilosti vrátane identifikácie osoby poskytujúcej technické a odborné kapacity podľa § 34 ods. 3,
d) lehotu, v ktorej môže byť doručená námietka

31. Uzavretie zmluvy

31.1. Verejný obstarávateľ po uplynutí lehôt stanovených zákonom o verejnom obstarávaní písomne vyzve úspešného uchádzača na uzavretie zmluvy.

31.2 Úspešný uchádzač je povinný poskytnúť riadnu súčinnosť potrebnú na uzavretie zmluvy v súlade s § 56 ods. 8 a podľa § 114 ods. 7 zákona o verejnom obstarávaní.

31.3 Zmluva s úspešným uchádzačom, ktorého ponuka bola prijatá, bude uzavretá v lehote viazanosti ponúk a to **najskôr jedenásty deň odo dňa odoslania informácie o výsledku vyhodnocovania ponúk** podľa § 55 zákona o verejnom obstarávaní, ak nebola podaná žiadosť o nápravu, ak žiadosť o nápravu bola doručená po uplynutí lehoty podľa § 164 ods.5 alebo ods. 6 zákona o verejnom obstarávaní.

31.4 Uzavretá zmluva nesmie byť v rozpore so súťažnými podkladmi a s ponukou predloženou úspešným uchádzačom.

31.5 **Verejný obstarávateľ nesmie uzavrieť zmluvu s uchádzačom, ktorý má povinnosť zapisovať sa do registra partnerov verejného sektora (ďalej len ako "RPVS") a nie je zapísaný v RPVS alebo ktorého subdodávatelia alebo subdodávatelia podľa osobitného predpisu, ktorí majú povinnosť zapisovať sa do RPVS, nie sú zapísaní v RPVS.**

31.6 **Verejný obstarávateľ nesmie uzavrieť zmluvu s uchádzačom, ktorý má povinnosť zapisovať sa do RPVS a ktorého konečným užívateľom výhod zapísaným v RPVS je**

1. prezident Slovenskej republiky,
2. člen vlády Slovenskej republiky (ďalej len „vláda“),
3. vedúci ústredného orgánu štátnej správy, ktorý nie je členom vlády,
4. vedúci orgánu štátnej správy s celoslovenskou pôsobnosťou,
5. sudca Ústavného súdu Slovenskej republiky alebo sudca,
6. generálny prokurátor Slovenskej republiky, špeciálny prokurátor alebo prokurátor,
7. verejný ochranca práv,
8. predseda Najvyššieho kontrolného úradu Slovenskej republiky a podpredseda Najvyššieho kontrolného úradu Slovenskej republiky,
9. štátny tajomník,
10. generálny tajomník služobného úradu,
11. prednosta okresného úradu,
12. primátor hlavného mesta Slovenskej republiky Bratislavy, primátor krajského mesta alebo primátor okresného mesta, alebo
13. predseda vyššieho územného celku.

31.7 Verejný obstarávateľ nesmie uzavrieť zmluvu s uchádzačom, ktorého subdodávateľ a subdodávateľ podľa osobitného predpisu, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora, majú v RPVS zapísaného konečného užívateľa výhod, ktorým je osoba podľa vyššie uvedeného bodu 1-13.

32. Ďalšie informácie

32.1. Verejný obstarávateľ si vyhradzuje právo možnosti zrušiť použitý postup zadávania zákazky podľa § 57 zákona o verejnom obstarávaní.

32.2. Verejný obstarávateľ si vyhradzuje právo primerane predĺžiť lehotu viazanosti ponúk a o tejto skutočnosti informuje všetkých uchádzačov.

32.3. Ponuky musia byť v súlade s platnými právnymi predpismi SR.

32.4. Uchádzači nemajú právo na úhradu nákladov spojených so spracovaním ponúk a s účasťou v tomto verejnom obstarávaní.

32.5. Táto súťaž sa uskutočňuje podľa zákona o verejnom obstarávaní. Ďalšie postupy, vzťahy, termíny, povinnosti a pod. viažuce sa k vyhlásenému postupu verejného obstarávania, ktoré nie sú popísané alebo špecifikované v týchto súťažných podkladoch, sa v tomto verejnom obstarávaní riadia všeobecnými ustanoveniami zákona o verejnom obstarávaní.

32.6 Verejný obstarávateľ v súlade s § 41 zákona o verejnom obstarávaní stanovuje pravidlá pre využívanie subdodávateľov nasledovne:

a) uchádzač v ponuke uvedie podiel zákazky, ktorý má v úmysle zadať subdodávateľom, navrhovaných subdodávateľov a predmety subdodávok ako aj jeho podiel na plnení predmetu zmluvy (% vyjadrenie podielu v EUR bez DPH) a to na formulári, ktorý tvorí Prílohu č. 3 týchto Súťažných podkladov.

b) navrhovaný subdodávateľ spĺňal podmienky účasti týkajúce sa osobného postavenia a neexistovali u neho dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7 a 8; oprávnenie dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu sa preukazuje vo vzťahu k tej časti predmetu zákazky alebo koncesie, ktorý má subdodávateľ plniť.

32.7 V súlade s § 41 ods. 3 zákona o verejnom obstarávaní verejný obstarávateľ vyžaduje, aby úspešný uchádzač v zmluve najneskôr v čase jej uzavretia uviedol údaje o všetkých známych subdodávateľoch, údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia.

.

32.8 Pravidlá pre zmenu subdodávateľov sú uvedené v návrhu zmluvy.

32.9 Verejný obstarávateľ vyhlasuje, že osobné údaje bude spracúvať len za účelom účasti uchádzača v predmetnom verejnom obstarávaní a plnenia si zákonných povinností s tým súvisiacimi a v súlade so zákonom o ochrane osobných údajov a príslušnými právnymi predpismi EÚ, a to za použitia primeraných technických, organizačných a bezpečnostných opatrení. Spracúvanie osobných údajov verejným obstarávateľom sa vykonáva počas trvania vyhlásenej súťaže a na dobu potrebnú k výkonu práv a povinností vyplývajúcich zo všeobecne záväzných právnych predpisov.

A.2 Podmienky účasti

33. Podmienky účasti vo verejnom obstarávaní, týkajúce sa osobného postavenia

33.1 Uchádzač musí spĺňať nasledovné podmienky účasti týkajúce sa osobného postavenia uvedené v § 32 ods. 1 zákona o verejnom obstarávaní:

A) Podmienka účasti podľa § 32 ods. 1 písm. e), že je oprávnený dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu.
Uvedenú podmienku účasti preukáže uchádzač v súlade s § 32 ods. 2 písm. e) doloženým dokladom o oprávnení dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu, ktorý zodpovedá predmetu zákazky.
Verejný obstarávateľ má oprávnenie použiť údaje z informačných systémov verejnej správy podľa zákona č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním IS verejnej správy, preto v súlade s § 32 ods. 3 zákona uchádzač nemusí doklad o oprávnení dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu, ktorý zodpovedá predmetu zákazky podľa § 32 tohto bodu predkladať.

B) Podmienka účasti podľa § 32 ods. 1 písm. f), že nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v Slovenskej republike a v štáte sídla, miesta podnikania alebo obvyklého pobytu.
Uvedenú podmienku účasti preukáže uchádzač v súlade s § 32 ods. 2 písm. f) doloženým čestným vyhlásením.

V prípade, že uchádzač má splnenie tejto podmienky účasti zapísané v Zozname hospodárskych subjektov podľa § 152 a nasl. zákona, vedenom Úradom pre verejné obstarávanie (ďalej len "Zoznam hospodárskych subjektov"), nemusí uvedený doklad podľa § 32 ods. 1 písm. f) zákona predkladať.

