



ÚRAD GEODÉZIE, KARTOGRAFIE A KATASTRA SLOVENSKEJ REPUBLIKY

Chlumeckého 2, P. O. Box 57, 820 12 Bratislava 212

Výzva na predkladanie ponúk

„NÁVRH ORGANIZAČNÝCH A TECHNICKÝCH OPATRENÍ RIADENIA INFORMAČNEJ BEZPEČNOSTI V SÚLADE S POŽIADAVKAMI ZAISTENIA KYBERNETICKEJ BEZPEČNOSTI A OCHRANY OSOBNÝCH ÚDAJOV V ZMYSLE EURÓPSKEJ A NÁRODNEJ LEGISLATÍVY“

(zadávanie zákazky s nízkou hodnotou podľa § 117 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o VO“))

1. Identifikácia verejného obstarávateľa:

Názov: Úrad geodézie, kartografie a katastra Slovenskej republiky
IČO: 00166260
Sídlo: Chlumeckého 2, P. O. Box 57, 820 12 Bratislava 212
Štatutárny orgán: Ing. Ján Mrva - predseda
Internetová adresa organizácie (URL): <http://www.skgeodesy.sk/sk/ugkk/>
Profil VO: <http://www.uvo.gov.sk/vyhľadavanie-profilov/zakazky/676>
Profil zákazky: <https://eo.eks.sk/ElektronickaTabula/Detail/1791>

2. Názov zákazky:

„Návrh organizačných a technických opatrení riadenia informačnej bezpečnosti v súlade s požiadavkami zaistenia kybernetickej bezpečnosti a ochrany osobných údajov v zmysle európskej a národnej legislatívy“

3. Opis predmetu zákazky:

Kód CPV :

- 79417000-0 Bezpečnostné poradenstvo
- 72310000-1 Spracovanie údajov
- 71241000-9 Štúdia realizovateľnosti, poradenská služba, analýza
- 72316000-3 Analýza údajov
- 72223000-0 Služby informačných technológií
- 72330000-2 Služby na štandardizáciu a klasifikáciu obsahu a dát

Predmetom zákazky je vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizáciu opatrení pre potreby ÚGKK podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

- Požiadavky kladené na informačné technológie verejnej správy v zmysle Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“)
- Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).

Detailná špecifikácia predmetu obstarávania je uvedená v prílohe č. 1 tejto výzvy.

Opis súčasného stavu – dokument s označením „*Štúdie zabezpečenia súladu a identifikácie povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020*“ tvorí neverejnú časť opisu predmetu zákazky a bude poskytnutý na základe podpísanej zmluvy o výmene dôverných informácií (NDA).

4. Možnosť predloženia ponuky na celý predmet zákazky, resp. jeho časť

Uchádzač musí predložiť ponuku na celý predmet obstarávania, zákazka nie je rozdelená na časti

5. Miesto dodania predmetu zákazky:

Úrad geodézie, kartografie a katastra Slovenskej republiky, Chlumeckého 2, 812 20 Bratislava, Slovenská republika.

6. Predpokladaná hodnota zákazky:

60.000,00 EUR bez DPH

Predpokladanú hodnotu zákazky (PHZ) uvedenú vyššie považuje verejný obstarávateľ za finančný limit a okolnosť dôležitú pre plnenie zmluvy.

7. Spôsob tvorby ceny.

- 7.1 Všetky uchádzačom navrhované ceny uvedené v ponuke budú vyjadrené v EUR v štruktúre podľa prílohy č. 2 tejto výzvy.
- 7.2 Navrhovaná cena musí byť stanovená podľa 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 a vyjadrená v eurách v súlade so zákonom č. 659/2007 Z. z. o zavedení meny euro v Slovenskej republike a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Vyhlášok č. 97/ 2008 Z . z. a 75/2008 Z. z.
- 7.3 Navrhovaná cena musí byť v súlade s § 2 citovaného zákona o cenách založená na cene obchodného alebo sprostredkovateľského výkonu, ekonomicky oprávnených nákladoch a primeranom zisku. Návrh ceny musí obsahovať všetky náklady spojené s plnením predmetu zákazky. V prípade, že bude hospodársky subjekt úspešný, nebude akceptovaný žiadny nárok na zmenu navrhovanej ceny z dôvodu chýb a opomenutí jeho povinností.
- 7.4 Uchádzač stanoví cenu za predmet zákazky na základe vlastných výpočtov, činností, výdavkov a príjmov podľa platných právnych predpisov. Uchádzač je pred predložením svojej ponuky povinný vziať do úvahy všetko, čo je nevyhnutné na úplné a riadne plnenie zmluvy, pričom do svojich zmluvných cien zahrnie všetky náklady spojené s plnením predmetu zákazky, ktoré môžu akýmkoľvek spôsobom ovplyvniť cenu a charakter ponuky alebo poskytnutia služby. V prípade, že uchádzač bude úspešný, nebude akceptovaný žiadny nárok uchádzača na zmenu navrhovanej ceny z dôvodu chýb a opomenutí jeho povinností. Návrh ceny musí obsahovať všetky náklady spojené s plnením predmetu zákazky.
- 7.5 Verejný obstarávateľ požaduje, aby uchádzači stanovili celkovú cenu za predmet zákazky tak, aby v nej boli zahrnuté všetky náklady. V cene musia byť započítané všetky náklady, ktoré s ňou bezprostredne súvisia, pričom tieto nesmú byť vyjadrené číslom „0“, ani záporným číslom.
- 7.6 Ak uchádzač nie je platcom DPH, na skutočnosť, že nie je platcom DPH, upozorní označením „Nie som platcom DPH“.

8. Lehota na dodanie alebo dokončenie predmetu zákazky:

Verejný obstarávateľ uzavrie s úspešným uchádzačom zmluvu o dielo podľa § 536 až 565 a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a príslušných ustanovení zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Lehota dodania predmetu zákazky: podľa zmluvy (viď príloha č. 4 tejto Výzvy)

9. Podmienky účasti

§ 32 ods. 1 písm. e) zákona o VO	Doklad preukazujúci oprávnenie poskytovať službu, ktorá je predmetom zákazky	Výpis zo živnostenského, resp. obchodného registra
§ 32 ods. 1 písm. f) zákona o VO	nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v SR alebo v štáte sídla, miesta podnikania alebo obvyklého pobytu,	Čestné vyhlásenie, že dodávateľ nemá uložený zákaz účasti vo verejnom obstarávaní
§ 34 ods. 1 písm. a) zákona o VO	Zoznam poskytnutých služieb za predchádzajúce tri roky od vyhlásenia tohto zadávania zákazky s uvedením cien, lehôt dodania a odberateľov, z ktorého musí vyplývať, že uchádzač poskytol minimálne 3 služby rovnakého alebo obdobného charakteru ako je predmet zákazky (t. j. vypracovanie bezpečnostnej dokumentácie a/alebo poskytnutie služieb súvisiacich s realizáciou opatrení vyplývajúcich zo zákona č. 69/2018 Z. z.)	Zoznam poskytnutých služieb / Referencia
§ 34 ods. 1 písm. d) zákona o VO	opis technického vybavenia, študijných a výskumných zariadení a opatrení použitých uchádzačom alebo záujemcom na zabezpečenie kvality	Certifikát
§ 34 ods. 1 písm. g) zákona o VO	údaje o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy	Doklady, dokumenty alebo údaje
§ 40 ods. 6 písm. f) zákona o VO	konflikt záujmov podľa § 23 nemožno odstrániť inými účinnými opatreniami	Čestné vyhlásenie dodávateľa, že nie je v konflikte záujmov v predmetnom verejnom

		obstarávaní napr. podľa vzoru v prílohe č. 3
--	--	-----------------------------------------------------

Vo vzťahu k podmienkam účasti podľa § 32 zákona o VO:

- Uchádzač nepredkladá doklady podľa § 32 ods. 1 písm. e) a f) zákona o VO; verejný obstarávateľ za účelom overenia splnenia uvedených podmienok účasti použije údaje z informačných systémov verejnej správy;
- Ak je uchádzač zapísaný v zozname hospodárskych subjektov – uvedie uchádzač odkaz na stránku záznamu v zozname hospodárskych subjektov alebo reg. číslo hospodárskeho subjektu.

Vo vzťahu k podmienkam účasti podľa § 34 ods. 1 písm. a) zákona o VO:

- Uchádzač predloží zoznam poskytnutých služieb s uvedením cien, lehôt dodania a odberateľov; pričom z poskytnutého zoznamu musí vyplývať, že predmetom plnenia bolo poskytnutie služieb rovnakého alebo obdobného charakteru ako je predmet zákazky (vyžaduje sa uvedenie popisu poskytnutých služieb);
- Ak má uchádzač evidovanú referenciu zahrňujúcu poskytnutie služieb v rozsahu stanovenom verejným obstarávateľom v evidencii referencií – uchádzač uvedie odkaz na zverejnenú referenciu v evidencii referencií vedenej Úradom pre verejné obstarávanie.
- Pre posúdenie minimálnej požadovanej úrovne, musí byť z ceny resp. rozsahu každej kvalifikovanej referencie vyčíslená hodnota resp. rozsah, ktorá zohľadňuje
 - o alikvotný rozsah len pre požadované posudzované obdobie,
 - o len poskytnutie služieb rovnakého alebo podobného charakteru ako je predmet zákazky,
 - o alikvotný podiel uchádzača (alebo tretej osoby, prostredníctvom ktorej preukazuje splnenie podmienky účasti) v skupine dodávateľov.

Vo vzťahu k podmienkam účasti podľa § 34 ods. 1 písm. d) zákona o VO:

- Uchádzač predloží sken originálu alebo úradne overenej kópie platného certifikátu:
 - o originál resp. úradne overenú kópiu platného certifikátu systému manažérstva bezpečnosti informácií podľa EN ISO 27001 v oblasti bezpečnosti aktív informačných systémov, infraštruktúry informačných technológií a komunikácií, resp. iný certifikát (doklad) prezentujúci zavedený systém manažérstva bezpečnosti informácií dodávateľa.

Verejný obstarávateľ uzná ako rovnocenné osvedčenia vydané príslušnými orgánmi členských štátov a prijme aj iné dôkazy predložené uchádzačom, ktoré sú rovnocenné opatreniam na zabezpečenie kvality podľa požiadaviek na vystavenie príslušného certifikátu podľa tohto bodu.

Vo vzťahu k podmienkam účasti podľa § 34 ods. 1 písm. g) zákona o VO:

- Uchádzač predloží doklady, dokumenty alebo údaje (napr. vlastnoručne podpísaný profesijný životopis, certifikát alebo osvedčenie) a zoznam praktických skúseností osôb, ktoré budú zodpovedné za plnenie zmluvy na poskytnutie služieb (experti č. 1 až 2).
- Uchádzač musí preukázať splnenie minimálnych úrovní expertov nasledovne:
 - o kľúčový expert č. 1: expert pre architektúru bezpečnosti:
 - a. minimálne 3-ročná preukázateľná odborná prax v oblasti návrhu bezpečnostnej architektúry informačných systémov,

- b. minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v návrhu bezpečnostnej architektúry informačných systémov
- c. platný certifikát CISSP (Certified Information Systems Security Professional) alebo CISM (Certified Information Security Manager) alebo iný ekvivalentný, vydaný vedúcou akreditačnou a certifikačnou autoritou uznávanou medzinárodne v oblasti IT bezpečnosti a,
 - o kľúčový expert č. 2: expert pre systémy monitorovania bezpečnosti
 - a. minimálne 3-ročná preukázateľná odborná prax na projektoch v oblasti správy a prevádzky bezpečnostných riešení na centralizované monitorovanie bezpečnosti informačných systémov;
 - b. minimálne dve (2) preukázateľné profesionálne praktické skúsenosti v oblasti správy a prevádzky bezpečnostných riešení centralizovaného monitorovania bezpečnosti siete a/alebo informačných systémov, súčasťou ktorých bolo poskytovanie služieb monitorovania bezpečnosti v reálnom čase s požadovanou funkcionalitou na automatické vyhodnocovanie súladu s definovanými kritériami a na automatizovanú notifikáciu o podozrivých udalostiach.
- Z predložených dokladov musia byť zrejme minimálne údaje o vzdelaní, odbornej kvalifikácii a odbornej praxi osôb zodpovedných za poskytnutie služby, čo uchádzač preukáže predložením životopisov. Verejný obstarávateľ uzná aj iné doklady, ktorými sa preukazuje odborná spôsobilosť expertov, pokiaľ budú obsahovať požiadavky určené verejným obstarávateľom.
- Z každého predloženého životopisu alebo ekvivalentného dokladu musia vyplývať nasledovné údaje/skutočnosti:
 - o meno a priezvisko,
 - o najvyššie dosiahnuté vzdelanie (inštitúcia, od-do, získaný titul/certifikát),
 - o história zamestnania/odbornej praxe (zamestnávateľ/odberateľ, trvanie pracovného pomeru/trvanie poskytovaných služieb, pozícia),
 - o praktické skúsenosti (názov referencie/projektu, odberateľ/zamestnávateľ, predmet - popis referencie/projektu, pozícia na projekte (stručný opis činností, ktoré expert vykonával), obdobie rok od - do, meno a priezvisko aspoň jednej kontaktnej osoby a číslo telefónu odberateľa, kde si bude môcť verejný obstarávateľ overiť informácie),
 - o dátum a podpis.
- V prípade certifikátov verejný obstarávateľ prijme aj iný obsahom a rozsahom rovnocenný doklad vydaný príslušnou inštitúciou v inom členskom štáte Európskej únie, predložený uchádzačom preukazujúci požadovanú skutočnosť.

10. Obsah ponuky

Ponuka na každú časť zákazky musí obsahovať minimálne nasledovné doklady a dokumenty:

- doklady a dokumenty preukazujúce splnenie podmienok účasti podľa bodu 9. tejto výzvy,
- naskenovaný ocenený cenový formulár/cenník uvedený v prílohe č. 2 tejto výzvy podpísaný štatutárnym zástupcom uchádzača,
- „Časový harmonogram zhotovenia Diela“ spracovaný podľa požiadaviek uvedených v Zmluve o dielo vo forme podrobného grafického a vecného znázornenia po jednotlivých pracovných položkách/aktivitách s množstvom pracovníkov na nich nasadených, rozpracovanom na jednotlivé týždne. Uchádzač je viazaný maximálnou dĺžkou lehoty trvania poskytovania služieb uvedenou v Zmluve o dielo a nemôže v Časovom harmonograme uviesť dlhšiu lehotu realizácie predmetu zmluvy.

