908

ZMLUVA O POSKYTOVANÍ SLUŽIEB PRE PREVÁDZKU A ÚDRŽBU INFORMAČNÝCH SYSTÉMOV SAMOSPRÁVY

uzatvorená v zmysle § 269 ods. 2 v spojení s § 261 ods. 2 zákona 513/91 Z.z. - Obchodný zákonník v znení neskorších predpisov (ďalej len „zmluva")

I. ZMLUVNÉ STRANY

1. Objednávateľ:

   Názov: Mesto Poprad

   Sídlo: Nábrežie Jána Pavla II. 2802/3, 058 42 Poprad

   Štatutárny orgán: Ing. Anton Danko – primátor mesta

   Osoba oprávnená na jednanie vo veciach zmluvy: Mgr. Jaroslav Maitner

   Osoba oprávnená na jednanie v technických veciach: Mgr. Jaroslav Maitner

   IČO: 00326470

   DIČ: 2021031144

   IČ DPH: Mesto Poprad nie je platcom DPH, SK 2021031144 – zdaniteľná osoba registrovaná pre daň podľa §7a Zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov

   Bankové spojenie: Všeobecná úverová banka, a.s.

   IBAN: SK75 0200 0000 0000 2452 4562

   SWIFT(BIC): SUBASKBX

   (ďalej v texte len „objednávateľ")

2. Poskytovateľ:

   Obchodné meno: CORA GEO, s. r. o.

   Sídlo: A. Kmeťa 5397/23, 036 01 Martin

   Prevádzka: Štefánikova 15, 058 01 Poprad

   Štatutárny zástupca: Ing. Jozef Habiňák, konateľ

   Osoba oprávnená na jednanie vo veciach Zmluvy: Ing. Ján Valko

   Osoba oprávnená na jednanie v technických veciach: Ing. Ján Valko

   IČO: 31612989

   DIČ: 2020433888

   IČ DPH: SK2020433888

   Bankové spojenie: UniCredit Bank Slovakia, a.s.

   IBAN: SK39 1111 0000 0066 0540 5016

   SWIFT(BIC): UNCRSKBX

   Zápis v registri: Zapísaná v Obchodnom registri OS Žilina, oddiel Sro., vložka č. 2134 L

   (ďalej v texte len „poskytovateľ")

   (ďalej v texte objednávateľ a poskytovateľ spolu len „zmluvné strany")

Uzatvárajú túto zmluvu ako výsledok zadávania nadlimitnej zákazky, vyhlásenej vo vestníku EU s názvom predmetu: „Poskytovanie služieb pre prevádzku a údržbu informačných systémov“, s cieľom zabezpečiť plnohodnotné využívanie existujúcich informačných systémov Mesta Poprad.

II. PREDMET PLNENIA

1. Predmetom tejto zmluvy je odplatné poskytovanie v tejto zmluve stanovených služieb poskytovateľom pre prevádzku a údržbu informačných systémov poskytovateľa v produkčnom a testovacom prostredí a to informačného systému samosprávy (ďalej „CG ISS“), dokumentačného informačného systému (ďalej len „CG DISS), geografického informačného systému (ďalej len „CG GISAM“) a CG WebGIS, riešenia pre podporu eGovernmentu (ďalej len „CG eGOV“) spolu s integračným rozhraním v zmysle Dohody o integračnom zámere Mesta Poprad a NASES, a súvisiacich aktivít s cieľom zabezpečiť plnohodnotné využívanie dodaných produktov v nasledujúcich rokoch v nasledovnom členení:

- Údržba licencií dodaného licenčného softvéru
- Update - údržba licencií dodaného aplikačného softvéru
- Upgrade - technické zhodnotenie dodaného aplikačného softvéru
- Hot - line podpora
- Riadenie projektu
- Technická podpora
- Metodická podpora
- Školenia
- Bezpečnostná politika

(ďalej v texte len „Podpora“) za podmienok uvedených v tejto zmluve vrátane jej príloh.

Výklad pojmov na účely tejto zmluvy:

- ASW - znamená aplikačný softvér,
- LSW - znamená databázový softvér
- ISS - znamená informačný systém samosprávy,
- NU - znamená licencie pre pomenovaných používateľov,
- ANU - znamená licencia pre pomenovaného správcu ,
- Multilicencia - znamená licencia pre ľubovoľný počet používateľov,
- Portál Modul - znamená licencia na Portál ISS,
- CPU - znamená hlavný procesor počítača
- ASFU - znamená druh licencie
- HW - znamená hardvérové vybavenie
- ČD - znamená človekodní = 8 človekohodín
- ČH - znamená človekohodín = 60 minút práce jedného človeka,
- HotLine - znamená služba zhotoviteľa, komunikácia prostredníctvom mailov, telefonátov a vzdialenej správy
- SQL dávky - znamená databázové dávky
- UPDATE - znamená aktualizácia dodaného IS na novšiu verziu zo strany poskytovateľa
- UPGRADE - znamená dodanie vyššej verzie dodaného IS zo strany poskytovateľa
- 1 ČH - znamená človekohodina = 60 min

- 1 ČD - znamená človekodeň = 8 ČH
- Ročná podpora - znamená podpora poskytovaná v priebehu jedného kalendárneho roka
- FO - znamená fyzická osoba
- PO - znamená právnická osoba
- Autorský zákon - znamená zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov
- Zmluvný rozsah - znamená predplatený rozsah danej služby/ podpory na jeden rok.
- HelpDesk znamená portál poskytovateľa pre zapisovanie požiadaviek objednávateľa

2. Poskytovateľ týmto prehlasuje, že je v plnom rozsahu oprávnený vykonávať predmet tejto zmluvy.

3. Ročná podpora pozostáva z nižšie uvedených činností:

Časť 1. Údržba licencií dodaného licenčného softvéru

- Aktualizácia verzií licenčného softvéru ORACLE v termínoch vydania a podľa pravidiel autorskej spoločnosti.