Uchádzač zapísaný do Zoznamu hospodárskych subjektov vedeného Úradom pre verejné obstarávanie môže doklady požadované na preukázanie splnenia podmienok účasti podľa § 32 ods. 1 písm. e) až f) zákona o verejnom obstarávaní nahradiť predložením informácie o jeho zapísaní do zoznamu hospodárskych subjektov, prípadne potvrdením o jeho zapísaní do zoznamu hospodárskych subjektov podľa § 152 zákona o verejnom obstarávaní. V súlade s § 152 ods. 3 zákona o verejnom obstarávaní bude uznaný aj rovnocenný zápis alebo potvrdenie o zápise vydané príslušným orgánom iného členského štátu, ktorým záujemca preukazuje splnenie podmienok účasti vo verejnom obstarávaní. Bude prijatý aj iný rovnocenný doklad predložený záujemcom. Obstarávateľ je v súlade s § 152 ods. 5 bez ohľadu na odsek 4 oprávnený od záujemcu dodatočne vyžiadať doklad podľa § 32 ods. 2 písm. b) a c).

V prípade podmienky účasti podľa § 32 ods. 2 písm. e) ZVO vyššie uvedené pravidlo platí pre hospodárske subjekty (záujemcov) taxatívne vymenované v § 2 ods. 2 zákona č. 272/2015 Z. z. o registri právnických osôb, podnikateľov a orgánov verejnej moci a o zmene a doplnení niektorých zákonov. V ostatných prípadoch je uchádzač alebo záujemca naďalej povinný predložiť doklad preukazujúci splnenie predmetnej podmienky účasti týkajúcej sa osobného postavenia (napríklad výpis z obchodného registra alebo živnostenského registra).

33.2 Ak uchádzač má sídlo, miesto podnikania alebo obvyklý pobyt mimo územia Slovenskej republiky a štát jeho sídla, miesta podnikania alebo obvyklého pobytu nevydáva niektoré z dokladov uvedených v bode 34.1 alebo nevydáva ani rovnocenné doklady, možno ich nahradiť čestným vyhlásením podľa predpisov platných v štáte jeho sídla, miesta podnikania alebo obvyklého pobytu. Ak právo štátu uchádzača so sídlom, miestom podnikania alebo obvyklým pobytom mimo územia Slovenskej republiky neupravuje inštitút čestného

vyhlásenia, môže ho nahradiť vyhlásením urobeným pred súdom, správnym orgánom, notárom, inou odbornou inštitúciou alebo obchodnou inštitúciou podľa predpisov platných v štáte sídla, miesta podnikania alebo obvyklého pobytu uchádzača.

34 Podmienky účasti vo verejnom obstarávaní, týkajúce sa finančného alebo ekonomického postavenia

nevyžaduje sa

35. Podmienky účasti vo verejnom obstarávaní, týkajúce sa technickej alebo odbornej spôsobilosti

Podmienky účasti vo verejnom obstarávaní, týkajúce sa technickej alebo odbornej spôsobilosti pre Časť 1 zákazky: Implementácia technických opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

35.1 Uchádzač musí spĺňať nasledovné podmienky účasti týkajúce sa technickej alebo odbornej spôsobilosti:

A) Podmienka účasti podľa § 34 ods. 1 písm. a):
Uchádzač musí predložiť zoznam dodaných tovarov za posledné tri roky odo dňa vyhlásenia súťaže. Zoznam predloží s uvedením cien, odberateľov, termínov poskytovania služieb, kontaktných údajov na overenie plnenia; dokladom je referencia, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ podľa zákona o verejnom obstarávaní.

Minimálna úroveň požadovaná verejným obstarávateľom podľa bodu A):
Uchádzač predloží zoznam poskytnutých služieb rovnakého alebo podobného charakteru ako je predmet zákazky za posledné 3 roky od vyhlásenia verejného obstarávania v min. súhrnnej výške 50 000,00 Eur bez DPH, pričom jedna zákazka musí byť v minimálnej hodnote 10 000 Eur bez DPH . Za poskytnutie služieb rovnakého alebo podobného charakteru ako je predmet zákazky sa považujú napr. Implementácia log manažment a SIEM riešenia ktorého súčasťou bola analýza súladu systémov a sietí s požiadavkami zákona o kybernetickej bezpečnosti, dátová analýza zdrojov dát a spracovania auditných záznamov, návrh architektúry spracovania a zberu logov, nasadenie a prevádzka log manažment a SIEM riešenia. Implementácia riešenia ktorého súčasťou bola správa a riadenie prístupov koncových používateľov alebo privilegovaných prístupov a ktorá zahŕňala analýzu existujúcich procesov a návrh ich optimalizácie, integráciu viacerých cieľových systémov pre správu prístupov a rovnako viacero integrovaných aplikácií pre riadenie prístupov. Implementácia riešenia pre správu a ochranu koncových pracovných staníc a mobilných zariadení. Implementácia nástroja pre detekciu a správu zraniteľností ktorého súčasťou bol návrh procesov a postupov pre zabezpečenie riadenia zraniteľností. Vypracovanie stratégie kontinuity činností a návrhu vzoru plánov kontinuity a obnovy.

Uchádzač môže vyššie uvedené zmluvy/požiadavky preukázať jednou zmluvou alebo kombináciou viacerých zmlúv.

V prípade ak odberateľom nebol verejný obstarávateľ alebo obstarávateľ podľa tohto zákona zoznam poskytnutých služieb bude obsahovať minimálne nasledovné údaje:

a) názov projektu/zákazky
b) stručný popis predmetu projektu/zákazky (popis zrealizovaných alebo realizovaných častí služby tak, aby bolo možné jednoznačne posúdiť splnenie podmienky služby rovnakého alebo podobného charakteru ako je predmet zákazky),
c) čas realizácie/plnenia projektu/zákazky, t.j. od - do (mesiac, rok),
d) názov a sídlo odberateľa/objednávateľa projektu/zákazky,
e) finančný objem projektu/zákazky v eur bez DPH,

f) meno a priezvisko, mailová adresa, telefón kontaktnej osoby pre overenie referencie.

V prípade, ak uchádzač uvádza zmluvu, ktorej realizácia presahuje stanovené obdobie rokov, tzn. poskytnutie služieb (zmluvy) začalo pred 3 rokmi, alebo nebolo skončené do vyhlásenia verejného obstarávania (rozhodné obdobie), uchádzač v zozname uvedie zvlášť rozpočtový náklad iba za tú časť dodávky služieb, ktorá bola realizovaná v rozhodnom období.
V prípade, ak poskytnutie služieb realizoval uchádzač ako člen združenia alebo ako subdodávateľ, vyčísli a započíta iba finančný objem, realizovaný ním samotným.

B) Podmienka účasti podľa § 34 ods. 1 písm. g):
Údaje o vzdelaní a odbornej praxi alebo o odbornej kvalifikácií osôb určených na plnenie zmluvy alebo koncesnej zmluvy alebo riadiacich zamestnancov, ak nie sú kritériom na vyhodnotenie ponúk.

Minimálna požadovaná úroveň:
Verejný obstarávateľ požaduje od uchádzača preukázať údaje o odbornej praxi alebo odbornej kvalifikácii osôb, ktorí budú realizovať poskytnutie služby, predložením profesijných životopisov podpísaných dotknutou osobou a predložením dokladov, ktoré sú uvedené pri jednotlivých členoch tímu.

Každý uchádzačom predložený profesijný životopis alebo ekvivalentný doklad, podpísaný príslušným členom tímu, musí obsahovať minimálne:
a) meno a priezvisko príslušného kľúčového experta,
b) história zamestnania/odbornej praxe príslušného experta vo vzťahu k predmetu zákazky (zamestnávateľ/odberateľ, trvanie pracovného pomeru/trvanie odbornej praxe / rok od – do, pozícia, ktorú príslušný kľúčový expert zastával),
c) praktické skúsenosti príslušného kľúčového experta (názov projektu/predmetu plnenia, odberateľ/zamestnávateľ, popis projektu/predmetu plnenia, pozícia na projekte/predmete plnenia, obdobie rok),
d) podpis príslušného kľúčového experta.