- Ak uchádzač nevypracoval ponuku sám, uvedie v ponuke osobu, ktorej služby alebo podklady pri jej vypracovaní využil. Údaje podľa prvej vety uchádzač uvedie v rozsahu meno a priezvisko, obchodné meno alebo názov, adresa pobytu, sídlo alebo miesto podnikania a identifikačné číslo, ak bolo pridelené.

Uchádzač môže predložiť iba jednu ponuku. Uchádzač nemôže byť v tej istej časti v tom istom postupe zadávania zákazky členom skupiny dodávateľov, ktorá predkladá ponuku. Verejný obstarávateľ vylúči ponuku predloženú uchádzačom, ktorý je súčasne členom skupiny dodávateľov.

11. Kritériá na vyhodnotenie cenových ponúk:

a) Kritérium

- Najnižšia cena celkom za predmet zákazky*

**Pozn.: v prípade platiteľov DPH cena s DPH, v prípade neplatiteľov DPH celková cena*

b) Spôsob vyhodnotenia:

Cena za predmet zákazky sa bude hodnotiť nasledovným spôsobom: nakoľko predmetom hodnotenia ponuky je najnižšia cena celkom, komisia na vyhodnotenie ponúk alebo zodpovedný pracovník bude ponuky hodnotiť poradovým systémom. Ponuke s najnižšou cenou celkom za predmet zákazky bude priradené prvé miesto, ostatným ponukám druhé, tretie, atď. Úspešnou ponukou sa stane ponuka uchádzača, ktorá sa umiestni v zmysle vyššie uvedeného na prvom mieste, a ktorý splní podmienky účasti; ostatné ponuky sa stanú neúspešnými ponukami.

12. Lehota a spôsob predkladania ponúk:

- Lehota na predkladanie ponúk: **01.02.2021 do 12:00** hod.
- Doručenie výlučne elektronicky prostredníctvom systému EO EKS prostredníctvom profilu zákazky uvedeného v bode 1. tejto výzvy.
- Komunikácia medzi objednávateľom a hospodárskymi subjektmi sa uskutočňuje **výhradne elektronickým spôsobom prostredníctvom systému EO EKS**, ktorý zabezpečí trvalé zachytenie ich obsahu. V prípade preukázateľného výpadku/nedostupnosti systému EO EKS možno komunikáciu medzi verejným obstarávateľom/objednávateľom a záujemcami/uchádzačmi uskutočňovať aj písomne, vrátane predkladania ponúk – a to mailom na adresu kontaktnej osoby uvedenej v bode 1. tejto výzvy.
- Ponuky sa predkladajú v slovenskom jazyku.

13. Podmienky financovania predmetu zákazky:

Predmet zákazky sa bude financovať formou bezhotovostného platobného styku v lehote splatnosti 30 dní od jej doručenia objednávateľovi.
Verejný obstarávateľ neposkytuje zálohové platby, ani preddavok.

Prílohy:

- Príloha č. 1: Opis predmetu zákazky,
- Príloha č. 2: Cenník (vzor),
- Príloha č. 3: Čestné vyhlásenie o neexistencii konfliktu záujmov (vzor),

- Príloha č. 4: Návrh zmluvy.

----- v. r. -----

Ing. Ján Mrva
predseda ÚGKK SR

Príloha č.1 Opis predmetu zákazky

Predmetom zákazky je vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizácia opatrení pre potreby SR podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

Požiadavky kladené na informačné technológie verejnej správy v zmysle zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“)

Požiadavky zaistenia kybernetickej bezpečnosti v zmysle zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).

1. Požadovaná riadiaca dokumentácia Úradu geodézie, kartografie a katastra Slovenskej republiky (ďalej len „ÚGKK SR“) v oblasti informačnej bezpečnosti.

1.1 Vypracovanie/aktualizácia bezpečnostnej dokumentácie

Bezpečnostná dokumentácia musí byť vypracovaná s ohľadom na prevádzkovanú infraštruktúru IKT, aplikačnú a bezpečnostnú architektúru a implementované bezpečnostné opatrenia, organizačné usporiadanie, pracovné roly, zodpovednosti a rozdelenie právomocí v rámci riadenia operačných rizík rezortu ÚGKK SR.

1.1.1 Identifikácia legislatívnych a normatívnych požiadaviek:

Dokumentácia musí obsahovať komplexné posúdenie všetkých legislatívnych a normatívnych požiadaviek kladených na ÚGKK SR ako prevádzkovateľa základných služieb, ako prevádzkovateľa informačných technológií verejnej správy a ako organizáciu spracúvajúcu osobné údaje svojich zamestnancov, klientov a prípadných tretích osôb. Dokument musí určiť všetky relevantné požiadavky, mapovať ich plnenie v prostredí ÚGKK SR a stanoviť pravidlá priebežnej kontroly ich dodržiavania.

1.1.2 Návrh bezpečnostných politík informačnej / kybernetickej bezpečnosti

Bezpečnostné politiky musia obsahovať základné zásady a ciele v nasledovných oblastiach riadenia IB/KB:

1. Organizácia bezpečnosti
2. Riadenie bezpečnostných rizík
3. Riadenie informačných aktív
4. Riadenie dodávateľských vzťahov
5. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií
6. Riadenie a prevádzka informačno-komunikačných technológií
7. Riadenie súladu a kontinuity procesov a činností

1.1.3 Klasifikácia informácií a kategorizácia sietí a informačných systémov

Výstup musí obsahovať zoznam vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy a ich podporných systémov a podsystémov. Zoznam môže byť v textovej, tabuľkovej alebo grafickej forme a aktíva

musia byť klasifikované v súlade s klasifikačnou schémou podľa prílohy č. 2. Vyhlášky o BO KB. Osobitne musia byť ohodnotené osobné údaje spracúvané v jednotlivých informačných systémoch. Klasifikácia musí zároveň zahrňovať aj:

- popis a stav zabezpečenia Informačného systému,
- zhodnotenie bezpečnostných rizík,
- zhodnotenie zálohovania,
- návrh riešenia na konkrétne zistené problémy.

Zoznam vychádza z existujúceho dokumentu Objednávateľa - Štúdia zabezpečenia súladu a identifikácie povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (ďalej len „štúdia“) a súpisu uvedeného v bode 3.

1.2 Vymedzenie rozsahu a spôsobu plnenia opatrení

Predmetom zákazky je vypracovanie a dodanie súborov požadovanej dokumentácie v nasledovnom členení:

1. Organizácia informačnej bezpečnosti, riadenie aktív a rizík
2. Personálna bezpečnosť a riadenie dodávateľov.
3. Riadenie technických zraniteľností, bezpečnosti sietí a informačných systémov, správa riadenie prístupov k informačným systémom, využitie kryptografických mechanizmov
4. Bezpečnostné incidenty, riadenie, monitoring, testovanie a bezpečnostné audity
5. Fyzická bezpečnosť

1.2.1 Organizácia informačnej bezpečnosti

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- menovanie a určenie zodpovedností a právomocí manažéra informačnej a kybernetickej bezpečnosti,
- aplikovanie princípu najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,
- oddelenie zodpovedností a právomocí používateľov,
- aplikovanie zásady nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrovanie rizík,
- zásady jasného vymedzenia právomoci, povinnosti a zodpovednosti používateľov.

1.2.2 Riadenie aktív, hrozieb a rizík

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- inventarizácia všetkých aktív, od ktorých závisí poskytovanie služieb ÚGKK SR,
- identifikácia zodpovedných osôb za inventarizáciu aktív,
- identifikácia vlastníkov aktív,
- identifikácia zraniteľností a hrozieb,
- analýza rizík s ohľadom na identifikované aktíva,
- určenie vlastníkov rizík,
- návrh organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík,
- identifikácia implementovaných bezpečnostných opatrení,
- identifikácia bezpečnostných opatrení, ktoré nebudú implementované spolu s odôvodnením,

- analýza funkčného dopadu,
- návrh postupov pre pravidelné preskúvanie identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

1.2.3 Personálna bezpečnosť

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- postupy pri zaradení alebo presune osoby do niektorej z bezpečnostných rolí,
- postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,
- budovanie bezpečnostného povedomia a plán vzdelávania zamestnancov ÚGKK SR,
- hodnotenie účinnosti vzdelávania zamestnancov ÚGKK SR a dodávateľov zastávajúcich niektorú z bezpečnostných rolí,
- kontrola dodržiavania a riešenie prípadov porušenia definovaných bezpečnostných politík, vrátane disciplinárneho postupu pri ich porušení.

1.2.4 Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- popis spôsobu riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
- analýzu rizík dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
- návrh kontrolných a auditných postupov pre overenie dodržiavania bezpečnostných požiadaviek dodávateľmi služieb,
- definovanie obsahu zmluvy s treťou stranou, vývoj a akvizícia siete a informačného systému základnej služby s ohľadom na:
 - zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a
 - zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.

1.2.5 Riadenie technických zraniteľností systémov a zariadení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- metódy a nástroje na identifikáciu a ošetrovanie existujúcich zraniteľností SW a HW a využívanie publikovaných informácií (výrobcovia, bezpečnostné organizácie, ...) – s ohľadom na informácie uvedené v kapitole 6 štúdie.

1.2.6 Riadenie bezpečnosti sietí a informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- Pravidlá pre segmentáciu sietí a riadenie komunikácie medzi segmentami, blokovanie neautorizovaných portov a návrh segmentácie a komunikačných pravidiel s ohľadom na prevádzkované systémy a technológie v ÚGKK SR,
- Podmienky pre umiestnenie špecifikovaných služieb do vyhradených segmentov siete,
- Postupy pre bezpečnostnú konfiguráciu serverov,
- ochranu prepojenia medzi internými a externými sieťami, vytváranie black-listov,
- zaistenie bezpečného mobilného a vzdialeného prístupu do interných sietí,
- evidenciu a monitorovanie bezpečnosti všetkých vstupno-výstupných bodov na hranici siete, ochranu pred prienikom a únikom dát,
- ochranu pred škodlivým kódom na zariadeniach, ktoré sa pripájajú do internej siete z externého prostredia,

- zmluvné zaručenie bezpečnosti pripojenia dodávateľov vrátane preukázania plnenia.

1.2.7 Riadenie bezpečnosti prevádzky siete a informačného systému

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

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

1.2.8 Riadenie prístupov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- zásady riadenia prístupu k informáciám,
- identifikáciu a autentizáciu používateľov,
- práva a povinnosti používateľov a rolí zodpovedných za riadenie prístupu používateľov,
- riadenie prístupu k sieťam, operačnému systému a jeho službám, prístup k aplikáciám,
- riadenie vzdialeného prístupu,
- monitorovanie prístupov, vedenie prevádzkových záznamov o prístupe do siete a informačného systému,
- vykonávanie pravidelných kontrol prístupových účtov a prístupových oprávnení.

1.2.9 Používanie kryptografických opatrení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- používanie dostatočne odolných kryptografických prostriedkov na zaistenie dôvernosti, integrity, dostupnosti a hodnovernosti údajov v rámci sietí a informačných systémov,
- pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
- riadenie a ochranu kryptografických kľúčov a certifikátov počas ich celého životného cyklu,
- využívanie kryptografie pri dvojfaktorovej autentifikácii používateľov,
- vykonávanie kontroly a auditu v tejto oblasti.

1.2.10 Riešenie bezpečnostných incidentov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- detekciu, evidenciu a riešenie bezpečnostných incidentov,
- určenie právomocí a zodpovedností používateľov a zodpovedných rolí,
- postupy hlásenia bezpečnostných incidentov s dosahom na spracúvanie osobných údajov voči orgánu dohľadu a voči dotknutým osobám,
- pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálného systému včasného varovania.

1.2.11 Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- bezpečnostný dohľad nad činnosťou sietí, informačných systémov a ich používateľov,
- vytváranie a zaznamenávanie prevádzkových záznamov o

- manipulácii s osobnými, chránenými a prísne chránenými informáciami a údajmi alebo s nimi spojenými informačnými aktívami,
 - iniciácii, akceptácii alebo odmietnutí pripojenia do siete alebo informačného systému,
 - zmene prístupových práv používateľov,
 - zmene pravidiel bezpečnostných prvkov,
 - varovných alebo chybových hláseniach systémov,
 - podozrivých alebo škodlivých aktivitách a ďalších informáciách nevyhnutných na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia,
- ochranu a uchovávanie prevádzkových záznamov,
 - určenie zodpovedných rolí za monitorovanie a vyhodnocovanie prevádzkových záznamov, nahlásenie podozrivej aktivity,
 - vykonávanie auditu kybernetickej bezpečnosti.

1.2.12 Riadenie kontinuity procesov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- požiadavky na zabezpečenie kontinuity riadenia informačnej a kybernetickej bezpečnosti pri vzniku bezpečnostného incidentu,
- vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému,
- vykonanie analýzy dopadov bezpečnostného incidentu na prevádzkované služby,
- určenie adekvátnych zdrojov na zabezpečenie riadenia kontinuity činností,
- určenie komunikačného plánu spolu s kontaktnými údajmi, určeníami rolí a zodpovedností,
- určenie cieľovej doby a cieľového bodu obnovy,
- testovanie a vyhodnocovanie procesu riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
- určenie plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému,
- pravidelné preverenie záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.

1.2.13 Fyzická bezpečnosť a bezpečnosť prostredia

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- technické a organizačné opatrenia na zaistenie fyzickej ochrany siete a informačného systému alebo aspoň ich najdôležitejších komponentov pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií a fyzickým prístupom nepovolaných osôb,
- požiadavky na bezpečné uloženie fyzických záznamov obsahujúcich citlivé a osobné údaje a podmienky ich archivácie,
- ochranu prevádzkového priestoru v závislosti na kritickosti komponentov,
- kontrolu dodržiavania pravidiel na prácu v zabezpečenom priestore,
- zabezpečenie vhodného prevádzkového prostredia a dodávky podporných služieb,
- požiadavky na kapacity v bezpečne vzdialenom záložnom zabezpečenom priestore,
- zaistenie súladu prevádzky s vnútornými predpismi a zmluvnými záväzkami, zásadu „čistého stola“ a „čistej obrazovky“,
- kontrolu dodržiavania pravidiel,

- životný cyklus a ochranu technických komponentov sietí a informačných systémov a všetkých typov relevantných záloh.

1.3 Analýza rizík

Očakávaným výstupom je dokument, ktorý musí obsahovať posúdenie bezpečnostných rizík vyplývajúcich z hrozieb pôsobiacich na aktíva v správe ÚGKK SR.

2. Osobitné požiadavky

2.1 Posúdenie prevádzkovaných základných služieb

Výstup musí pokrývať identifikáciu a posúdenie prevádzkovaných základných služieb so zvážením súvisiacej infraštruktúry IKT, aplikačnej a bezpečnostnej architektúry a spoločenskej zodpovednosti ÚGKK SR.

2.2 Návrh bezpečnostnej stratégie kybernetickej bezpečnosti

Bezpečnostná stratégia kybernetickej bezpečnosti musí vychádzať z výsledkov analýzy rizík kybernetickej bezpečnosti a musí obsahovať formuláciu cieľov kybernetickej bezpečnosti a základné princípy na dosiahnutie týchto cieľov, určenie právomocí a zodpovedností za riadenie kybernetickej bezpečnosti, rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

2.3 Popis existujúceho stavu

V rámci analýzy je potrebné vychádzať zo štúdie. V kapitole 6, 7 a 9 štúdie je definovaná analýza aktuálneho stavu v rámci ÚGKK SR a riadených organizácií GKÚ a VÚGK.

V rámci navrhovania technických opatrení ÚGKK SR preferuje využitie existujúcich systémov monitoringu Zabbix, CA Spectrum, spracovania logov - Splunk log management, systémy pre file sharing – Microsoft SharePoint. Od úspešného uchádzača sa vyžaduje, aby sa primárne orientoval na využitie existujúcich systémov a ich prípadné rozšírenie novými modulmi.

V rámci riešenia bude vítaná iniciatíva úspešného uchádzača na konsolidáciu existujúcich supportných systémov a návrh optimalizácie ich využitia nielen v oblasti KB. V prípade ak z analýz vystane odporúčanie na implementáciu iného podporného systému, ktorý realizuje špecifický typ činnosti ÚGKK SR sa nebráni takejto implementácii.

2.4 Súvisiace aktivity

Bezpečnostné opatrenia navrhnuté v rámci tohto obstarania musia byť implementované v rámci existujúceho a súvisiacich obstarávaní a preto je dôležité osobitne špecifikovať technické požiadavky v nasledovných oblastiach:

- WAN siete – požiadavky na nastavenia FW, sledovania perimetra siete, pripojenie vzdialených pobočiek, parametre IPSEC
- VPN prístupy – zabezpečenie a odporúčané spôsoby pripojenia do privátnej siete, obmedzenia prístupov a protokolov
- LAN siete - požiadavky potrebné implementovať v rámci sietí LAN
- Servery – požiadavky potrebné implementovať na úrovni Operačných systémov a aplikácií
- Klientske PC – odporúčania na zabezpečenie pracovných staníc
- WIFI – odporúčania na zabezpečenia wifi sietí s dôrazom na rozdelenie pre Guest siete a privátne siete

2.5 Implementačné aktivity

Existujúce systémy monitorovania a spracovania logov – Zabbix, CA Spectrum, Splunk.

Na základe vzniknutej dokumentácie a popisov existujúceho stavu sa od úspešného uchádzača vyžaduje zabezpečenie implementácie monitoringu a logovania do existujúcich alebo novo špecifikovaných systémov slúžiacich na zber a vyhodnocovanie bezpečnostných udalostí na úrovni sietí, firewallov, serverov, klientskych staníc a ďalších identifikovaných zdrojov udalostí v rámci infraštruktúry ÚGKK SR.

Implementačnými aktivitami sa na účely tejto Zmluvy rozumejú služby poskytované úspešným uchádzačom v nasledovnom delení a rozsahu:

1. implementačné služby poskytované vo vzťahu k Informačným systémom v rámci infraštruktúry ÚGKK SR:
 - a. implementácia funkcionality zbierania Záznamov z prevádzky Informačných systémov (tzv. log collector) a nastavenie korelačných pravidiel vo vzťahu ku Kybernetickým bezpečnostným incidentom;
 - b. analýza prostredia ÚGKK SR, v ktorom sa nachádzajú Informačné systémy,
 - c. klasifikácia informácií a kategorizácia Informačných systémov.

V rámci implementácie požaduje ÚGKK SR návrh rozdelenia rolí, systémov projektov v systémoch monitoringu, stanovenia úrovni tresholdov v rámci delenia hrozieb a manuály na spracovanie incidentov v existujúcich alebo novo implementovaných systémoch

Pre využitie v budúcich projektoch sa od úspešného uchádzača vyžaduje vypracovanie implementačného manuálu a postupu ako pridávať ďalšie potrebné zdroje do systémov monitoringu a logovania udalostí. Implementačný manuál bude k dispozícii pre všetky cieľové existujúce alebo novo implementované podporné systémy.

3. Súpis Informačných systémov

V nasledujúcej tabuľke sa nachádza zoznam informačných systémov, ktoré sú prevádzkované v priestoroch Objednávateľa a je požadované spracovať základný rozsah bezpečnostného auditu v rozsahu uvedenom v kapitole 1.1.3 Opisu predmetu zákazky.

Informačným systémom sa rozumejú siete a informačné systémy ÚGKK SR, prostredníctvom ktorých je prevádzkovaná Základná služba, a to:

- elektronická komunikačná sieť;
- informačný systém; a
- každé zariadenie a komunikačný systém alebo Informácie, ktoré sú v sieťach a informačných systémoch podľa bodov i. a ii. tohto písm. vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov;

<i>Kategória</i>	<i>Názov systému</i>	<i>Typ aplikácie</i>	<i>Web server</i>	<i>Úložisko</i>	<i>Publikácia internet</i>	<i>Charakteristika systému</i>
Systémy správy katastra nehnuteľností						75 pracovísk KO OÚ (2x VÚK, 73x ostatné), kópie údajov ÚGKK, VÚGK, GKÚ
	WISKN	Desktop aplikácia		.dbf súbory	Nie	
	WRKN	Desktop aplikácia		MS SQL Server	Nie	
	SKM/Kokeš	Desktop aplikácia		.vgi súbory	Nie	
	VÚK	Desktop aplikácia		Oracle DB	Nie	Novšia verzia katastrálneho systému 2 lokality Pezinok, Galanta
Staršie katastrálne portály						

Nový katastrálny portál ESKN	Katasterportal	Webový portál	Oracle WebAS	Oracle DB	Ano	Postavené na Oracle technológiách
	Cica	Webový portál	IIS	Oracle DB, MS SQL	Ano	IIS, Aspx stránky
						Prešiel CSIRT testami; 3 prostredia
	eskn-portal	Webový portál	WebLogic	Oracle DB	Ano	Weblogic
	Portal	Webový portál	IIS	Oracle DB	Ano	MS IIS
	GisPortal	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	Správa používateľov	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	lom	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	Nevizuálne rozhrania	Dátové služby	IIS	Oracle DB	Ano	MS IIS
	Metainformačný systém ESKN	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
Nové interné systémy ESKN						3 prostredia
	Rezortná elektronická podateľňa	Backend služby	IIS	MS SQL Server	Nie	MS IIS, HSM, PKI
	Centrálne elektronické registratúrne stredisko	Webová aplikácia+služby	IIS	Oracle DB	Ano	MS IIS

Pomocné systémy KN	Centrálny systém katastra nehnuteľností	Webová aplikácia	WebLogic	Oracle DB	Ano	Weblogic
	Integračná platforma	ESB	Oracle SOA Suite	Oracle DB	Nie	Oracle SOA Suite
	Rezortný IAM	IAM		Oracle DB	Nie	
	Monitoring			Filesystem, DB	Nie	CA Spectrum, Zabix
	Splunk			Filesystem, DB	Nie	Splunk
	ELPO	Desktop aplikácia			Nie	
	ELODO	Webová aplikácia		HSM	Nie	PKI, HSM
Základná báza GIS	ArcGIS Desktop, ArcGIS Pro	Desktop aplikácia		Oracle DB, filesystem	Nie	
	LP360, LasTools	Desktop aplikácia		.LAS súbory, filesystem	Nie	
	Inpho MatchAT, OrthoVista, OrthoMaster	Desktop aplikácia		.TIF súbory, filesystem	Nie	
	Mapový klient ZBGIS	Webová aplikácia		Oracle DB, filesystem	Ano	
	Transformačná služba	Webová aplikácia		Oracle DB, filesystem	Ano	
	Konverzná služba	Webová aplikácia		Oracle DB, filesystem	Ano	

Interné systémy centra	Metainformačný systém ZBGIS	Webová aplikácia	Postgre SQL Server	Ano	
	Portál ZBGIS	Webový portál	Oracle DB, filesystem	Ano	
	Integračná platforma	ESB	Postgre SQL Server	Ano	
	Webové mapové služby	Dátové služby	Oracle DB, filesystem	Ano	
	Obchodný modul	Webová aplikácia	Oracle DB	Ano	
	Doména skgeodesy		LDAP		správa užívateľov cez ActiveDirectory (AD), DNS, Certifikačná autorita skgeodesy.local, DHCP
	Emailový server	Exchange server 15.0		Ano	Exchange -> Outlook-owa
	Intranet	webová stránka	IIS	Nie	
	Sharepoint		IIS	Nie	
	Kamerový bezpečnostný systém		File system	Nie	
GKÚ	SPIN	Webová aplikácia		Nie	Asseco ERP
	Dochádzkový systém	Webová aplikácia		Nie	
	Poskytovanie údajov	Webová aplikácia		Ano	

VÚGK	CallCentrum	Webová aplikácia		Nie	Call centrum manager
	SKPOS	Webová aplikácia+backend	Apache	Ano	Slovenská priestorová a observačná služba
	Skripty na distribúciu údajov SPI, SGI	Skripty na serveri		Filesytém	Nie
	Špecifické služby z KN + registrácia	Webová aplikácia		Oracle DB	Ano

Príloha č. 2 - Cenník

Názov položky	Parameter	Hodnota
Navrhovaná celková cena	V EUR bez DPH	
	DPH v EUR	
	V EUR s DPH	

Príloha č. 3 – Čestné vyhlásenie o neexistencii konfliktu záujmov (vzor)

Čestné vyhlásenie

[doplňte názov uchádzača], zastúpený [doplňte meno a priezvisko štatutárneho zástupcu] ako uchádzač, ktorý predkladá ponuku v rámci zadávania zákazky s nízkou hodnotou na predmet zákazky „Návrh organizačných a technických opatrení riadenia informačnej bezpečnosti v súlade s požiadavkami zaistenia kybernetickej bezpečnosti a ochrany osobných údajov v zmysle európskej a národnej legislatívy“ vyhláseným Úradom geodézie, kartografie a katastra Slovenskej republiky, týmto

čestne vyhlasujem, že

- v súvislosti s uvedeným postupom zadávania zákazky:
 - som nevyvíjal a nebudem vyvíjať voči žiadnej osobe na strane verejného obstarávateľa, ktorá je alebo by mohla byť zainteresovaná v zmysle ustanovení § 23 ods. 3 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v platnom znení („zainteresovaná osoba“) akékoľvek aktivity, ktoré by mohli viesť k zvýhodneniu nášho postavenia v súťaži,
 - som neposkytol a neposkytnem akejkoľvek čo i len potencionálne zainteresovanej osobe priamo alebo nepriamo akúkoľvek finančnú alebo vecnú výhodu ako motiváciu alebo odmenu súvisiacu so zadaním tejto zákazky,
 - budem bezodkladne informovať verejného obstarávateľa o akejkoľvek situácii, ktorá je považovaná za konflikt záujmov alebo ktorá by mohla viesť ku konfliktu záujmov kedykoľvek v priebehu procesu verejného obstarávania,
 - poskytnem verejnému obstarávateľovi v tomto zadávaní zákazky presné, pravdivé a úplné informácie.

V [doplňte miesto], dňa [doplňte dátum]

 a priezvisko
 osoby¹]

[doplňte meno
 a podpis oprávnenej

¹ Oprávnená osoba uchádzača, t. j. jeho štatutárny orgán alebo člen štatutárneho orgánu alebo iný zástupca uchádzača, ktorý je oprávnený konať v mene uchádzača v obchodných záväzkových vzťahoch.

Príloha č. 4 – Návrh zmluvy**Zmluva o dielo**

uzavretá podľa § 536 až 565 a podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „**Obchodný zákonník**“) a príslušných ustanovení zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o verejnom obstarávaní**“)
(ďalej len „**Zmluva**“)

medzi nasledovnými zmluvnými stranami

Objednávateľ:

Názov: Úrad geodézie, kartografie a katastra Slovenskej republiky
Sídlo: Chlumeckého 2, 820 12 Bratislava 212
IČO: 00166260
DIČ: 2020830240
Zastúpený: Ing. Ján Mrva, predseda
Bankové spojenie: Štátna pokladnica
Číslo účtu- IBAN: SK40 8180 0000 0070 0006 3046
 (ďalej len „**Objednávateľ**“)

a

Názov:

Sídlo:
IČO:
DIČ:
Zastúpený:
Zapísaný v:
Bankové spojenie:
Číslo účtu- IBAN:
 (ďalej len „**Zhotoviteľ**“)

(Objednávateľ a Zhotoviteľ spoločne ďalej len ako „**Zmluvné strany**“ a jednotlivito „**Zmluvná strana**“)

Úvodné ustanovenia

- A. Zmluvné strany uzatvárajú Zmluvu ako výsledok zadávania zákazky s nízkou hodnotou podľa zákona o verejnom obstarávaní na predmet zákazky „Návrh organizačných a technických opatrení riadenia informačnej bezpečnosti v súlade s požiadavkami zaistenia kybernetickej bezpečnosti a ochrany osobných údajov v zmysle európskej a národnej legislatívy“ (ďalej aj „zadávanie zákazky“) za podmienok uvedených v tejto Zmluve.
- B. Zhotoviteľ týmto vyhlasuje, že:
1. sa oboznámil a preskúmal všetky podmienky a okolnosti súvisiace s realizáciou predmetu zmluvy,
 2. predmet zmluvy je mu jasný a na základe svojej odbornej spôsobilosti, technického vybavenia a personálu, ktorý má k dispozícii, je spôsobilý a zaväzuje sa ho vykonávať riadne, kompletne a na požadovanej odbornej úrovni v súlade so zmluvou a všeobecne záväznými právnymi predpismi.