Uchádzač vyššie uvedeným spôsobom preukáže splnenie nasledovných minimálnych požiadaviek týkajúcich sa jednotlivých členov tímu expertov č. 1 - 6:

Kľúčový expert č. 1 Projektový manažér
a) vysokoškolské vzdelanie 2 stupňa;
b) minimálne 3-ročné praktické skúsenosti (odborná prax) v oblasti projektového riadenia IT projektov; túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
c) minimálne 2 (dve) praktické skúsenosti (odborná prax) s realizáciou projektu v pozícii projektového manažéra, s aplikovaním metodiky riadenia IPMA, PRINCE2 alebo ekvivalentnej, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
d) platný certifikát projektového manažmentu IPMA minimálne úrovne „B“ alebo PRINCE 2 úrovne „Practitioner“, alebo ekvivalent daného certifikátu; túto podmienku účasti uchádzač preukáže prostredníctvom kópie platného certifikátu;

Kľúčový expert č. 2 - Špecialista pre bezpečnosť IT
a) vysokoškolské vzdelanie 2 stupňa;
b) minimálne 3-ročné praktické skúsenosti v oblasti bezpečnosti Infraštruktúry, aplikácií a realizácie riešení pre oblasť bezpečnosti (identifikácia bezpečnostných rizík, monitoring, analýza a testovanie bezpečnostných hrozieb), túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom
c) minimálne 2 (dve) profesionálne praktické skúsenosti v projektoch, v pozícii Špecialista pre bezpečnosť v oblasti bezpečnosti infraštruktúry, aplikácií a realizácie riešení pre oblasť bezpečnosti

(identifikácia bezpečnostných rizík, monitoring, analýza a testovanie bezpečnostných hrozieb), túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom
d) platný certifikát CISSP alebo CISA alebo CISM alebo ekvivalent; túto podmienku účasti záujemca preukáže prostredníctvom kópie platného certifikátu;

Kľúčový expert č. 3 – Aplikačný špecialista pre oblasť log manažmentu a SIEM

a) minimálne 3-ročné praktické skúsenosti v oblasti analýzy, návrhu, konfigurácii a parametrizácii riešení log manažment a SIEM riešení, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
b) minimálne 2 (dve) profesionálne praktické skúsenosti v projektoch zo zameraním na log manažment a SIEM ktorých súčasťou bola analýza súladu systémov a sietí s požiadavkami zákona o kybernetickej bezpečnosti, dátová analýza zdrojov dát a spracovania auditných záznamov, návrh architektúry spracovania a zberu logov, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
c) platný produktový certifikát pre riešenie zamerané na log manažment a SIEM riešenie.

Kľúčový expert č. 4 – Kľúčový expert pre sieťovú a serverovú infraštruktúru

a) minimálne 3-ročné praktické skúsenosti v oblasti návrhu, prevádzky a technickej podpory sieťovej a serverovej infraštruktúry
b) minimálne 2 (dve) profesionálne praktické skúsenosti ktorých súčasťou bol návrh, prevádzka, alebo podpora sieťovej a/alebo serverovej infraštruktúry, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
c) platný produktový certifikát pre kľúčové sieťové a serverové technológie prevádzkované obstarávateľom (Cisco, CheckPoint, Microsoft), úroveň certifikácie CCIE pre Cisco, CCSE pre CheckPoint, a MCSE pre Microsoft pre túto podmienku je možné splniť i viacerými osobami na pozícii kľúčového experta

Kľúčový expert č. 5 – Aplikačný špecialista pre oblasť kontroly a riadenia prístupov

a) minimálne 3-ročné praktické skúsenosti v oblasti správy a riadenie prístupov koncových používateľov alebo privilegovaných prístupov, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
b) minimálne 2 (dve) profesionálne praktické skúsenosti v projektoch zo zameraním na správu a riadenie prístupov koncových používateľov alebo privilegovaných prístupov ktorých súčasťou bola analýza existujúcich procesov a návrh ich optimalizácie, integrácia viacerých cieľových systémov pre správu prístupov a rovnako viacero integrovaných aplikácií pre riadenie prístupov, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
c) platný produktový certifikát pre riešenie zamerané na správu a riadenie prístupov.

Kľúčový expert č. 6 – Aplikačný špecialista pre oblasť identifikácie technických zraniteľností

a) minimálne 3-ročné praktické skúsenosti v oblasti testovania a identifikácie technických zraniteľností, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
b) minimálne 2 (dve) profesionálne praktické skúsenosti v projektoch zo zameraním na testovanie a identifikáciu technických zraniteľností, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom.
c) platný certifikát CISSP alebo ekvivalent; túto podmienku účasti záujemca preukáže prostredníctvom kópie platného certifikátu.

Kľúčový expert č. 7 – Expert pre oblasť stratégie kontinuity činností

a) minimálne 3-ročné praktické skúsenosti v oblasti riadenia kontinuity činností, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
b) minimálne 2 (dve) profesionálne praktické skúsenosti v projektoch zo zameraním na vypracovanie stratégie kontinuity činností a návrhu plánov kontinuity a obnovy, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom,
c) platný certifikát alebo osvedčenie preukazujúci znalosti v oblasti plánovania kontinuity činností.

Ako dôkaz odbornej spôsobilosti certifikovaných špecialistov bude za každého certifikovaného špecialistu predložený podpísaný životopis alebo ekvivalentný doklad a príslušný platný certifikát.
Verejný obstarávateľ na vysvetlenie uvádza, že v prípade preukázania splnenia podmienok týkajúcich sa certifikátov pre jednotlivých expertov, verejný obstarávateľ nebude akceptovať účasť na školení a požaduje predloženie riadneho a vydaného certifikátu v zmysle podmienok konkrétnej certifikačnej autority (vo väčšine prípadov úspešne absolvovanými skúškami).

Uchádzač na preukázanie splnenia vyššie uvedených podmienok účasti musí na každú pozíciu definovať jedného kľúčového experta.

Podmienky účasti vo verejnom obstarávaní, týkajúce sa technickej alebo odbornej spôsobilosti pre Časť 2 zákazky: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti:

A) Podmienka účasti podľa § 34 ods. 1 písm. a):
Uchádzač musí predložiť zoznam dodaných tovarov za posledné tri roky odo dňa vyhlásenia súťaže. Zoznam predloží s uvedením cien, odberateľov, termínov poskytovania služieb, kontaktných údajov na overenie plnenia; dokladom je referencia, ak odberateľom bol verejný obstarávateľ alebo obstarávateľ podľa zákona o verejnom obstarávaní.

Minimálna požadovaná úroveň:
Uchádzač predloží zoznam poskytnutých služieb rovnakého alebo podobného charakteru ako je predmet zákazky za posledné 3 roky od vyhlásenia verejného obstarávania v min. súhrnnej výške 50 000,00 Eur bez DPH, pričom jedna zákazka musí byť v minimálnej hodnote 10 000 Eur bez DPH . Za poskytnutie služieb rovnakého alebo podobného charakteru ako je predmet zákazky sa považujú napr. tvorba bezpečnostnej dokumentácie a opatrení potrebných na plnenie požiadaviek legislatívy vyplývajúcej zo zákonov (Zákon o KB, Zákon o ITVS) ako klasifikácia informácií a kategorizácia sietí a informačných systémov, tvorba smerníc na výkon analýzy rizík a analýzy dopadov (AR/BIA), smernica o bezpečnej prevádzke IS a sietí, politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP, smernica pre bezpečný vývoj a údržbu aplikácií a IS (Secure Software Development Life Cycle - SSDLC) a návrh bezpečnostných požiadaviek pre aplikácie podľa klasifikačných stupňov, návrh katalógu rizík a spôsobov ich riadenia, podpora pri definovaní plánu stratégie obnovy pre jednotlivé IS a pri definovaní BCP a DRP.
Uchádzač môže vyššie uvedené zmluvy/požiadavky preukázať jednou zmluvou alebo kombináciou viacerých zmlúv.