Článok I.

Predmet Zmluvy

1. Predmetom Zmluvy je záväzok Zhotoviteľa zhotoviť Dielo riadne, včas a bez vád:
 - a) **záväzok Zhotoviteľa zhotoviť a odovzdať Objednávateľovi „Riadiacu, prevádzkovú dokumentáciu a návrh a realizácia opatrení pre potreby ÚGKK SR“** podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým podľa požiadaviek kladených na informačné technológie vo verejnej správe v zmysle zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 134/2020 Z. z. (ďalej len „Zákon o ITVS“) a podľa požiadaviek zaistenia kybernetickej bezpečnosti v zmysle zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu (ďalej len „Úrad“), najmä vyhlášky č. 362/2018 a všeobecne záväzných právnych predpisov platných a účinných v Slovenskej republike upravujúcich tento druh činností, a to na 2 ks elektronického nosiča dát (formát PDF na CD/DVD, na USB kľúč, externý prenosný pevný disk s primeranou kapacitou a rozhraním nim. USB 3.0 alebo vyšším a pod.) a 2 ks tlačeneho vyhotovenia v slovenskom jazyku,
 - b) **záväzok Zhotoviteľa implementovať bezpečnostné opatrenia a zabezpečiť ich napojenie na systémy monitoringu a log processingu** do existujúcich alebo novo špecifikovaných systémov slúžiacich na zber a vyhodnocovanie bezpečnostných udalostí na úrovni sietí, firewallov, serverov, klientskych staníc a ďalších identifikovaných zdrojov udalostí v rámci infraštruktúry Objednávateľa („implementačné aktivity“),

a to všetko podľa špecifikácie uvedenej v prílohe č. 1 Zmluvy „Špecifikácia predmetu Zmluvy“, ktorá tvorí neoddeliteľnú súčasť Zmluvy (ďalej len „**príloha č. 1**“) a za podmienok uvedených v Zmluve, (ďalej aj „**Dielo**“ alebo „**Predmet zmluvy**“).
2. Objednávateľ sa zaväzuje zaplatiť Zhotoviteľovi za riadne, včas a bez vád dodané Dielo.

Článok II.

Čas, miesto a spôsob plnenia Zmluvy

1. Zhotoviteľ sa zaväzuje zhotoviť a odovzdať Dielo Objednávateľovi v termíne do 6 (šiestich) mesiacov odo dňa nadobudnutia účinnosti Zmluvy.
2. Zmluvné strany sa dohodli, že vykonanie Diela bude Zhotoviteľ realizovať na základe časového harmonogramu spracovaného za podmienok podľa tejto Zmluvy. Pre vylúčenie pochybností sa má za to, že úkony a činnosti uvedené v časovom harmonograme začínajú plynúť odo dňa účinnosti Zmluvy a končí sa dňom odovzdania a prevzatia ukončeného Diela. Pre vylúčenie pochybností sa má za to, že všetky taxatívne stanovené/dojednané lehoty podľa tejto Zmluvy, ktoré sú pre plnenie/splnenie povinnosti zo strany Zhotoviteľa alebo sú pre úkon akceptácie a/alebo potvrdenia a/alebo rozhodnutia zo strany Objednávateľa ustanovené/dojednané touto zmluvou, sú súčasťou časového

harmonogramu a v maximálnej dĺžke plynutia času započítané do časového harmonogramu predloženého Zhotoviteľom a o tieto sa časový harmonogram nemôže predlžovať.

3. Zhotoviteľ je povinný zhotoviť a odovzdať Dielo bez vád, riadne a včas. Dielo je zhotovené a odovzdané riadne, ak spĺňa všetky požiadavky podľa Zmluvy, podľa pokynov Objednávateľa a zodpovedá prílohe č. 1 Zmluvy.
4. Dielo musí byť zhotovené:
 - a) v kvalite stanovenej Objednávateľom, v súlade s platnými a účinnými technickými normami, v súlade s platnými a účinnými právnymi predpismi;
 - b) bez chýb, ktoré by mohli mať za následok vznik škody alebo inej ujmy na strane Objednávateľa alebo tretej osoby.
5. Miestom plnenia je sídlo Objednávateľa, pokiaľ Objednávateľ písomne neoznámí iné miesto plnenia.
6. Zhotoviteľ sa zaväzuje pri odovzdaní predmetu zmluvy tento odovzdať Objednávateľovi na dátovom nosiči (CD/DVD, USB kľúč, externý prenosný pevný disk s primeranou kapacitou a rozhraním nim. USB 3.0 alebo vyšším a pod.) a zároveň v listinnej podobe (pre výstupy podľa odseku 1 písm. a) článku I. tejto Zmluvy). Predmet zmluvy bude Zhotoviteľom odovzdaný v podobe, ktorá umožní jeho ďalšie využitie a spracovanie.
7. Zmluvné strany sa dohodli, že pred odovzdaním a prevzatím Diela Objednávateľ vykoná test poskytnutých implementačných aktivít. Pokiaľ test preukáže, že implementačné aktivity boli Zhotoviteľom realizované riadne a zodpovedajú výsledku predpokladanom Zmluvou, spíšu Zmluvné strany Protokol o prevzatí. V prípade, ak implementačné aktivity nebude možné na základe funkčných testov vykonať do termínu určeného v ods. 1 tohto článku tejto Zmluvy, považuje sa táto skutočnosť za podstatné porušenie Zmluvy zo strany Zhotoviteľa, pričom táto skutočnosť oprávňuje Objednávateľa od Zmluvy okamžite odstúpiť.
8. Závazok Zhotoviteľa zhotoviť Dielo je splnený dňom odovzdania riadne zhotoveného Diela bez vád Objednávateľovi v lehote podľa odseku 1 tohto článku tejto Zmluvy, tak aby Dielo bolo možné používať spôsobom a na účel dohodnutý v tejto Zmluve a podpisom Protokolu o prevzatí oprávnenou osobou Objednávateľa a Zhotoviteľa podľa článku VI. ods. 2 tejto Zmluvy. Odovzдание a prevzatie diela Zmluvné strany potvrdia podpísaním Protokolu o prevzatí, ktorý tvorí Prílohu č. 2 tejto Zmluvy.
9. Zhotoviteľ po zhotovení Diela vyzve e-mailom oprávnenú osobu Objednávateľa alebo písomne Objednávateľa najmenej päť (5) dní vopred na prevzatie Diela v sídle Objednávateľa.
10. Objednávateľ sa zaväzuje riadne zhotovené Dielo prevziať. Dielo je prevzaté Objednávateľom momentom podpísania Protokolu o prevzatí. Zodpovednosť Zhotoviteľa za zhotovené Dielo podľa príslušných právnych predpisov nie je jeho odovzdaním dotknutá.

11. Ak pri preberaní Diela Objednávateľ zistí, že má vady, ktoré bránia používaniu Diela, Dielo neprevezme a spíše so Zhotoviteľom zápis o zistených vadách, spôsobe a termíne ich odstránenia. Zhotoviteľ má povinnosť odovzdať Dielo po odstránení týchto väd. Až po odstránení väd môžu zmluvné strany pristúpiť k spísaniu Protokolu o prevzatí. V prípade, že má Dielo vady zistené pri odovzdávaní diela a Zhotoviteľ neodstráni vady v lehote do odovzdania Diela podľa odseku 1 tohto článku tejto Zmluvy, dostáva so do omeškania s odovzdaním Diela.
12. Odovzdaním diela podľa tohto článku tejto Zmluvy a podpisom Protokolu o prevzatí oprávnenou osobou Objednávateľa podľa článku VI. ods. 2 tejto Zmluvy sa Dielo bude považovať za vykonané a jeho predmet za odovzdaný Objednávateľovi.
13. Vlastnícke právo k Dielu, jeho logickým celkom ako aj jeho jednotlivým súčastiam, ktoré môžu byť predmetom vlastníckeho práva, prechádzajú na Objednávateľa dňom ich protokolárneho odovzdania Objednávateľovi. Týmto okamihom prechádza na Objednávateľa aj nebezpečenstvo škody na Diele.
14. Objednávateľovi vzniká právo užívať Dielo v súlade s touto zmluvou dňom podpísania Protokolu o prevzatí, ak sa zmluvné strany výslovne nedohodnú inak.

Článok III.

Cena a platobné podmienky

1. Celková cena za Predmet Zmluvy je stanovená ako výsledok zadávania zákazky uvedenej pod písm. A. Úvodných ustanovení tejto Zmluvy v súlade so zákonom NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhláškou Ministerstva financií SR č. 87/1996 Z. z., ktorou sa vykonáva zákon NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov nasledovne:
 - a. Eur bez DPH (slovom: Eur bez DPH) Eur s DPH (slovom: Eur s DPH).
2. V prípade, že sa v priebehu plnenia zmluvy z neplatiteľa DPH stane platiteľ DPH a naopak, cena za dielo sa z tohto dôvodu nebude meniť.
3. V prípade zmeny výšky sadzby DPH všeobecne záväzným právnym predpisom, bude cena upravená formou písomného dodatku k tejto Zmluve.
4. Zhotoviteľovi nevznikne nárok na úhradu akýchkoľvek dodatočných nákladov, ktoré nie sú započítané do ceny Predmetu Zmluvy. Cena za Predmet Zmluvy zohľadňuje primerané, preukázateľné náklady Zhotoviteľa a je konečná.
5. Cena za Predmet Zmluvy je konečná a zahŕňa všetky náklady Zhotoviteľa za Predmet Zmluvy podľa článku I. tejto Zmluvy a prílohy č. 1. Právo na zaplatenie ceny vznikne Zhotoviteľovi po riadnom a včasnom odovzdaní Diela bez väd, t.j. po podpísaní Protokolu o prevzatí.
6. Zmluvné strany sa dohodli, že cena za Predmet Zmluvy je určená podľa Informačných systémov Objednávateľa v čase podpisu tejto Zmluvy (v zmysle Prílohy č. 1 tejto Zmluvy).

V prípade, ak počas trvania Zmluvy dôjde k zmene rozsahu Informačných systémov zavedením, rozšírením alebo nasadením ďalšieho Informačného systému alebo jeho časti (napr. nový modul, nová alebo rozšírená funkcionálna Informačného systému a pod.), Zmluvné strany sa zaväzujú na základe vzájomnej dohody k primeranému navýšeniu ceny ešte pred takýmto zavedením, rozšírením alebo nasadením Informačného systému v súlade s § 18 zákona o verejnom obstarávaní postupom podľa ods. 2 článku XIII. tejto Zmluvy. V prípade, ak k navýšeniu ceny podľa predchádzajúcej vety nedôjde, Zhotoviteľ nie je povinný k poskytovaniu služieb predstavujúcich Predmet Zmluvy vo vzťahu k Informačným systémom podľa predchádzajúcej vety a nezodpovedá za akékoľvek škody, ktoré by v dôsledku absencie poskytovania služieb predstavujúcich Predmet Zmluvy vo vzťahu k týmto Informačným systémom Objednávateľovi alebo tretej osobe vznikli.

- a. Informačným systémom (ďalej len „Informačný systém“) sa na účely tejto Zmluvy rozumejú siete a informačné systémy Objednávateľa, prostredníctvom ktorých je prevádzkovaná Základná služba, a to:
 - i. elektronická komunikačná sieť;
 - ii. informačný systém; a
 - iii. každé zariadenie a komunikačný systém alebo Informácie, ktoré sú v sieťach a informačných systémoch podľa bodov i. a ii. tohto písm. vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov;
 - b. Základnou službou sa na účely tejto Zmluvy rozumie služba, ktorá je zaradená v zozname základných služieb podľa § 3 písm. k) Zákona o KB a:
 - i. závisí od informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 Zákona o KB;
 - ii. je informačným systémom verejnej správy podľa § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. v znení zákona č. 570/2009 Z. z. (§ 2 ods. 3 zákona č. 95/2019 Z. z.);
 - iii. je prvkom kritickej infraštruktúry podľa § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre;
7. Zhotoviteľovi nevznikne nárok na úhradu akýchkoľvek dodatočných nákladov, ktoré nie sú započítané do ceny Predmetu zmluvy. Cena za Predmet zmluvy zohľadňuje primerané, preukázateľné náklady a primeraný zisk Zhotoviteľa a je konečná.
 8. Cena za Predmet Zmluvy podľa odseku 1 tohto článku Zmluvy sa Zhotoviteľovi zaplatí na základe vystavenej faktúry, ktorej neoddeliteľnou súčasťou je Protokol o prevzatí. Úhrada faktúry sa realizuje bezhotovostným prevodom na bankový účet Zhotoviteľa uvedený v záhlaví Zmluvy. Akúkoľvek zmenu bankových údajov v priebehu zmluvného plnenia je Zhotoviteľ povinný neodkladne oznámiť Objednávateľovi a za týmto účelom nie je potrebné vyhotoviť dodatok k zmluve. Zmena čísla účtu bude vo vzťahu k Objednávateľovi účinná odo dňa písomného oznámenia zmeny Objednávateľovi.
 9. Splatnosť faktúry je tridsať (30) dní od jej doručenia na adresu Objednávateľa.

10. Faktúra musí spĺňať náležitosti daňového dokladu podľa príslušných právnych predpisov a dohodnutých zmluvných podmienok a musí obsahovať minimálne:
- číslo faktúry
 - obchodné meno a sídlo, IČO, DIČ Zhotoviteľa
 - obchodné meno a sídlo, IČO, DIČ Objednávateľa
 - deň odoslania a deň splatnosti faktúry
 - číslo a názov zmluvy
 - názov finančného ústavu a číslo účtu Zhotoviteľa, na ktorý má byť platba poukázaná
 - výška ceny bez dane v EUR, sadzba dane, fakturovaná suma celkom vrátane DPH
 - podpis oprávnenej osoby
 - povinnou prílohou faktúry je Protokol o prevzatí podpísaný oprávnenými zástupcami oboch zmluvných strán
11. V prípade, že faktúra nebude spĺňať náležitosti podľa príslušných právnych predpisov, prípadne bude obsahovať nesprávne, alebo neúplné údaje, Objednávateľ je oprávnený faktúru vrátiť pred jej splatnosťou Zhotoviteľovi na prepracovanie, ktorý vyhotoví novú faktúru, ktorej plynie nová tridsať (30) dňová lehota splatnosti, a to odo dňa je doručenia na adresu Objednávateľa.

Článok IV.

Práva a povinnosti Zmluvných strán

1. Práva a povinnosti Objednávateľa:

- a) Objednávateľ je povinný poskytnúť Zhotoviteľovi potrebnú súčinnosť pri plnení Predmetu Zmluvy, najmä poskytnúť Zhotoviteľovi na požiadanie všetky podklady, ktoré sú podľa Zhotoviteľa nevyhnutné pre zhotovenie Diela. Objednávateľ zodpovedá za správnosť a úplnosť ním poskytnutých podkladov. S poskytnutými podkladmi Zhotoviteľ nie je oprávnený nakladať inak ako za účelom zhotovenia Diela, najmä ich sprístupniť tretím osobám, a to ani po zániku/zrušení Zmluvy.
- b) Objednávateľ je oprávnený kontrolovať zhotovovanie Diela v každom stupni jeho realizácie. Ak pri kontrole zistí, že Zhotoviteľ porušuje svoje povinnosti, má právo žiadať, aby Zhotoviteľ odstránil vady vzniknuté vadnou realizáciou Diela a ďalej ho zhotovoval riadne.
- c) Objednávateľ je povinný včas informovať Zhotoviteľa o všetkých skutočnostiach potrebných na zabezpečenie úspešného plnenia záväzkov podľa Zmluvy.
- d) Objednávateľ sa zaväzuje zaplatiť Zhotoviteľovi za riadne zhotovené a dodané Dielo dohodnutú cenu v súlade s podmienkami Zmluvy.

- e) V súvislosti so zhotovovaním Diela v sídle Objednávateľa, je Objednávateľ povinný zabezpečiť prístup do vopred určených priestorov Objednávateľa zamestnancom Zhotoviteľa a týchto zamestnancov aj riadne poučiť o všetkých povinnostiach a bezpečnostných opatreniach súvisiacich s prítomnosťou v priestoroch Objednávateľa.

2. Práva a povinnosti Zhotoviteľa:

- a) Zhotoviteľ je povinný pri zhotovovaní Diela postupovať na vysokej profesionálnej úrovni, so všetkou odbornou starostlivosťou, ktorú možno pri poctivom obchodnom styku a realizácii predmetu zmluvy od Zhotoviteľa požadovať a riadne a včas plniť všetky svoje povinnosti podľa zmluvy a dodržiavať počas zmluvného plnenia administratívne nariadenia Objednávateľa, ktoré nie sú v rozpore so zmluvou a ktoré podmieňujú priebeh a okolnosti zmluvného plnenia.
- b) Zhotoviteľ je povinný realizovať predmet plnenia s využitím osôb/expertov, prostredníctvom ktorých preukazoval splnenie podmienok účasti v zadávaní zákazky na uzavretie tejto Zmluvy, a ktoré sa budú aktívne podieľať na riešení úloh projektu a budú garantovať kvalitu a odbornosť realizovaných činností a výstupov projektu počas celej doby trvania Zmluvy; menovite prostredníctvom:
- i.
 - ii.
- c) Zhotoviteľ je povinný vyžiadať si vopred písomný súhlas Objednávateľa, týkajúci sa zmeny expertov podľa písm. b) vyššie, ktorých používa na realizáciu tejto Zmluvy. V prípade, ak niektorý z uvedených expertov ukončí spoluprácu so Zhotoviteľom, v prípade úmrtia experta alebo v inom relevantnom prípade, ktorý zabraňuje expertovi riadne vykonávať plnenie tejto Zmluvy, je Zhotoviteľ povinný o tejto skutočnosti bez zbytočného odkladu písomne informovať Objednávateľa. Zhotoviteľ sa zaväzuje, že bude mať na realizáciu plnenia k dispozícii minimálne taký počet expertov, aký bol stanovený v rámci podmienok účasti v zadávaní zákazky na uzavretie tejto Zmluvy. Pri zmene experta, musí tento expert spĺňať minimálne požiadavky stanovené Objednávateľom v rámci podmienok účasti v zadávaní zákazky na uzavretie tejto Zmluvy. Žiadosť o písomný súhlas pri zmene experta predloží Zhotoviteľ v písomnej forme spolu s dokladmi preukazujúcimi splnenie predmetných minimálnych požiadaviek na expertov pred ich nástupom na výkon činností podľa tejto Zmluvy. Po kladnom stanovisku Objednávateľa môže príslušný expert začať vykonávať príslušné činnosti v rámci plnenia tejto Zmluvy.
- d) Zhotoviteľ je povinný zhotoviť Dielo na svoje náklady a na svoje riziko podľa podmienok uvedených v Zmluve.
- e) Zmluvné strany sa dohodli, že od pokynov Objednávateľa sa môže Zhotoviteľ odchýliť, len ak je to naliehavo nevyhnutné v záujme Objednávateľa a Zhotoviteľ nemôže včas dostať jeho súhlas. Zhotoviteľ je však povinný o takomto postupe Objednávateľa bez zbytočného odkladu písomne informovať,

- f) Zhotoviteľ je povinný bez zbytočného odkladu upozorniť na nevhodnú povahu alebo vady vecí, podkladov alebo pokynov daných mu Objednávateľom na realizáciu diela, ak Zhotoviteľ mohol túto nevhodnosť zistiť pri vynaložení odbornej spôsobilosti,
- g) Zhotoviteľ je povinný podľa potreby Objednávateľa zúčastňovať sa na rokovaníach k plneniu Predmetu Zmluvy.
- h) Zhotoviteľ je povinný oznámiť Objednávateľovi všetky okolnosti, ktoré zistil pri plnení svojich záväzkov, a ktoré môžu mať vplyv na zmenu pokynov Objednávateľa týkajúcich sa dosiahnutia účelu stanoveného Zmluvou alebo sú podľa názoru Zhotoviteľa nevyhnutné na riadne plnenie záväzkov podľa Zmluvy.
- i) Zhotoviteľ sa zaväzuje neodkladne písomne informovať Objednávateľa o každom prípadnom zdržaní, či iných skutočnostiach, ktoré by mohli ohroziť včasné a riadne vykonanie a odovzdanie Diela.
- j) Zhotoviteľ sa zaväzuje zabezpečiť od svojich zamestnancov a/alebo subdodávateľov realizujúcich dielo, plnenie nasledovných povinností:
 - 1. dodržiavanie záväzku mlčanlivosti o informáciách, s ktorými počas výkonu prác pre Objednávateľa prišli do styku, a to aj po ukončení pracovného alebo obdobného pomeru,
 - 2. zachovávať mlčanlivosť o údajoch, vrátane osobných údajoch, s ktorými počas výkonu prác pre Objednávateľa prišli do styku. Údaje, vrátane osobných údajov, ku ktorým počas plnenia tejto zmluvy prišiel Zhotoviteľ do styku, nesmie ďalej spracúvať ani ich využiť pre vlastnú potrebu.
- k) Zhotoviteľ je povinný oznámiť Objednávateľovi najmenej dvadsaťštyri (24) hodín vopred, že sa jeho zamestnanci dostavia do priestorov Objednávateľa za účelom poskytovania služieb súvisiacich s touto Zmluvou, pričom v rovnakej lehote je povinný predložiť Objednávateľovi písomný zoznam týchto zamestnancov, pričom zo zoznamu musí byť zrejmé, že títo zamestnanci spĺňajú kvalifikačné predpoklady na plnenie Predmetu Zmluvy (uviedenie pracovnej pozície) a boli poučení o povinnostiach podľa tejto Zmluvy (preukazujú svojim podpisom).
- l) V prípade, ak dôjde k zmene zmluvy podľa § 18 ods. 8 zákona o verejnom obstarávaní, povinnosti vyplývajúce z odseku 2 tohto článku Zmluvy sa vzťahujú aj na nového Zhotoviteľa.
- m) Zhotoviteľ nesmie plnenie podľa tejto rámcovej dohody ako celok odovzdať na realizáciu inému subjektu,
- n) Zhotoviteľ sa zaväzuje po ukončení poskytovania Predmetu Zmluvy odovzdať Objednávateľovi všetky podklady, dáta, údaje a informácie (najmä počítačovo spracované dáta a analýzy) súvisiace s plnením tejto Zmluvy, ktoré má k dispozícii,
- o) Zhotoviteľ sa zaväzuje v lehote do 3 pracovných dní po ukončení poskytovania Predmetu Zmluvy preukázateľne bezpečným spôsobom vymazať, odstrániť alebo iným spôsobom znehodnotiť všetky dáta (vrátane ich záložných kópií), ktoré mu poskytol

Objednávateľ v rámci súčinnosti za účelom alebo v súvislosti s predmetom plnenia Zmluvy, a o ich vymazaní, odstránení alebo znehodnotení písomne informovať Objednávateľa; v prípade listinných dokumentov sa Zhotoviteľ zaväzuje tieto bezodkladne vrátiť Objednávateľovi.

3. Zmluvné strany sa dohodli, že sa budú navzájom informovať o všetkých otázkach, ktoré súvisia s plnením predmetu Zmluvy.
4. Zmluvné strany sa pri realizácii diela zaväzujú poskytovať si vzájomne súčinnosť, ktorou sa pre účely tejto zmluvy rozumie taká súčinnosť zmluvných strán, ktorá je nevyhnutná a náležitá pre riadne plnenie tejto Zmluvy, a ktorá spočíva najmä v:
 - a) poskytnutí všetkých potrebných údajov, dokumentov a prístupov zo strany Objednávateľa, ktoré môžu byť oprávnené požadované zo strany Zhotoviteľa za účelom riadneho plnenia predmetu tejto zmluvy,
 - b) zo strany Objednávateľa v zabezpečení pripravenosti príslušných priestorov, v ktorých sa bude realizovať Dielo, vrátane ich uvoľnenia a sprístupnenia, zabezpečení funkčných prípojných miest na elektrickú energiu, zabezpečení prístupu zamestnancov Zhotoviteľa, resp. ním určených osôb do príslušných priestorov v súvislosti s plnením predmetu tejto zmluvy v rozsahu potrebnom k vykonaniu diela,
 - c) umožnením prístupu k hardvérovému a softvérovému vybaveniu Objednávateľa v rozsahu potrebnom k vykonaniu diela.
 - d) Zabezpečení súčinnosti tretích strán (dodávateľov informačných systémov) na strane Objednávateľa.

Článok V.

Zodpovednosť za chyby a záruka, zodpovednosť za škodu

1. V prípade omeškania so zhotovením Diela podľa článku II. tejto Zmluvy, prináleží Objednávateľovi zmluvná pokuta 0,05% z celkovej ceny diela s DPH uvedenej článku III tejto zmluvy za každý aj začatý deň omeškania, maximálne do 100% zmluvnej ceny Diela.
2. V prípade, ak bude Zhotoviteľ vykonávať plnenie Predmetu Zmluvy bez využitia osôb uvedených v článku IV, odsek 2 písm. b) tejto Zmluvy po dobu dvoch po sebe nasledujúcich týždňov alebo tieto osoby nahradí alebo zmení v rozpore s ust. článku IV, odsek 2 písm. c) tejto Zmluvy, je Objednávateľ oprávnený účtovať Zhotoviteľovi zmluvnú pokutu vo výške 500 € za každý jeden prípad.
3. Zmluvné strany sa dohodli, že zmluvná pokuta sa uplatňuje formou faktúry vystavenej Objednávateľom. Lehota na zaplatenie zmluvnej pokuty je 14 (štrnásť) kalendárnych dní odo dňa doručenia faktúry na zaplatenie zmluvnej pokuty Zhotoviteľovi. Na prijímanie, odosielanie a náležitosti faktúry sa primerane vzťahujú ustanovenia článku III. tejto zmluvy.

4. Zaplataenie zmluvnej pokuty nemá vplyv na nárok na náhradu škody vzniknutej v súvislosti s porušením zmluvných povinností, ktorú je možné vymáhať samostatne.
5. V prípade omeškania Objednávateľa so zaplataením ceny podľa tejto zmluvy, je Zhotoviteľ oprávnený požadovať zaplataenie úrokov z omeškania, ktoré je Zhotoviteľ oprávnený Objednávateľovi účtovať v sadzbe stanovenej všeobecne záväznými právnymi predpismi platnými a účinnými na území Slovenskej republiky v čase vyúčtovania úrokov z omeškania.
6. Zhotoviteľ zodpovedá za to, že Dielo bude zhotovené podľa tejto zmluvy, technických noriem a všeobecne záväzných právnych predpisov a že počas záručnej doby bude mať vlastnosti dohodnuté v tejto zmluve.
7. Zmluvné strany sa dohodli, že počas záručnej doby má Objednávateľ právo požadovať od Zhotoviteľa bezplatné odstránenie väd a Zhotoviteľ je povinný vady bezplatne odstrániť.
8. Nárok na odstránenie väd musí byť uplatnený písomne na adresu uvedenú v záhlaví tejto Zmluvy resp. elektronickou komunikáciou na adresu oprávnenej osoby Zhotoviteľa uvedenú v článku 6 ods. 1 písm. b) tejto Zmluvy.
9. Zhotoviteľ sa zaväzuje, že v každom konkrétnom prípade riadne reklamovanú vadu odstráni spôsobom a v termíne určenom Objednávateľom.
10. V prípade ak Zhotoviteľ nezačne práce na odstránení vady plnenia v dobe určenej Objednávateľom, je Objednávateľ v prípade akútnosti odstránenia problému oprávnený zabezpečiť odstránenie väd treťou stranou, pričom sa tento stav bude považovať za porušenie zmluvného plnenia zo strany Zhotoviteľa a Objednávateľovi vzniká oprávnenosť refundácie vzniknutých nákladov a škôd takýmto porušením spôsobených.
11. Záručná doba na Dielo je 24 mesiacov.