Zoznam poskytovaných alebo poskytnutých služieb za predchádzajúce tri roky od vyhlásenia verejného obstarávania s uvedením cien, lehôt dodania a odberateľov, ktorý má obsahovať minimálne nasledujúce údaje:
a) názov projektu/zákazky
b) stručný popis predmetu projektu/zákazky (popis zrealizovaných alebo realizovaných častí služby tak, aby bolo možné jednoznačne posúdiť splnenie podmienky služby rovnakého alebo podobného charakteru ako je predmet zákazky),

c) čas realizácie/plnenia projektu/zákazky, t.j. od - do (mesiac, rok),
d) názov a sídlo odberateľa/objednávateľa projektu/zákazky,
e) finančný objem projektu/zákazky v eur bez DPH,
f) meno a priezvisko, mailová adresa, telefón kontaktnej osoby pre overenie referencie.

Opis opatrení použitých uchádzačom alebo záujemcom na zabezpečenie kvality alebo bezpečnosti.
V prípade, ak uchádzač uvádza zmluvu, ktorej realizácia presahuje stanovené obdobie rokov, tzn. poskytnutie služieb (zmluvy) začalo pred 3 rokmi, alebo nebolo skončené do vyhlásenia verejného obstarávania (rozhodné obdobie), uchádzač v zozname uvedie zvlášť rozpočtový náklad iba za tú časť dodávky služieb, ktorá bola realizovaná v rozhodnom období.
V prípade, ak poskytnutie služieb realizoval uchádzač ako člen združenia alebo ako subdodávateľ, vyčísli a započíta iba finančný objem, realizovaný ním samotným.

B) Podmienka účasti podľa § 34 ods. 1 písm. g):
Údaje o vzdelaní a odbornej praxi alebo o odbornej kvalifikácií osôb určených na plnenie zmluvy alebo koncesnej zmluvy alebo riadiacich zamestnancov, ak nie sú kritériom na vyhodnotenie ponúk.

Minimálna požadovaná úroveň:
Verejný obstarávateľ požaduje od uchádzača preukázať údaje o odbornej praxi alebo odbornej kvalifikácii osôb, ktorí budú realizovať poskytnutie služby, predložením profesijných životopisov podpísaných dotknutou osobou a predložením dokladov, ktoré sú uvedené pri jednotlivých členoch tímu.

Každý uchádzačom predložený profesijný životopis alebo ekvivalentný doklad, podpísaný príslušným členom tímu, musí obsahovať minimálne:
• meno a priezvisko príslušného kľúčového experta,
• história zamestnania/odbornej praxe príslušného experta vo vzťahu k predmetu zákazky (zamestnávateľ/odberateľ, trvanie pracovného pomeru/trvanie odbornej praxe / rok od – do, pozícia, ktorú príslušný kľúčový expert zastával),
• praktické skúsenosti príslušného kľúčového experta (názov projektu/predmetu plnenia, odberateľ/zamestnávateľ, popis projektu/predmetu plnenia, pozícia na projekte/predmete plnenia, obdobie rok),
• podpis príslušného kľúčového experta.

Uchádzač vyššie uvedeným spôsobom preukáže splnenie nasledovných minimálnych požiadaviek týkajúcich sa jednotlivých členov tímu expertov č. 1 - 3:

Kľúčový expert č. 1 Projektový manažér
a) vysokoškolské vzdelanie 2 stupňa;
b) minimálne 3-ročné praktické skúsenosti (odborná prax) v oblasti projektového riadenia IT projektov; túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
c) minimálne 2 (dve) praktické skúsenosti (odborná prax) s realizáciou projektu v pozícii projektového manažéra, s aplikovaním metodiky riadenia IPMA, PRINCE2 alebo ekvivalentnej, pričom obsahom projektu bola implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti, túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
d) platný certifikát projektového manažmentu IPMA minimálne úrovne „B“ alebo PRINCE 2 úrovne „Practitioner“, alebo ekvivalent daného certifikátu; túto podmienku účasti uchádzač preukáže prostredníctvom kópie platného certifikátu;

Kľúčový expert č. 2 - Expert pre riadenie bezpečnosti a riadenie rizík
a) vysokoškolské vzdelanie 2 stupňa;

b) minimálne 3-ročné praktické skúsenosti v oblasti riadenia bezpečnosti spolu s riadením rizík informačných systémov; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom,
c) minimálne 2 (dve) profesionálne praktické skúsenosti v oblasti implementácie organizačných opatrení v súlade zo zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti; túto podmienku účasti uchádzač preukáže životopisom alebo ekvivalentným dokladom;
d) platný certifikát v oblasti riadenia bezpečnosti CISM alebo ekvivalent; túto podmienku účasti záujemca preukáže prostredníctvom kópie platného certifikátu;
e) platný certifikát v oblasti riadenia rizík CRISC alebo ekvivalent; túto podmienku preukáže prostredníctvom kópie platného certifikátu.
f) platný certifikát v oblasti auditu ISO 27001 Lead auditor alebo ekvivalent; túto podmienku preukáže prostredníctvom kópie platného certifikátu.

Kľúčový expert č. 3 – Expert pre riadenie IT služieb
a) vysokoškolské vzdelanie 2 stupňa;
b) minimálne 3-ročné praktické skúsenosti (odborná prax) v oblasti analýzy, správy a prevádzky informačných systémov; túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
c) minimálne 2 (dve) profesionálne praktické skúsenosti s analýzou, správou a prevádzkou IT služieb v oblasti implementácie organizačných opatrení v súlade zo zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti; túto podmienku účasti uchádzač preukáže profesijným životopisom alebo ekvivalentným dokladom;
d) platný certifikát v riadení IT služieb minimálne úrovne ITIL 4 Foundation alebo ekvivalent daného certifikátu; túto podmienku účasti uchádzač preukáže prostredníctvom kópie platného certifikátu.
e) platný certifikát v oblasti riadenia rizík CRISC alebo ekvivalent; túto podmienku preukáže prostredníctvom kópie platného certifikátu

Ako dôkaz odbornej spôsobilosti certifikovaných špecialistov bude za každého certifikovaného špecialistu predložený podpísaný životopis alebo ekvivalentný doklad a príslušný platný certifikát.
Verejný obstarávateľ na vysvetlenie uvádza, že v prípade preukázania splnenia podmienok týkajúcich sa certifikátov pre jednotlivých expertov, verejný obstarávateľ nebude akceptovať účasť na školení a požaduje predloženie riadneho a vydaného certifikátu v zmysle podmienok konkrétnej certifikačnej autority (vo väčšine prípadov úspešne absolvovanými skúškami).

Uchádzač na preukázanie splnenia vyššie uvedených podmienok účasti musí na každú pozíciu definovať jedného kľúčového experta.

36. Doklady preukazujúce splnenie podmienok účasti

36.1 Ak je doklad alebo dokument vyhotovený v cudzom jazyku, predkladá sa spolu s jeho úradným prekladom do štátneho jazyka, to neplatí pre doklady a dokumenty vyhotovené v českom jazyku.

36.2 Doklady vyhotovené uchádzačom, musia byť podpísané uchádzačom alebo osobou oprávnenou konať za uchádzača. Doklady vystavené iným subjektom alebo úradom, uchádzač podpisovať nemusí.