Článok VI. Oprávnené osoby

1. Osoby oprávnené na obchodné a vecné rokovania:
 - a) za Objednávateľa:

Meno a priezvisko:
e-mail:
tel.:
 - b) za Zhotoviteľa

Meno a priezvisko:
e-mail:
tel.:
2. Osoba oprávnená podpísať Protokol o prevzatí:
 - a) za Objednávateľa:

Meno a priezvisko:
--------------------	-------

e-mail:

tel.:

b) za Zhotoviteľa:

Meno a priezvisko:

e-mail:

tel:

Článok VII. Autorské práva

1. Ak v zmysle platných všeobecne záväzných právnych predpisov Slovenskej republiky výsledok činnosti Zhotoviteľa pri plnení Predmetu Zmluvy (vrátane jeho zamestnancov, iných osôb alebo akýchkoľvek tretích osôb, ktoré na plnenie Predmetu Zmluvy použil) bude chránený ako autorské dielo, momentom prevzatia odbornej služby, t.j. podpísaním Protokolu o prevzatí oboma Zmluvnými stranami, Zhotoviteľ bezodplatne poskytuje výhradne Objednávateľovi v neobmedzenom rozsahu licenciu na akékoľvek všeobecne záväznými právnymi predpismi vymedzené dovolené použitie tohto autorského diela po dobu trvania autorských práv (ďalej len „**Autorská licencia**“). Objednávateľ má právo tieto časti Diela ďalej spracovávať, prekladať, meniť alebo dopĺňať. Odplata za poskytnutie Autorskej licencie je zahrnutá v odmene za Dielo a a zmluvné strany majú za to, že je primeraná k rozsahu a spôsobu použitia predmetu ochrany práva duševného vlastníctva. Objednávateľ v rozsahu Autorskej licencie je oprávnený udeliť tretím osobám sublicenciu, ako aj postúpiť ju na tretiu osobu, s čím Zhotoviteľ súhlasí. Za prípadné nároky tretích osôb z dôvodu poskytnutia Autorskej licencie objednávateľovi zodpovedá Zhotoviteľ.
2. Zhotoviteľ zároveň vyhlasuje, že v prípade, že na tvorbu diela použil subdodávateľov, vysporiadal všetky právne záväzky týkajúce sa autorskoprávnej ochrany pred odovzdaním diela Objednávateľovi. V prípade uplatnenia akýchkoľvek nárokov subdodávateľov alebo tretích strán vyplývajúcich z porušenia autorských práv uplatnených po odovzdaní diela Objednávateľovi, nebude Objednávateľ zodpovedať za tieto nároky, resp. prípadnú škodu, ale zodpovednosť v plnej miere nesie Zhotoviteľ, ktorý sa zaviazal uvedené nároky vysporiadať ešte pred odovzdaním diela Objednávateľovi. Zhotoviteľ v uvedenom prípade plne zodpovedá za škodu spôsobenú Objednávateľovi, subdodávateľom alebo tretím osobám. Uvedené ustanovenie sa obdobne uplatní v prípade uplatnenia nárokov akýchkoľvek tretích osôb, ktoré nie sú subdodávateľom.
3. Hmotne zachytený výsledok činnosti Zhotoviteľa pri plnení Predmetu Zmluvy alebo jeho časť sa stáva po jeho akceptovaní, t.j. po podpísaní akceptačného protokolu zástupcami oboch zmluvných strán, vlastníctvom objednávateľa.

Článok VIII. Zánik Zmluvy a sankcie

1. Zmluva zaniká:
 - a) písomnou dohodou Zmluvných strán,

- b) písomnou výpoveďou,
 - c) písomným odstúpením od Zmluvy,
 - d) riadnym splnením Predmetu Zmluvy.
2. Dohoda podľa odseku 1 písm. a) tohto článku Zmluvy musí byť uzatvorená písomne, podpísaná oboma Zmluvnými stranami a musí obsahovať dohodu o vzájomnom vyrovnaní nevysporiadaných majetkovoprávných vzťahov vzniknutých v súvislosti so Zmluvou, inak je neplatná.
 3. Každá zo Zmluvných strán môže od Zmluvy odstúpiť v prípade podstatného porušenia povinností druhou Zmluvnou stranou. Odstúpenie je účinné doručením písomného oznámenia o odstúpení druhej Zmluvnej strane. Odstúpenie musí mať písomnú formu, musí byť doručené druhej Zmluvnej strane a musí v ňom byť uvedený konkrétny dôvod odstúpenia, inak je neplatné. Odstúpením od Zmluvy sa Zmluva neruší od počiatku, ale až odo dňa doručenia odstúpenia druhej Zmluvnej strane.
 4. Objednávateľ je oprávnený odstúpiť od Zmluvy pri podstatnom porušení Zmluvy Zhotoviteľom, pričom za podstatné porušenie Zmluvy Zhotoviteľom sa považuje najmä ak:
 - a) Zhotoviteľ opakovane porušil svoje zmluvné povinnosti uvedené v Zmluve, t. j. nezhotovil a neodovzdal Dielo riadne a včas, resp. v termínoch podľa Zmluvy,
 - b) na Zhotoviteľa bol podaný návrh na vyhlásenie konkurzu, bol na jeho majetok vyhlásený konkurz alebo bol návrh na jeho vyhlásenie zamietnutý pre nedostatok majetku alebo vstúpil do likvidácie alebo bolo začaté konanie o reštrukturalizácii,
 - c) Zhotoviteľ pri plnení Zmluvy závažným spôsobom porušuje práva tretích osôb,
 - d) ak súd právoplatne uzná kohokoľvek zo štatutárneho orgánu Zhotoviteľa alebo zamestnancov Zhotoviteľa za vinných z trestného činu bezprostredne súvisiaceho s uzatváraním a/alebo plnením tejto rámcovej dohody a/alebo objednávok vystavených na základe a v súlade s touto rámcovou dohodou,
 - e) má na základe dôveryhodných informácií dôvodné podozrenie, že Zhotoviteľ uzavrel v danom verejnom obstarávaní alebo počas plnenia Zmluvy, s iným hospodárskym subjektom Zmluvu narúšajúcu hospodársku súťaž.
 5. Objednávateľ je oprávnený odstúpiť od Zmluvy aj podľa § 19 zákona o verejnom obstarávaní.
 6. Zhotoviteľ je oprávnený odstúpiť od Zmluvy pri podstatnom porušení Zmluvy Objednávateľom, pričom za podstatné porušenie Zmluvy Objednávateľom sa považuje ak je Objednávateľ v omeškaní s platbou za faktúru o viac ako šesťdesiat (60) dní po jej splatnosti.
 7. Zmluvu môže ktorákoľvek zo Zmluvných strán písomne vypovedať bez udania dôvodu s 1- mesačnou výpovednou lehotou. Výpovedná lehota začína plynúť prvým dňom mesiaca

nasledujúceho po mesiaci, v ktorom bola písomná výpoveď doručená druhej Zmluvnej strane.

8. Predčasné ukončenie Zmluvy, bez ohľadu na Zmluvnú stranu, ktorá Zmluvu vypovedala alebo od nej odstúpila, sa nedotýka zodpovednosti Zhotoviteľa za vady dovtedy dodaného plnenia Predmetu Zmluvy.

Článok X.

Doručovanie a komunikácia Zmluvných strán

1. Akákoľvek písomná komunikácia medzi zmluvnými stranami v tejto súvislosti sa bude adresovať príslušnej zmluvnej strane na nižšie uvedenú adresu a bude sa považovať za doručenú v prípade:
 - a) doručenia faxom po tom, ako bolo odosielateľovi doručené potvrdenie, že prenos údajov prebehol v poriadku,
 - b) osobného doručenia prostredníctvom kuriérskej služby alebo inak, po jej prijatí,
 - c) doručenia e-mailom, po doručení potvrdenia od príjemcu o prijatí, pričom príjemca nie je oprávnený vo vlastnom e-mailovom klientovi odmietnuť odoslanie potvrdenia o prijatí e-mailu, alebo
 - d) doporučenej zásielky, k dátumu uvedenému na potvrdení o doručení alebo na potvrdení o tom, že zásielku nemožno doručiť.
2. Za deň doručenia zásielky Zmluvnej strane, ktorej bola adresovaná, sa považuje takisto deň:
 - a) v ktorom ju táto Zmluvná strana odoprela prijať,
 - b) ktorým márne uplynula odberná lehota pre jej vyzdvihnutie si na pošte alebo
 - c) v ktorý bola na nej zamestnancom pošty vyznačená poznámka, že “adresát sa odšťahoval”, “adresát je neznámy” alebo iná poznámka, ktorá podľa poštového poriadku znamená nedoručiteľnosť zásielky.
3. Na vylúčenie pochybností je osoba oprávnená na obchodné a vecné rokovania oprávnená uskutočniť všetky úkony podľa tejto Zmluvy, okrem úkonov smerujúcich k zmene alebo zániku Zmluvy. Zmena osoby oprávnenej na obchodné a vecné rokovania je Zmluvná strana povinná oznámiť druhej Zmluvnej strane, nevyžaduje sa uzavretie dodatku k Zmluve.
4. Písomná komunikácia bude adresovaná nasledovne:

Zásielky pre objednávateľa:

Úrad geodézie, kartografie a katastra Slovenskej republiky

Pre:

Adresa: Chlumeckého 2, 820 12 Bratislava

Telefón: +421 2 2081 6080

E-mail:

WEB: www.skgeodesy.sk

Zásielky pre Zhotoviteľa:

Do pozornosti: Zhotoviteľ názov

Meno Priezvisko

Adresa:

Telefón:

E-mail:

WEB:

5. Dôležité písomnosti podľa tejto Zmluvy (ako napr. oznámenia o odstúpení a iné písomné oznámenia) sa musia doručovať osobne alebo prostredníctvom doporučenej zásielky.

Článok XI.

Dôverné informácie

1. Pre účely a v rámci plnenia predmetu zmluvy sa vzájomne vymieňané a s predmetom plnenia súvisiace informácie považujú za dôverné (ďalej len „dôverná informácia“). Za dôverné sa považujú najmä informácie spadajúce do rozsahu obchodného tajomstva Zhotoviteľa podľa § 17 Obchodného zákonníka (teda všetky skutočnosti obchodnej, výrobnéj alebo technickej povahy súvisiace s podnikom Zhotoviteľa, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle Zhotoviteľa utajené a Zhotoviteľ zodpovedajúcim spôsobom ich utajenie zabezpečuje). Za dôverné sa podľa vôle Zhotoviteľa považujú najmä všetky technické informácie, ktoré sú súčasťou tejto zmluvy, ďalej know-how, štruktúra a hospodárske výsledky Zhotoviteľa, jeho majetok, pohľadávky a záväzky, stratégie a plány a informácie týkajúce sa predmetov chránených duševným vlastníctvom. Za dôverné sa považujú tiež informácie zmluvnou stranou ako pôvodcom takto výslovne označené.
2. Objednávateľ a Zhotoviteľ sa zaväzujú, že bez písomného súhlasu druhej zmluvnej strany akékoľvek dôverné informácie, zverené si navzájom pred, počas zmluvného plnenia, ako i v rámci plnenia predmetu tejto zmluvy, nesprístupnia tretím stranám ani ich nepoužijú na iné účely ako na účely plnenia predmetu tejto zmluvy a/alebo pre výkon práv vyplývajúci zo záväzkového vzťahu v rámci tejto zmluvy resp. zo záväzkového vzťahu vzniknutého v súvislosti s touto zmluvou.
3. Za porušenie záväzku podľa odseku 2 sa nepovažuje poskytnutie informácii v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov v rozsahu nevyhnutne potrebnom na základe uvedenej legislatívy, sprístupnenie informácií v rozsahu

požadovanom právoplatným rozhodnutím súdu alebo iného štátneho orgánu alebo právnymi predpismi SR, vrátane zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Pred takým sprístupnením informuje o požiadavke na sprístupnenie druhú zmluvnú stranu a vykoná primerané opatrenia potrebné na ochranu dôverných informácií druhej zmluvnej strany. Dotknutá zmluvná strana je v prípade takéhoto sprístupnenia povinná neodkladne na výzvu druhej zmluvnej strany označiť údaje a informácie, ktoré tvoria predmet jej obchodného tajomstva a z tohto dôvodu nemôžu byť sprístupnené.

4. Dôvernými informáciami nie sú informácie, ktoré sa bez porušenia tejto Zmluvy stali verejne známymi, informácie získané oprávnene inak, ako od druhej zmluvnej strany a informácie, ktorých používanie upravujú osobitné predpisy, napr. informácie, ktoré je objednávateľ povinný sprístupniť podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) alebo iných právnych predpisov.
5. Ustanovenie odseku 1 tejto Zmluvy sa nevzťahuje na splnenie povinnosti zverejňovať zmluvy podľa zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a Uznesenia vlády Slovenskej republiky č. 491/2010 alebo iného v budúcnosti prijatého právneho predpisu alebo uznesenia vlády SR. Zhotoviteľ je povinný na účely zverejnenia bezodkladne na výzvu objednávateľa označiť údaje a informácie, ktoré tvoria predmet jeho obchodného tajomstva a z tohto dôvodu nemôžu byť zverejnené.

Článok XII.

Ochrana osobných údajov

1. Zhotoviteľ za účelom poskytovania Predmetu Zmluvy je v nevyhnutnom rozsahu oprávnený na prístup k osobným údajom, ktoré sa nachádzajú v nasledovných informačných systémoch objednávateľa: Informačný systém geodézie, kartografie a katastra (ďalej len „informačný systém GKK“).
2. Zhotoviteľ podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“) a na neho nadväzujúceho zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 18/2018 Z. z.“) vystupuje ako „tretia strana“ pri prístupe k osobným údajom obsiahnutým v informačných systémoch objednávateľa. „Tretia strana“ je podľa GDPR fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.
3. V rámci predmetného informačného systému GKK uvedeného v ods. 1 tohto článku tejto Zmluvy má Zhotoviteľ prístup k osobným údajom dotknutých osôb, ktorými sa rozumejú

fyzické osoby, t.j. vlastníci a účastníci konaní, ktorých osobné údaje sú obsiahnuté v Informačnom systéme GKK (ďalej len „dotknuté osoby“).

4. Zhotoviteľ sa zaväzuje pri plnení tejto rámcovej dohody dodržiavať ustanovenia GDPR a zákona č. 18/2018 Z. z.
5. Zhotoviteľ je oprávnený osobné údaje, ku ktorým má prístup za účelom plnenia tejto rámcovej dohody iba prehliadať a nie je oprávnený vykonávať s nimi akékoľvek ďalšie operácie. Zhotoviteľ nie je oprávnený osobné údaje, ku ktorým má prístup za účelom plnenia tejto rámcovej dohody, ďalej spracúvať.
6. Za bezpečnosť sprístupnených osobných údajov zodpovedá Zhotoviteľ tým, že ich chráni najmä pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou alebo rozširovaním. Zhotoviteľ sa za týmto účelom zaväzuje prijať primerané technické, organizačné a personálne opatrenia.
7. Objednávateľ je oprávnený požadovať od Zhotoviteľa preukázanie vykonania všetkých predpísaných bezpečnostných opatrení na ochranu osobných údajov podľa bodu 9.6 tejto rámcovej dohody.
8. Zhotoviteľ sa zaväzuje preukázateľne poučiť svojich zamestnancov o ich právach a povinnostiach pri ochrane osobných údajov vyplývajúcich z platných právnych predpisov, ako aj o zodpovednosti v prípade ich porušenia.
9. Zhotoviteľ sa zaväzuje bezodkladne oznámiť objednávateľovi každý prípad podozrenia úniku, straty, zničenia, zneužitia alebo iného nenáležitého nakladania s osobnými údajmi.
10. Zhotoviteľ nie je oprávnený osobné údaje poskytnúť ani sprístupniť inej fyzickej osobe alebo právnickej osobe, ani nie je oprávnený tieto osobné údaje zverejniť a po ukončení platnosti tejto rámcovej dohody je povinný vykonať všetky opatrenia k tomu, aby osobné údaje, ku ktorým mal prístup počas plnenia tejto rámcovej dohody nemohli byť ďalej použité, predovšetkým aby nedošlo k ich neoprávnenému šíreniu, sprístupňovaniu, poskytovaniu alebo zverejňovaniu, alebo k akejkoľvek spracovateľskej alebo inej operácii a odovzdá objednávateľovi všetky doklady súvisiace s osobnými údajmi obsiahnutými v informačných systémoch objednávateľa, ku ktorým mal počas plnenia tejto rámcovej dohody prístup.
11. Ak Zhotoviteľ akýmkoľvek spôsobom poruší ktorúkoľvek zo svojich povinností uvedených v tomto článku tejto rámcovej dohody, je objednávateľ oprávnený uplatniť si voči Zhotoviteľovi nárok na zaplatenie zmluvnej pokuty vo výške 5 000 € (slovom päťtisíc eur). Objednávateľ je oprávnený uplatniť si voči Zhotoviteľovi právo na zaplatenie zmluvnej pokuty vo výške podľa tohto bodu rámcovej dohody za každé porušenie povinnosti podľa tohto článku tejto rámcovej dohody. Bod 6.7 tejto rámcovej dohody sa primerane vzťahuje aj na uplatnenie tejto zmluvnej pokuty.
12. Zhotoviteľ berie na vedomie, že v prípade porušenia ustanovení GDPR alebo zákona č. 18/2018 Z. z. je Úrad na ochranu osobných údajov Slovenskej republiky oprávnený uložiť sankcie. Pokiaľ Úrad na ochranu osobných údajov Slovenskej republiky udelí

objednávateľovi sankcie v súvislosti s činnosťou Zhotoviteľa a porušením jeho povinností pri ochrane osobných údajov podľa tejto rámcovej dohody, Zhotoviteľ sa zaväzuje zaplatiť sankcie uložené v dôsledku porušenia jeho povinností. Uvedené platí aj v prípade, že porušenie spôsobí ktorákoľvek z osôb, ktoré konali v mene Zhotoviteľa alebo v zastúpení Zhotoviteľa na základe zákonného zmocnenia, poverenia alebo plnej moci. Zhotoviteľ v tomto prípade zodpovedá ako keby porušenie spôsobil sám.

Článok XIII.

Záverečné ustanovenia

1. Zmluva nadobúda platnosť dňom jej podpísania Zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky podľa § 47a ods. 1 zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov v nadväznosti na § 5a ods. 1 a 6 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.
2. Akékoľvek zmeny a dodatky k Zmluve je možné uskutočniť len v súlade s § 18 zákona o verejnom obstarávaní a vo forme písomných dodatkov podpísaných oboma Zmluvnými stranami.
3. Ostatné, v Zmluve neupravené práva a povinnosti Zmluvných strán sa riadia príslušnými ustanoveniami Obchodného zákonníka v platnom znení a s ním súvisiacimi právnymi predpismi účinnými v Slovenskej republike.
4. Zmluvné strany sa zaväzujú prednostne riešiť prípadné spory zo Zmluvy zmierom a dohodou. V prípade, že zmier nebude dosiahnutý, spor z právnych úkonov z realizácie predmetu zmluvy bude predložený vecne a miestne príslušnému súdu Slovenskej republiky.
5. Zmluvné strany vyhlasujú, že Zmluva jasne a zrozumiteľne vyjadruje ich slobodnú a vážnu vôľu byť viazaný jej obsahom. Ďalej spoločne vyhlasujú, že si Zmluvu pozorne prečítali, porozumeli jej a na dôkaz súhlasu s ňou ju podpisujú.
6. Zmluva je vyhotovená v piatich (5) rovnopisoch, tri (3) pre Objednávateľa a dva (2) pre Zhotoviteľa.
7. Neoddeliteľnou súčasťou tejto Zmluvy sú prílohy:

Príloha č. 1: Špecifikácia Predmetu zmluvy

Príloha č. 2: Vzor protokolu o prevzatí

V Bratislave dňa

V dňa

Za Objednávateľa:

Za Zhotoviteľa:

.....
Ing. Ján Mrva
predseda

.....
Meno, priezvisko, titul
pozícia

Príloha č. 1 Zmluvy: Špecifikácia Predmetu zmluvy

Predmetom zákazky je vypracovanie a aktualizácia riadiacej, prevádzkovej dokumentácie a návrh a realizácia opatrení pre potreby SR podľa slovenských a európskych legislatívnych požiadaviek, predovšetkým:

Požiadavky kladené na informačné technológie verejnej správy v zmysle Zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o ITVS“)

Požiadavky zaistenia kybernetickej bezpečnosti v zmysle Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon o KB“) a nadväzujúcich vyhlášok Národného bezpečnostného úradu, najmä vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška o BO KB“).

1. Požadovaná riadiaca dokumentácia Úradu geodézie, kartografie a katastra Slovenskej republiky (ďalej len „ÚGKK SR“) v oblasti informačnej bezpečnosti.

1.1 Vypracovanie/aktualizácia bezpečnostnej dokumentácie

Bezpečnostná dokumentácia musí byť vypracovaná s ohľadom na prevádzkovanú infraštruktúru IKT, aplikačnú a bezpečnostnú architektúru a implementované bezpečnostné opatrenia, organizačné usporiadanie, pracovné roly, zodpovednosti a rozdelenie právomocí v rámci riadenia operačných rizík rezortu ÚGKK SR.

1.1.1 Identifikácia legislatívnych a normatívnych požiadaviek:

Dokumentácia musí obsahovať komplexné posúdenie všetkých legislatívnych a normatívnych požiadaviek kladených na ÚGKK SR ako prevádzkovateľa základných služieb, ako prevádzkovateľa informačných technológií verejnej správy a ako organizáciu spracúvajúcu osobné údaje svojich zamestnancov, klientov a prípadných tretích osôb. Dokument musí určiť všetky relevantné požiadavky, mapovať ich plnenie v prostredí ÚGKK SR a stanoviť pravidlá priebežnej kontroly ich dodržiavania.

1.1.2 Návrh bezpečnostných politík informačnej / kybernetickej bezpečnosti

Bezpečnostné politiky musia obsahovať základné zásady a ciele v nasledovných oblastiach riadenia IB/KB:

1. Organizácia bezpečnosti
2. Riadenie bezpečnostných rizík
3. Riadenie informačných aktív
4. Riadenie dodávateľských vzťahov
5. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií
6. Riadenie a prevádzka informačno-komunikačných technológií
7. Riadenie súladu a kontinuity procesov a činností

1.1.3 Klasifikácia informácií a kategorizácia sietí a informačných systémov

Výstup musí obsahovať zoznam vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy a ich podporných systémov a podsystémov. Zoznam môže byť v textovej, tabuľkovej alebo grafickej forme a aktíva musia byť klasifikované v súlade s klasifikačnou schémou podľa prílohy č. 2. Vyhlášky o

BO KB. Osobitne musia byť ohodnotené osobné údaje spracúvané v jednotlivých informačných systémoch. Klasifikácia musí zároveň zahrňovať aj:

- popis a stav zabezpečenia Informačného systému,
- zhodnotenie bezpečnostných rizík,
- zhodnotenie zálohovania,
- návrh riešenia na konkrétne zistené problémy.

Zoznam vychádza z existujúceho dokumentu Objednávateľa - Štúdia zabezpečenia súladu a identifikácie povinností vyplývajúcich zo zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (ďalej len „štúdia“) a súpisu uvedeného v bode 3.

1.2 Vymedzenie rozsahu a spôsobu plnenia opatrení

Predmetom zákazky je vypracovanie a dodanie súborov požadovanej dokumentácie v nasledovnom členení:

6. Organizácia informačnej bezpečnosti, riadenie aktív a rizík
7. Personálna bezpečnosť a riadenie dodávateľov.
8. Riadenie technických zraniteľností, bezpečnosti sietí a informačných systémov, správa riadenie prístupov k informačným systémom, využitie kryptografických mechanizmov
9. Bezpečnostné incidenty, riadenie, monitoring, testovanie a bezpečnostné audity
10. Fyzická bezpečnosť

1.2.1 Organizácia informačnej bezpečnosti

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- menovanie a určenie zodpovedností a právomocí manažéra informačnej a kybernetickej bezpečnosti,
- aplikovanie princípu najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,
- oddelenie zodpovedností a právomocí používateľov,
- aplikovanie zásady nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrovanie rizík,
- zásady jasného vymedzenia právomocí, povinností a zodpovedností používateľov.

1.2.2 Riadenie aktív, hrozieb a rizík

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- inventarizácia všetkých aktív, od ktorých závisí poskytovanie služieb ÚGKK SR,
- identifikácia zodpovedných osôb za inventarizáciu aktív,
- identifikácia vlastníkov aktív,
- identifikácia zraniteľností a hrozieb,
- analýza rizík s ohľadom na identifikované aktíva,
- určenie vlastníkov rizík,
- návrh organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík,
- identifikácia implementovaných bezpečnostných opatrení,
- identifikácia bezpečnostných opatrení, ktoré nebudú implementované spolu s odôvodnením,
- analýza funkčného dopadu,

- návrh postupov pre pravidelné preskúvanie identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

1.2.3 Personálna bezpečnosť

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- postupy pri zaradení alebo presune osoby do niektorej z bezpečnostných rolí,
- postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,
- budovanie bezpečnostného povedomia a plán vzdelávania zamestnancov ÚGKK SR,
- hodnotenie účinnosti vzdelávania zamestnancov ÚGKK SR a dodávateľov zastávajúcich niektorú z bezpečnostných rolí,
- kontrola dodržiavania a riešenie prípadov porušenia definovaných bezpečnostných politík, vrátane disciplinárneho postupu pri ich porušení.

1.2.4 Riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- popis spôsobu riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
- analýzu rizík dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
- návrh kontrolných a auditných postupov pre overenie dodržiavania bezpečnostných požiadaviek dodávateľmi služieb,
- definovanie obsahu zmluvy s treťou stranou, vývoj a akvizícia siete a informačného systému základnej služby s ohľadom na:
 - zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a
 - zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii.

1.2.5 Riadenie technických zraniteľností systémov a zariadení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- metódy a nástroje na identifikáciu a ošetrovanie existujúcich zraniteľností SW a HW a využívanie publikovaných informácií (výrobcovia, bezpečnostné organizácie, ...) – s ohľadom na informácie uvedené v kapitole 6 štúdie.

1.2.6 Riadenie bezpečnosti sietí a informačných systémov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- Pravidlá pre segmentáciu sietí a riadenie komunikácie medzi segmentami, blokovanie neautorizovaných portov a návrh segmentácie a komunikačných pravidiel s ohľadom na prevádzkované systémy a technológie v ÚGKK SR,
- Podmienky pre umiestnenie špecifikovaných služieb do vyhradených segmentov siete,
- Postupy pre bezpečnostnú konfiguráciu serverov,
- ochranu prepojenia medzi internými a externými sieťami, vytváranie black-listov,
- zaistenie bezpečného mobilného a vzdialeného prístupu do interných sietí,
- evidenciu a monitorovanie bezpečnosti všetkých vstupno-výstupných bodov na hranici siete, ochranu pred prienikom a únikom dát,
- ochranu pred škodlivým kódom na zariadeniach, ktoré sa pripájajú do internej siete z externého prostredia,
- zmluvné zaručenie bezpečnosti pripojenia dodávateľov vrátane preukázania plnenia.

1.2.7 Riadenie bezpečnosti prevádzky siete a informačného systému

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

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

1.2.8 Riadenie prístupov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- zásady riadenia prístupu k informáciám,
- identifikáciu a autentizáciu používateľov,
- práva a povinnosti používateľov a rolí zodpovedných za riadenie prístupu používateľov,
- riadenie prístupu k sieťam, operačnému systému a jeho službám, prístup k aplikáciám,
- riadenie vzdialeného prístupu,
- monitorovanie prístupov, vedenie prevádzkových záznamov o prístupe do siete a informačného systému,
- vykonávanie pravidelných kontrol prístupových účtov a prístupových oprávnení.