36.3 V prípade, ak uchádzač preukáže splnenie podmienok účasti (ktorých minimálne štandardy sú uvedené vo finančnom vyjadrení) predložením dokladov s finančnými premennými uvedenými v mene inej ako je mena EUR, verejný obstarávateľ použije na prepočet kurz stanovený Európskou centrálnou bankou k poslednému dňu roka, v ktorom bol predmet zmluvy dodaný/ ku ktorému bola účtovná závierka vystavená.

37. SPOLOČNÉ PODMIENKY K PREUKAZOVANIU SPLNENIA PODMIENOK ÚČASTI

37.1 Uchádzač môže doklady na preukázanie splnenia podmienok účasti predbežne nahradiť:

37.1.1 jednotným európskym dokumentom v zmysle § 39 ZVO (podrobnejšie inštrukcie sú v na web stránke Úradu pre verejné obstarávanie: https://www.uvo.gov.sk/jednotny-europsky-dokument-pre-verejne-obstaravanie-602.html), a/alebo

37.1.2 čestným vyhlásením podľa § 114 ZVO, v ktorom vyhlási, že spĺňa všetky podmienky účasti určené verejným obstarávateľom a poskytne verejnému obstarávateľovi na požiadanie doklady, ktoré čestným vyhlásením nahradil. Uchádzač môže v čestnom vyhlásení uviesť aj informácie o dokladoch, ktoré sú priamo a bezodplatne prístupné v elektronických databázach, vrátane informácií potrebných na prístup do týchto databáz a informácie o dokladoch, ktoré verejnému obstarávateľovi predložil v inom verejnom obstarávaní a sú naďalej platné.

37.2 Verejný obstarávateľ v súvislosti Jednotným európskym dokumentom obmedzuje informácie požadované na preukázanie splnenia podmienky účasti (týkajúce sa časti IV: Podmienky účasti oddiel A až D) na jednu otázku, s odpoveďou áno alebo nie (α: Globálny údaj pre všetky podmienky účasti), t. j. či hospodárske subjekty spĺňajú všetky požadované podmienky účasti, týkajúce sa ekonomického a finančného postavenia a technickej alebo odbornej spôsobilosti.

37.3 Ak uchádzač použije JED alebo čestné vyhlásenie, verejný obstarávateľ môže na účely zabezpečenia riadneho priebehu verejného obstarávania postupovať podľa § 39 ods. 6 ZVO.

37.4 Doklady preukazujúce splnenie podmienok účasti predkladá verejnému obstarávateľovi uchádzač podľa § 55 ods. 1 ZVO v čase a spôsobom určeným verejným obstarávateľom.

37.5. Skupina dodávateľov preukazuje splnenie podmienok účasti vo verejnom obstarávaní týkajúcich sa osobného postavenia za každého člena skupiny osobitne a splnenie podmienok účasti vo verejnom obstarávaní týkajúcich sa finančného a ekonomického postavenia a technickej spôsobilosti alebo odbornej spôsobilosti preukazuje spoločne. Oprávnenie dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu preukazuje člen skupiny len vo vzťahu k tej časti predmetu zákazky alebo koncesie, ktorú má zabezpečiť.

37.5 Verejný obstarávateľ nevyžaduje ani predloženie dokladu alebo dokladov, ktoré má k dispozícii z iného verejného obstarávania a ktoré sú aktuálne a platné. Uchádzač na účely identifikácie dokladu podľa prvej vety tohto bodu uvedie v ponuke identifikáciu verejného obstarávania, v ktorom predložil doklad podľa prvej vety tohto bodu s presnou identifikáciou časti ponuky, v ktorej sa tento doklad nachádza.

A.3 Kritériá hodnotenia

37. Všeobecné požiadavky na spôsob určenia ceny

37.1 Pri určovaní cien jednotlivých položiek je potrebné venovať pozornosť všetkým požadovaným údajom, ako aj pokynom na zhotovenie ponuky vyplývajúcich pre uchádzačov z týchto súťažných podkladov, vrátane obchodných podmienok dodania predmetu obstarávania.

37.2 Uchádzač uvedie vo svojej ponuke uvedie pre každú časť predmetu zákazky na ktorú predkladá ponuku navrhovanú maximálnu celkovú cenu vrátane dane z pridanej hodnoty (ďalej len „DPH"), ktoré bude musieť verejný obstarávateľ v zmysle slovenských právnych predpisov, v závislosti od uplatneného daňového režimu buď zaplatiť úspešnému uchádzačovi na základe faktúry, alebo priamo odviesť v zmysle režimu prenesenej daňovej povinnosti, a to vo výške stanovenej slovenskými právnymi predpismi.

37.3 Uchádzač musí v ponuke uviesť celkovú maximálnu predpokladanú cenu predmetu zákazky ako aj cenu každej položky určenej v Prílohe č. 5 Cenový návrh súťažných podkladov samostatne pre každú časť zákazky pre ktorú predkladá ponuku. Cenu ponúkaného predmetu zákazky predloží uchádzač vyplnením xls formulára Cenový návrh, ktorého vzor tvorí obsah Prílohy č. 5 Cenový návrh týchto súťažných podkladov

37.4 Všetky jednotkové ceny zaokrúhli uchádzač na 2 desatinné miesta. Ak uchádzač predloží cenu na viac ako určený počet desatinných miest, bude jeho cena zaokrúhlená v zmysle všeobecných platných pravidiel o zaokrúhľovaní (t. j. od číslice 5 - vrátane sa bude zaokrúhľovať smerom nahor

37.5 **Uchádzač uvedie cenu do formulára, ktorý tvorí Prílohu č. 5: Návrh na plnenie kritérií, týchto Súťažných podkladov, a to samostatne pre každú časť predmetu zákazky.**

38. Kritériá hodnotenia ponúk

38.2 Jediným kritériom hodnotenia ponúk je najnižšia **celková cena za predmet zákazky v euro s DPH** pre každú samostatnú časť zákazky ktorú musí uchádzač stanoviť a predložiť spôsobom uvedeným v tejto časti „ A.3 KRITÉRIÁ HODNOTENIA" týchto súťažných podkladov.

38.3 Úspešným uchádzačom pre každú časť zákazky sa stane uchádzač, ktorého ponuka kumulatívne spĺňa nasledovné:

- jeho **celková cena za predmet zákazky v euro s DPH** určená spôsobom uvedeným v časti „A.3 KRITÉRIÁ HODNOTENIA" týchto súťažných podkladov bude najnižšia, t. j. vo vyhodnotení ponúk sa umiestnil na prvom mieste
- splní požiadavky na ponuku stanovené verejným obstarávateľom
- splní podmienky účasti stanovené obstarávateľom v časti A. 3 týchto Súťažných podkladov.

Takáto ponuka bude identifikovaná ako úspešná. Ostatné ponuky, ktorých **celková cena v euro s DPH** určená spôsobom uvedeným v časti „A.3 KRITÉRIÁ HODNOTENIA" týchto súťažných podkladov bude vyššia ako celková cena úspešného uchádzača, t. j. v automatizovanom vyhodnotení ponúk sa neumiestnili na prvom mieste, budú identifikované ako neúspešné.

B.1 Opis predmetu zákazky

Časť 1 zákazky: Implementácia technických opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

V rámci analýzy technických opatrení v súlade so zákonom č.69/2018 Z. z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia analytických výstupov a súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu v priebehu 6 mesiacov:

Názov aktivity: Analýza stavu a príprava pre log management + mapovanie zdrojov
Zadanie:
Analýza stavu správy logov a auditných záznamov. Príprava pre log management a mapovanie zdrojov.
Popis:
Zaznamenávanie a uchovávanie auditných záznamov vytvára údajovú bázu pre aplikovanie požiadaviek na bezpečnostný monitoring.
Pre naplnenie procesných a technologických požiadaviek definovaných legislatívou je nutné realizovať niekoľko na seba nadväzujúcich krokov. V rámci projektu musia byť realizované nasledujúce aktivity:

- Identifikácie relevantných legislatívnych a normatívnych požiadaviek,
- vypracovanie jednotnej politiky zaznamenávania a uchovávania auditných záznamov (logov) týkajúcich sa:
    - prevádzky IS,
    - prvkov infraštruktúry,
    - aktivít príslušných používateľov týchto systémov,
    - aktivít pracovníkov zabezpečujúcich správu a prevádzky týchto systémov (administrátorov interných aj externých),
    - prevádzky pracovných staníc úradu,
- analýza existujúceho stavu logov, ich väzieb a súlad s navrhovanou politikou,
- vypracovanie návrhu na realizáciu úprav rozsahu a obsahu logov,

V rámci politiky zaznamenávania a uchovávania auditných záznamov predpokladáme definovať najmä nasledovné oblasti:

- rozsah systémov a komponentov z ktorých sa musia vytvárať auditné záznamy,
- typy udalostí a činností, ktoré sa majú zaznamenávať do auditných záznamov z jednotlivých systémov a komponentov,
- informácie zaznamenávane z jednotlivých udalostí,
- spôsob uchovávania auditných záznamov,
- spôsob a periodicita sledovania a vyhodnocovania auditných záznamov,
- spôsob zálohovania, archivovania a vymazávania auditných záznamov.
- Pravidlá logovania pre dodávateľov.
- Správa a konsolidácia logov, mapovanie zdrojov z troch lokalít (úrad, Datacentrum, vládny cloud) a do budúcnosti s možných ďalších.

Výstupy:

1. Politika zaznamenávania a uchovávania auditných záznamov.
2. Pravidlá logovania pre dodávateľov IT systémov na úrad.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

V rámci analýzy musí byť zhodnotený súlad aktuálneho stavu s politikou vytárania auditných záznamov. Výstupom analýzy bude prehľad formátov, obsahu a rozsahu logov pre jednotlivé systémy a prvky infraštruktúry. Pre implementáciu úprav budú navrhnuté priority na základe určenia dôležitosti konkrétneho systému, rozsahu a náročnosti úprav.

Názov aktivity: Príprava zadaní a mapovanie zdrojov pre implementáciu SIEM, kontrola kvality
Zadanie:
Identifikácia parametrov pre implementáciu bezpečnostného monitoringu SIEM (Security Information and Event Management)
Popis:
Údajovú bázu pre identifikáciu a vyhodnocovanie bezpečnostných udalostí tvoria prevádzkové logy a auditné záznamy. V tomto zmysle nadväzuje príprava implementácie SIEM riešenia na aktivitu mapujúcu stav spracovania logov a auditných záznamov v rámci ktorej budú zmapované zdroje a vypracovaná politika uchovávania auditných záznamov.
Implementácia SIEM nástroja zabezpečí naplnenie požiadaviek na bezpečnostný monitoring prevádzky IT

Návrh implementácie musí byť zameraný na definovanie kvantitatívnych a kvalitatívnych parametrov.
Primárnym kvantitatívnym parametrom pre implementáciu SIEM riešenia je :

- počet spracovaných udalostí za sekundu – EPS (events per second),
- distribúcia zberu dát v závislosti na architektúre prevádzkového prostredia.

Z hľadiska získavania logov pre vyhodnocovanie udalostí v SIEM je nutné predovšetkým definovať:

- zdroj logov a auditných záznamov, mapovanie zdrojov
- spôsob zberu – možnosti integrácie do centralizovaného zberu (syslog, log súboru, event logy),
- spôsob zberu – topológia architektúry prevádzkového prostredia,
- početnosť a objem dát pre definovanú časovú periódu.

Z hľadiska kvalitatívnych parametrov je to predovšetkým:

- požadovaná dostupnosť,
- úroveň zabezpečenia riešenia,
- podporované rozhrania a šablóny pre efektívnu integráciu,
- úroveň automatizácie pri vyhodnocovaní udalostí,
- podporné funkcie pre detekciu a analýzu bezpečnostných incidentov.

Výstupy:

1. Politika prevádzky SIEM.
2. Pravidlá logovania - integrácie do SIEM pre dodávateľov IT systémov na úrad.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

V rámci návrhu sa očakáva identifikácia a vyčíslené parametrov pre implementáciu riešenia. Zároveň sa očakáva návrh referenčnej architektúry pre nasadenie do existujúcej prevádzkovej infraštruktúry.

Názov aktivity: Analytická príprava a technické možnosti na dvojfaktorovú autentifikáciu pre vzdialene prístupy
Zadanie:
Analýza a identifikácia technických parametrov pre zabezpečenie kontroly a riadenia prístupov
Popis:
Pre zabezpečenie požadovanej úrovne integrity a bezpečnosti prístupov je nevyhnutné identifikovať kľúčové procesy správy prístupov a definovať politiky – požiadavky na ich zabezpečenie. Analýza a návrh musí zabezpečiť definovanie prístupových politík a zodpovednosti za procesy ktoré zahŕňajú celý životný cyklus jednotlivých typov prístupových účtov. Pre jednotlivé typy prístupových účtov sa predpokladá aplikovanie odlišnej úrovne zabezpečenia z pohľadu komplexnosti a časovej platnosti hesla.
Špecifikované parametre musia vychádzať z minimálnych požiadaviek definovaných vo všeobecných zásadách pre manažment prístupov IKT a pokryť procesy:

- Inicializácia hesla,
- Notifikácie a upozornenia,
- Exspirácia hesla,
- Revalidácia – prehodnotenie prístupov,
- Použitie generických privilegovaných prístupov.

Zároveň musia špecifikovať požiadavky a parametre technických riešení pre nasadenie:

- Dvojfaktorovej autentifikácie pre vzdialené prístupy
- Správy, riadenia a monitorovania privilegovaných prístupov,
- Segregovania privilegovaných prístup (viac-vrstvový model administrácie serverov a pracovných staníc).

Výstupy:

1. Smernica riadenia prístupov a prideľovania prístupových práv.
2. Zakreslenie procesov v Camunde.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Analýza a implementácia procesov riadenia zraniteľností - vulnerability manažment
Zadanie:
Analýza a návrh procesov riadenia zraniteľností
Popis:
Pre zabezpečenie efektívnej a promptnej reakcie na relevantné bezpečnostné hrozby je nutné v prvom rade definovať:

- vstupy na základe ktorých sa vyhodnocuje miera rizika (bezpečnostné varovania, pravidelné skenovanie, penetračné testovanie),
- proces hodnotenia miery rizika v nadväznosti na klasifikáciu aktív,
- zodpovednosti za spôsob schvaľovania eliminácie rizika.

Definované procesy pre riadenie zraniteľnosti sa predovšetkým musia zamerať na :

- pravidlá a procesy pre bezpečný vývoj a aplikovanie bezpečnostných mechanizmov,
- začlenenie testovania zraniteľnosti do procesu riadenia zmien,
- nasadenie nástroja pre pravidelné skenovanie, hodnotenie a manažment známych zraniteľností.

V rámci návrhu sa očakáva identifikácia a vyčíslené parametrov pre implementáciu riešenia nástroja pre pravidelné skenovanie, hodnotenie a manažment známych zraniteľností.
Výstupy:

1. Smernica hodnotenie zraniteľností a prevencia ich odhaľovania.
2. Zakreslenie procesov v Camunde.
3. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Analytická príprava a možnosti pre mobile device management
Zadanie:
Analýza a identifikácia technických parametrov pre zabezpečenie a správu mobilných zariadení.
Popis:
Efektívna ochrana mobilných zariadení (notebook, smartphone) je kľúčová pri eliminácií hrozieb a bezpečnostných rizík. Súčasťou zabezpečenia mobilných zariadení musí byť správa a ochrana zariadení:

- Správa zariadení musí zabezpečiť zvýšenie efektivity prevádzky a technickej podpory koncových používateľov.
- Ochrana mobilných zariadení pôsobí ako funkčný prvok a prevencia úniku dát a proti prípadným útokom uskutočneným prostredníctvom mobilného zariadenia.