1.2.9 Používanie kryptografických opatrení

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- používanie dostatočne odolných kryptografických prostriedkov na zaistenie dôvernosti, integrity, dostupnosti a hodnovernosti údajov v rámci sietí a informačných systémov,
- pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
- riadenie a ochranu kryptografických kľúčov a certifikátov počas ich celého životného cyklu,
- využívanie kryptografie pri dvojfaktorovej autentifikácii používateľov,
- vykonávanie kontroly a auditu v tejto oblasti.

1.2.10 Riešenie bezpečnostných incidentov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- detekciu, evidenciu a riešenie bezpečnostných incidentov,
- určenie právomocí a zodpovedností používateľov a zodpovedných rolí,
- postupy hlásenia bezpečnostných incidentov s dosahom na spracúvanie osobných údajov voči orgánu dohľadu a voči dotknutým osobám,
- pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálnemu systému včasného varovania.

1.2.11 Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- bezpečnostný dohľad nad činnosťou sietí, informačných systémov a ich používateľov,
- vytváranie a zaznamenávanie prevádzkových záznamov o
 - manipulácii s osobnými, chránenými a prísne chránenými informáciami a údajmi alebo s nimi spojenými informačnými aktívami,

- iniciácii, akceptácii alebo odmietnutí pripojenia do siete alebo informačného systému,
 - zmene prístupových práv používateľov,
 - zmene pravidiel bezpečnostných prvkov,
 - varovných alebo chybových hláseniach systémov,
 - podozrivých alebo škodlivých aktivitách a ďalších informáciách nevyhnutných na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia,
- ochranu a uchovávanie prevádzkových záznamov,
 - určenie zodpovedných rolí za monitorovanie a vyhodnocovanie prevádzkových záznamov, nahlásenie podozrivej aktivity,
 - vykonávanie auditu kybernetickej bezpečnosti.

1.2.12 Riadenie kontinuity procesov

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- požiadavky na zabezpečenie kontinuity riadenia informačnej a kybernetickej bezpečnosti pri vzniku bezpečnostného incidentu,
- vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému,
- vykonanie analýzy dopadov bezpečnostného incidentu na prevádzkované služby,
- určenie adekvátnych zdrojov na zabezpečenie riadenia kontinuity činností,
- určenie komunikačného plánu spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti,
- určenie cieľovej doby a cieľového bodu obnovy,
- testovanie a vyhodnocovanie procesu riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
- určenie plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému,
- pravidelné preverenie záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.

1.2.13 Fyzická bezpečnosť a bezpečnosť prostredia

Opatrenia popísané v jednotlivých dokumentoch/výstupoch musia pokrývať:

- technické a organizačné opatrenia na zaistenie fyzickej ochrany siete a informačného systému alebo aspoň ich najdôležitejších komponentov pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií a fyzickým prístupom nepovolaných osôb,
- požiadavky na bezpečné uloženie fyzických záznamov obsahujúcich citlivé a osobné údaje a podmienky ich archivácie,
- ochranu prevádzkového priestoru v závislosti na kritickosti komponentov,
- kontrolu dodržiavania pravidiel na prácu v zabezpečenom priestore,
- zabezpečenie vhodného prevádzkového prostredia a dodávky podporných služieb,
- požiadavky na kapacity v bezpečne vzdialenom záložnom zabezpečenom priestore,
- zaistenie súladu prevádzky s vnútornými predpismi a zmluvnými záväzkami, zásadu „čistého stola“ a „čistej obrazovky“,
- kontrolu dodržiavania pravidiel,
- životný cyklus a ochranu technických komponentov sietí a informačných systémov a všetkých typov relevantných záloh.

1.3 Analýza rizík

Očakávaným výstupom je dokument, ktorý musí obsahovať posúdenie bezpečnostných rizík vyplývajúcich z hrozieb pôsobiacich na aktíva v správe ÚGKK SR.

2. Osobitné požiadavky

2.1 Posúdenie prevádzkovaných základných služieb

Výstup musí pokrývať identifikáciu a posúdenie prevádzkovaných základných služieb so zvážením súvisiacej infraštruktúry IKT, aplikačnej a bezpečnostnej architektúry a spoločenskej zodpovednosti ÚGKK SR.

2.2 Návrh bezpečnostnej stratégie kybernetickej bezpečnosti

Bezpečnostná stratégia kybernetickej bezpečnosti musí vychádzať z výsledkov analýzy rizík kybernetickej bezpečnosti a musí obsahovať formuláciu cieľov kybernetickej bezpečnosti a základné princípy na dosiahnutie týchto cieľov, určenie právomocí a zodpovedností za riadenie kybernetickej bezpečnosti, rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

2.3 Popis existujúceho stavu

V rámci analýzy je potrebné vychádzať zo štúdie. V kapitole 6, 7 a 9 štúdie je definovaná analýza aktuálneho stavu v rámci ÚGKK SR a riadených organizácií GKÚ a VÚGK.

V rámci navrhovania technických opatrení ÚGKK SR preferuje využitie existujúcich systémov monitoringu Zabbix, CA Spectrum, spracovania logov - Splunk log management, systémy pre file sharing – Microsoft SharePoint. Od Zhotoviteľa sa vyžaduje, aby sa primárne orientoval na využitie existujúcich systémov a ich prípadné rozšírenie novými modulmi.

V rámci riešenia bude vítaná iniciatíva Zhotoviteľa na konsolidáciu existujúcich supportných systémov a návrh optimalizácie ich využitia nielen v oblasti KB. V prípade ak z analýz vystane odporúčanie na implementáciu iného podporného systému, ktorý realizuje špecifický typ činnosti ÚGKK SR sa nebráni takejto implementácii.

2.4 Súvisiace aktivity

Bezpečnostné opatrenia navrhnuté v rámci tohto obstarania musia byť implementované v rámci existujúceho a súvisiacich obstarávaní a preto je dôležité osobitne špecifikovať technické požiadavky v nasledovných oblastiach:

- WAN siete – požiadavky na nastavenia FW, sledovania perimetra siete, pripojenie vzdialených pobočiek, parametre IPSEC
- VPN prístupy – zabezpečenie a odporúčané spôsoby pripojenia do privátnej siete, obmedzenia prístupov a protokolov
- LAN siete - požiadavky potrebné implementovať v rámci sietí LAN
- Servery – požiadavky potrebné implementovať na úrovni Operačných systémov a aplikácií
- Klientske PC – odporúčania na zabezpečenie pracovných staníc
- WIFI – odporúčania na zabezpečenia wifi sietí s dôrazom na rozdelenie pre Guest siete a privátne siete

2.5 Implementačné aktivity

Existujúce systémy monitorovania a spracovania logov – Zabbix, CA Spectrum, Splunk.

Na základe vzniknutej dokumentácie a popisov existujúceho stavu sa od Zhotoviteľa vyžaduje zabezpečenie implementácie monitoringu a logovania do existujúcich alebo novo špecifikovaných systémov slúžiacich na zber a vyhodnocovanie bezpečnostných udalostí na úrovni sietí, firewallov, serverov, klientskych staníc a ďalších identifikovaných zdrojov udalostí v rámci infraštruktúry ÚGKK SR.

Implementačnými aktivitami sa na účely tejto Zmluvy rozumejú služby poskytované Zhotoviteľom v nasledovnom delení a rozsahu:

2. implementačné služby poskytované vo vzťahu k Informačným systémom v rámci infraštruktúry ÚGKK SR:
 - a. implementácia funkcionality zbierania Záznamov z prevádzky Informačných systémov (tzv. log collector) a nastavenie korelačných pravidiel vo vzťahu ku Kybernetickým bezpečnostným incidentom;
 - b. analýza prostredia ÚGKK SR, v ktorom sa nachádzajú Informačné systémy,
 - c. klasifikácia informácií a kategorizácia Informačných systémov.

V rámci implementácie požaduje ÚGKK SR návrh rozdelenia rolí, systémov projektov v systémoch monitoringu, stanovenia úrovni tresholdov v rámci delenia hrozieb a manuály na spracovanie incidentov v existujúcich alebo novo implementovaných systémoch

Pre využitie v budúcich projektoch sa od Zhotoviteľa vyžaduje vypracovanie implementačného manuálu a postupu ako pridávať ďalšie potrebné zdroje do systémov monitoringu a logovania udalostí. Implementačný manuál bude k dispozícii pre všetky cieľové existujúce alebo novo implementované podporné systémy.

3. Súpis Informačných systémov (v zmysle definície uvedenej v článku III, ods. 6 písm. a. Zmluvy)

V nasledujúcej tabuľke sa nachádza zoznam informačných systémov, ktoré sú prevádzkované v priestoroch Objednávateľa a je požadované spracovať základný rozsah bezpečnostného auditu v rozsahu uvedenom v kapitole 1.1.3

<i>Kategória</i>	<i>Názov systému</i>	<i>Typ aplikácie</i>	<i>Web server</i>	<i>Úložisko</i>	<i>Publikácia internet</i>	<i>Charakteristika systému</i>
Systémy správy katastra nehnuteľností						75 pracovísk KO OÚ (2x VÚK, 73x ostatné), kópie údajov ÚGKK, VÚGK, GKÚ
	WISKN	Desktop aplikácia		.dbf súbory	Nie	
	WRKN	Desktop aplikácia		MS SQL Server	Nie	
	SKM/Kokeš	Desktop aplikácia		.vgi súbory	Nie	
	VÚK	Desktop aplikácia		Oracle DB	Nie	Novšia verzia katastrálneho systému 2 lokality Pezinok, Galanta
Staršie katastrálne portály						
	Katasterportal	Webový portál	Oracle WebAS	Oracle DB	Ano	Postavené na Oracle technológiách
	Cica	Webový portál	IIS	Oracle DB, MS SQL	Ano	IIS, Aspx stránky
Nový katastrálny portál ESKN						Prešiel CSIRT testami; 3 prostredia
	eskn-portal	Webový portál	WebLogic	Oracle DB	Ano	Weblogic
	Portal	Webový portál	IIS	Oracle DB	Ano	MS IIS

Nové interné systémy ESKN	GisPortal	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	Správa používateľov	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	Iom	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
	Nevizuálne rozhrania	Dátové služby	IIS	Oracle DB	Ano	MS IIS
	Metainformačný systém ESKN	Webová aplikácia	IIS	Oracle DB	Ano	MS IIS
						3 prostredia
	Rezortná elektronická podateľňa	Backend služby	IIS	MS SQL Server	Nie	MS IIS, HSM, PKI
	Centrálne elektronické registratúrne stredisko	Webová aplikácia+služby	IIS	Oracle DB	Ano	MS IIS
	Centrálny systém katastra nehnuteľností	Webová aplikácia	WebLogic	Oracle DB	Ano	Weblogic
	Integračná platforma	ESB	Oracle SOA Suite	Oracle DB	Nie	Oracle SOA Suite
Pomocné systémy KN	Rezortný IAM	IAM		Oracle DB	Nie	
	Monitoring			Filesystem, DB	Nie	CA Spectrum, Zabbix
	Splunk			Filesystem, DB	Nie	Splunk

Základná báza GIS

ELPO	Desktop aplikácia		Nie	
ELODO	Webová aplikácia	HSM	Nie	PKI, HSM
ArcGIS Desktop, ArcGIS Pro	Desktop aplikácia	Oracle DB, filesystem	Nie	
LP360, LasTools	Desktop aplikácia	.LAS súbory, filesystem	Nie	
Inpho MatchAT, OrthoVista, OrthoMaster	Desktop aplikácia	.TIF súbory, filesystem	Nie	
Mapový klient ZBGIS	Webová aplikácia	Oracle DB, filesystem	Ano	
Transformačná služba	Webová aplikácia	Oracle DB, filesystem	Ano	
Konverzná služba	Webová aplikácia	Oracle DB, filesystem	Ano	
Metainformačný systém ZBGIS	Webová aplikácia	Postgre SQL Server	Ano	
Portál ZBGIS	Webový portál	Oracle DB, filesystem	Ano	
Integračná platforma	ESB	Postgre SQL Server	Ano	
Webové mapové služby	Dátové služby	Oracle DB, filesystem	Ano	
Obchodný modul	Webová aplikácia	Oracle DB	Ano	

**Interné systémy
centra**

	Doména skgeodesy		LDAP		správa užívateľov cez ActiveDirectory (AD), DNS, Certifikačná autorita skgeodesy.local, DHCP
	Emailový server	Exchange server 15.0		Ano	Exchange -> Outlook-owa
	Intranet	webová stránka	IIS	Nie	
	Sharepoint		IIS	Nie	
	Kamerový bezpečnostný systém		File system	Nie	
	SPIN	Webová aplikácia		Nie	Asseco ERP
	Dochádzkový systém	Webová aplikácia		Nie	
GKÚ	Poskytovanie údajov	Webová aplikácia		Ano	
	CallCentrum	Webová aplikácia		Nie	Call centrum manager
	SKPOS	Webová aplikácia+backend	Apache	Ano	Slovenská priestorová a observačná služba
VÚGK	Skripty na distribúciu údajov SPI, SGI	Skripty na serveri	Filesytém	Nie	

Špecifické služby z KN + registrácia	Webová aplikácia	Oracle DB	Ano
-----------------------------------------	------------------	-----------	-----

Príloha č. 2: Vzor protokolu o prevzatí

PROTOKOL O PREVZATÍ

Objednávateľ: Zhotoviteľ:	Úrad geodézie, kartografie a katastra Slovenskej republiky		
Zmluva č.:			
Predmet prevzatia (dielo):			
Miesto prevzatia:		Dátum:	
Osoby oprávnené na akceptáciu:	Za Objednávateľa: Za Zhotoviteľa:		
Vykonané kontroly, testy:			
Zistené vady:			
Termín a spôsob odstránenia väd			
Odovzdaná dokumentácia:			

Potvrdenie o prevzatí:					
Za Objednávateľa:			Za Zhotoviteľa:		
Meno	Podpis	Dátum	Meno	Podpis	Dátum