Analýza využitia mobile device managementu musí byť zameraná na spôsob implementácie, využiteľnosť a identifikáciu technických parametrov pre oblasti :

- centralizovaná bezpečná správa, evidencia a konfigurácia mobilných zariadení,

- oddelenie pracovných a súkromných dát, aplikácií (prostredí - kontajnerizácia),
- zabezpečenie vzdialených prístupov z mobilných zariadení k IKT zdrojom,
- zabezpečenie ochrany dát nachádzajúcich sa na mobilných zariadeniach,
- zabezpečenie prípadného bezpečného zmazania mobilného zariadenia na diaľku,
- spracovanie auditných záznamov o činnosti administrátora aj používateľov.

Výstupy:

1. Politika zabezpečenia mobilných zariadení.
2. Analýza existujúceho stavu a návrh implementácie, predpokladaný rozpočet.

Názov aktivity: Plánovanie kontinuity činností, vypracovanie návrhu Stratégie kontinuity a vytvorenie plánov kontinuity, Havarijné plánovanie, DRP – disaster recovery plány

Zadanie:

Zabezpečenie vypracovania stratégie kontinuity činností a návrhu vzoru plánov kontinuity a obnovy.

Popis:

Cieľom stratégie kontinuity činností je definovať a dokumentovať základný rámec na zaistenie kontinuity činností metódou „Worst Case Scenario“. V rámci stratégie kontinuity činností musia byť navrhnuté možné stratégie obnovy jednotlivých kritických procesov pre zvolené krízové udalosti a vybraná najoptimálnejšia stratégia.

Stratégia kontinuity činností musí vychádzať zo záverov už vypracovanej analýzy dopadov a analýzy rizík.

Stratégia kontinuity činností sa musí sústreďovať najmä na:

- výber alternatívnych metód, ktoré budú použité v prípade narušenia alebo neočakávanej udalosti na zabezpečenie kontinuity kritických procesov v súlade so stanovenou prioritou počas analýzy dopadov,
- zraniteľnosti a kritické prvky zlyhania (single points of failure) v kritických procesoch, ktoré boli identifikované počas analýzy rizík.

Stratégia kontinuity činností musí obsahovať:

- sumarizáciu výstupov z analýzy dopadov a analýzy rizík, vrátane požiadaviek na obnovu,
- definíciu havárie, predpoklady vymedzujúce haváriu,
- definíciu princípov, podľa ktorých budú realizované činnosti v havarijnom stave,
- identifikáciu zdrojov, ktoré budú použité v havarijnom stave,
- popis riadenia aktivít v havarijnom stave.

Stratégia kontinuity činností môže pozostávať z viacerých dokumentov vo viacúrovňovej architektúre (organizačná, procesná, technologická).

Súčasne je potrebné vypracovať vzorové dokumenty pre plánovanie prvotnej reakcie na neočakávanú udalosť, ktorá nastala, ako aj na určenie náhradných postupov pri vzniku neočakávanej udalosti (plánov kontinuity činností), resp. určenie postupov oživenia pri výpadku IKT komponentov (DRP). Tieto dokumenty poskytnú organizácii jednotný rámec pre vypracovávanie plánov.

Výstupy:

1. Návrh procesov a postupov pre Riadenie kontinuity prevádzky – vypracovanie smernice Riadenie kontinuity prevádzky. Zakreslenie procesov v Camunde.
2. Dokument: Analýza funkčných dopadov (BIA), určenie cieľovej doby obnovy a cieľového bodu obnovy
3. Dokument: Stratégia kontinuity činností.
4. Dokument: Vzorové dokumenty pre plánovanie prvotnej reakcie a plánov kontinuity činností
5. Dokumenty DRP pre:
    a. Systém registratúry
    b. Systémy LS Telcom, CRC Data Radiolab
    c. Dochádzkový systém
    d. Účtovníctvo a pohľadávky, softvérové riešenia Štátnej pokladnice

Názov aktivity: Integrácia na VISKB

Zadanie:
Integrácia na Vládny informačný systém kybernetickej bezpečnosti (VISKB).

Časť 2 zákazky: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

V rámci implementácie organizačných opatrení v súlade so zákonom č.69/2018 Z.z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia interných smerníc ako i súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu v priebehu 6 mesiacov:

1. **Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov**

Bezpečnostná dokumentácia upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.

a) Bezpečnostná dokumentácia:
   a. Bezpečnostná stratégia kybernetickej bezpečnosti,
   b. Riadenie bezpečnostných rizík,
   c. Riadenie informačných aktív,
   d. Pravidlá správania a dobrej praxe,
   e. Riadenie dodávateľských vzťahov,
   f. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
   g. Riadenie a prevádzka informačno-komunikačných technológií,
   h. Riadenie súladu,
   i. Riadenie kontinuity procesov a činností,
   j. Organizácia bezpečnosti,
   k. Bezpečnostná politika.

b) Bezpečnosť prevádzky IS a sietí:

Cieľom smernice je procesne zabezpečiť riadenie bezpečnosti sietí a informačných systémov a naplnenie požiadaviek na základe §11 Vyhlášky č. 362/2018 Z.z. o bezpečnosti prevádzky IT a §10 Vyhlášky č. 362/2018 Z.z. o bezpečnosti komunikačných sietí, zálohe dát, posudzovaní zraniteľností a ďalších ako aj zákona o KB:

- riadením prevádzky - riadením prístupov používateľov k sieťam a informačným systémom podľa § 12 zákona o KB,
- prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
- tým, že prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
- prostredníctvom bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
- tým, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,

- tým, že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
- prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,
- udržiavaním zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
- použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
- prostredníctvom blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
- neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty,
- prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
- implementovaním systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
- prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

c) Návrh procesov a postupov pre riadenie prevádzky:

Riadenie bezpečnosti prevádzky siete a informačného systému musí byť zaistené prostredníctvom určených pravidiel a postupov na:

- riadenie zmien,
- riadenie záplat a aktualizácií,
- riadenie kapacít,
- pravidelné zálohovanie a testovanie obnovy informácií zo záloh,
- ochranu pred škodlivým kódom,
- inštaláciu softvéru v sieťach a informačných systémoch,
- inštaláciu zariadení v sieťach a informačných systémoch a
- zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov

d) Kryptografické opatrenia - Návrh procesov a postupov pre kryptografickú ochranu informácií.

e) Riešenie kybernetických incidentov - Návrh procesov a postupov pre riešenie kybernetických incidentov.

Očakávané výstupy časti 1. Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov:

- Politika - Bezpečnostná stratégia kybernetickej bezpečnosti,
- Politika - Riadenie bezpečnostných rizík,
- Politika - Riadenie informačných aktív,
- Politika - Pravidlá správania a dobrej praxe,
- Politika - Riadenie dodávateľských vzťahov,
- Politika - Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
- Politika - Riadenie a prevádzka informačno-komunikačných technológií,
- Politika - Riadenie súladu,
- Politika - Riadenie kontinuity procesov a činností,
- Politika - Organizácia bezpečnosti,
- Bezpečnostná politika,

- Smernica - Bezpečnosť prevádzky IS a sietí,
- Smernica - Riadenie prevádzky (change management, zálohovanie, testovanie obnovy, inštalácia zariadení...),
- Smernica/Štandard - Kryptografická ochrana informácií,
- Smernica/Štandard - Riešenie kybernetických incidentov.

2. Inventarizácia, klasifikácia a kategorizácia informačných aktív

Smernica pre klasifikáciu informácií a kategorizácia sietí a informačných systémov podľa § 20 ods. 2 zákona č. 69/2018 Z.z. sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „príloha č.2“) . Ak prevádzkovateľ základnej služby disponuje vlastnou klasifikáciou informácií a kategorizáciou sietí a informačných systémov, vykoná sa mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2.

Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému. Predpokladom na úspešnú klasifikáciu informácií a kategorizáciu sietí a informačných systémov je pozostáva najmä z nižšie uvedených aktivít:

- špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií,
- návrhu procesu, systému alebo dátovej štruktúry,
- vývoja systému alebo spôsobu spracúvania informácií,
- implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií,
- prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií,
- zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb prevádzkovateľa základnej služby,
- nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom,
- vyradenia ako ukončenia procesu spracúvania informácií alebo vyňatia systému z prevádzky.

Informácia sa klasifikuje bez ohľadu na jej formát, spôsob uloženia, systémy, aplikácie alebo nástroje, v ktorých sa nachádza alebo prostredníctvom ktorých sa informácia spracúva alebo prostredníctvom ktorých je prenášaná.
Pri klasifikácii informácií sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informácie, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality služby. Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.
Kategorizácia sietí a informačných systémov je založená na klasifikácii informácií.
Kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.
Zoznam komponentov sietí a informačných systémov identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej alebo grafickej časti tak, že sú jednoznačne definované hranice vybranej siete a informačného systému, rozhrania medzi definovanými hranicami, bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti a požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich projektovanie, vytváranie, implementáciu a kontrolu.
Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaradia do vyššej bezpečnostnej kategórie.
Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej

úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.
Minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie sietí a informačných systémov sú uvedené v *prílohe č. 3*. k vyhláške č. 362/2018 Z. z.
Táto kapitola by mala pokryť vypracovanie dokumentov, ktoré budú pokrývať vypracovanie dokumentácie, ktorá bude pokrývať nižšie uvedenú problematiku:

a. Spracovanie metodiky pre klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
b. Vypracovanie klasifikačnej schémy,
c. Spracovanie klasifikácie informácií a kategorizácie sietí.

3. Vzdelávanie a príprava vzdelávacích materiálov pre IT aj nelT zamestnancov

Táto aktivita pozostáva z dvoch častí.
Prvá časť sa týka prípravy smernice, ktorá bude obsahovať informácie pre zodpovedných zamestnancov odboru informačných a komunikačných technológií, ktorá bude slúžiť ako nástroj na minimalizáciu, prevenciu a riešenie vzniknutých hrozieb a následných postupov spojených s neoprávneným prístupom do informačných systémov organizácie, siete organizácie a údajov, ktorými organizácia disponuje. Predmetná dokumentácia bude obsahovať postupy spojené s minimalizáciou rizík spojených s neoprávneným prístupom do informačných systémov, nástrojmi, ktoré by riešili prevenciu voči takémuto konaniu a spôsobmi riešenia už vzniknutých incidentov. Smernica bude slúžiť ako nástroj IT zamestnancov, podľa ktorého budú zodpovední IT zamestnanci riešiť vzniknuté incidenty a usmerňovať ostatných zamestnancov v predchádzaní takýmto incidentom.
Druhá časť bude pozostávať zo spracovania plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti. Plán rozvoja bezpečnostného povedomia bude obsahovať školiace materiály pre zamestnancov z pohľadu zvýšenia povedomia o kybernetickej bezpečnosti a hrozieb, ktoré zamestnancom hrozia, vzdelávanie zamestnancov o súčasných hrozbách a spôsoboch ako majú tieto hrozby reportovať zodpovedným IT zamestnancom.
Organizačná a personálna bezpečnosť bude pozostávať z nasledujúcich dokumentov:

a. Návrh procesov a postupov v oblasti personálnej bezpečnosti,
b. Spracovanie plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti

4. Vykonanie analýzy rizík kybernetickej bezpečnosti a návrh na riadenie rizík

Smernica upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.
Smernica výkonu analýzy rizík a analýzy dopadov musí definovať proces riadenia rizika pozostávajúci z cyklických a na seba nadväzujúcich procesov:

1. stanovenie kontextu rizík
2. posúdenie rizík
3. ošetrovanie rizík
4. komunikácia o rizikách
5. monitorovanie a preskúmanie rizika

Postup posudzovania rizík ako musí byť popísaný ako komplexný proces, ktorý pozostáva z:

1. identifikácie rizík,
2. analýzy rizík a
3. ohodnotenia rizík.

V rámci predmetnej smernice musí byť zabezpečené procesné nastavenie výkonu analýzy rizík a analýzy dopadov (AR/BIA) organizáciou vrátane:

- identifikácie aktív a ohodnotenia ich kritickosti,
- klasifikácie aktív a kategorizácie IS a sietí,
- identifikácie hrozieb a vektorov útokov,
- analýzy potenciálnych dopadov,
- identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
- identifikácie existujúcich opatrení a reziduálnych rizík,
- návrhu opatrení.

Návrh katalógu rizík a spôsobov ich riadenia:

Katalóg rizík definuje všetky možné ohrozenia, ktoré môžu pôsobiť na aktíva alebo chránené osobné údaje. Cieľom popisu rizika je zachytiť identifikované riziko do štruktúrovaného prehľadného formátu. V zozname rizík je potrebné uviesť najmä základné informácie o riziku, informácie pre analýzu rizík, informácie o odozve na vyhodnotenie rizika.
Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), bude obsahovať identifikované riziká z AR/BIA a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík a ich schválenia Bezpečnostným výborom Úradu pre reguláciu elektronických komunikácií a poštových služieb.

Predmetná kapitola bude popisovať nasledovné oblasti problematiky:

a. Návrh procesov a postupov spojených s riadením rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
b. Spracovanie inventarizácie aktív spolu s určením vlastníkov aktív kybernetickej bezpečnosti a informačnej bezpečnosti,
c. Spracovanie analýzy rizík kybernetickej bezpečnosti.

5. Analýza zmluvných vzťahov s tretími stranami z pohľadu KB, adaptácia odporúčaní do zmlúv

Riadenie dodávateľov - Návrh procesov a postupov pre riadenie kybernetickej bezpečnosti a informačnej bezpečnosti dodávateľských služieb, akvizícií a údržby IS. Smernica upravuje koncept životného cyklu vývoja systémov, ktorý sa vzťahuje na celý rad hardverových a softvérových konfigurácií, pretože systém sa môže skladať iba z hardvérových, iba zo softvérových alebo kombinácie oboch.

Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek: - od fázy zámeru projektu a návrhu požiadaviek (okrem funkčných požiadaviek je potrebné zadefinovať aj bezp. požiadavky) - cez fázy samotného vývoja (zabezpečenie vývojového prostredia a pod.) - testovania (otestovania nie len funkčných ale aj bezp. požiadaviek, vrátane zabezpečenia anonymizácie testovacích dát a pod.) - implementácie, nasadenia a riadenia zmien - až po bezpečné vyradenie IS z prevádzky - checklist bezpečného/kontrol vývoja webových aplikácií Návrh bezpečnostných požiadaviek pre aplikácie bude obsahovať základnú množinu (base line) týchto požiadaviek rozdelenú podľa klasifikačných stupňov.

6. Plán kontrol, interných auditov, compliance management

Návrh procesov a postupov pre riešenie kybernetických incidentov:

a) Zaznamenávanie udalostí a monitorovanie - Návrh procesov a postupov pre zaznamenávanie udalostí a monitorovanie,
b) Riadenie súladu a kontrolné činnosti - Návrh procesov a postupov overovania účinnosti bezpečnostných opatrení, vyhodnocovania aktuálnosti bezpečnostnej dokumentácie