Časť 2. UPDATE – Údržba licencií dodaného aplikačného softvéru

- Priebežné vykonávanie zmien vyplývajúcich zo všeobecne platnej legislatívy, ktoré priamo súvisia s funkciami príslušného modulu aplikačného softvéru.
- Zaisťovanie kompatibility aplikačného softvéru s novými verziami operačného systému používaného objednávateľom.
- Zaisťovanie kompatibility integračného rozhrania voči Ústrednému portálu verejnej správy a centrálnym registrom FO, PO a adries.
- Oprava chýb aplikačného softvéru vo forme kumulatívnych zmien a nových verzií.
- Kontrola implementácie nových verzií softvéru a súvisiacich opráv.
- Poplatok za používanie licencií v súlade s Autorským zákonom.
- Zapracovanie opisu zmien a dokumentácie k aplikačnému softvéru.

Zoznam modulov aplikačného softvéru a počet licencií, ktorých sa týka UPDATE tvorí Prílohu č. 3 tejto zmluvy.

Časť 3. UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru

- Zapracovanie špecifických požiadaviek – špecifickou požiadavkou sa rozumie požiadavka, ktorá sa realizuje na podnet objednávateľa a bude zabezpečovať spracovanie údajov podľa jeho postupov a návrhov, ktoré sú rozdielne od algoritmov dodávaných a zapracovaných do aplikačného softvéru, ktoré sa chápu ako štandardné.
- Špecifické analytické a programátorské práce, ktoré priamo nezasahujú do jednotlivých aplikácií, ale súvisia s prácou s nimi (napr. návrh a programovanie konverzného programu a pod.).

Rozsah 300 ČH/rok

Časť 4. Hot-line podpora

- Telefonická podpora v pracovné dni v čase od 8:00 do 16:00.

- Podpora formou vzdialenej správy.

Rozsah: 150 ČH/rok

Časť 5. Riadenie projektu

- Príprava a koordinácia aktivít súvisiacich s plnením špecifických požiadaviek.
- Príprava a koordinácia aktivít súvisiacich s integráciou aplikačného softvéru na okolité systémy.
- Príprava a koordinácia metodických dní a školení pre zákazníka.
- Aktualizácia dokumentácie súvisiacej s informačnými systémami, ktoré sú predmetom zákazky

Zmluvný rozsah 40 ČH/rok

Časť 6. Technická podpora

- Profylaktika
- Technická podpora v oblastiach databáza a dáta, operačný systém a systémové prostriedky, licenčný a aplikačný softvér, hardvérové vybavenie a sieť (špecifikácia IKT infraštruktúry objednávateľa tvorí prílohu č. 2 tejto zmluvy).
- Udržiavanie testovacej databázy.

Zmluvný rozsah 8 ČD/rok

Časť 7. - Metodická podpora

- Osobné konzultácie pracovníka poskytovateľa so zamestnancami objednávateľa za účelom riešenia konkrétnych otázok súvisiacich s využívaním informačného systému podľa bodu II. 1 tejto zmluvy.

Zmluvný rozsah 12 ČD/rok

Časť 8. - Školenia/metodické dni

- Odborné školenie k modulom aplikačného softvéru.
- Účasť na odborných metodických dňoch.

Zmluvný rozsah 20 osôb/rok

Časť 9. - Bezpečnostná politika

Aktualizácia dokumentu: Plán zálohy a obnovy informačných systémov samosprávy.

Zmluvný rozsah 1 x ročne

III. MIESTO, ČAS A SPÔSOB PLNENIA

1. Miestom realizácie plnenia tejto zmluvy je sídlo a prevádzka poskytovateľa, miestom odovzdania predmetu zmluvy je sídlo objednávateľa, pokiaľ sa zmluvné strany nedohodli inak.
2. Zmluva sa uzatvára na dobu určitú a to od 1.1.2023 do 31.12.2026. Servisné služby/podpora budú poskytované v rozsahoch prislúchajúcich kalendárnym rokom.
3. Podpora podľa článku II. bude realizovaná nasledovne:

3.1. Údržba licencií dodaného licenčného softvéru bude objednávateľovi poskytovaná najskôr po ich vydaní autorskou spoločnosťou a po poskytovateľom overenej a potvrdenej kompatibilite s ASW.

3.2. UPDATE – Údržbu licencií dodaného aplikačného softvéru si bude objednávateľ preberať v elektronickej forme z internetovej stránky poskytovateľa na základe poskytnutého prístupového mena a hesla.

3.3. UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru za účelom zapracovania špecifických požiadaviek objednávateľa bude realizovaný v termíne a rozsahu podľa vzájomnej dohody zmluvných strán.

3.4 Hot-line podporu zabezpečí poskytovateľ v čase od 8:00 hod. do 16:00 hod. v pracovných dňoch. V prípade, ak by poskytovateľ dočasne neposkytoval v určitých pracovných dňoch telefonickú podporu bude o tom objednávateľa v predstihu informovať.

3.5. Riadenie projektu, technická podpora, metodická podpora a školenia/metodické dni budú realizované v termíne a v rozsahoch podľa vzájomnej dohody zmluvných strán.

4. Odovzdanie a prevzatie realizovaných činnosti potvrdia obe zmluvné strany podpisom preberacieho a odovzdávacieho protokolu (ďalej len „preberací protokol").

5. Poskytovateľ môže realizovať v ASW zmeny, ktoré zvyšujú úroveň a možnosti použitia ASW a zmeny v dôsledku vývoja operačných systémov, programovacích prostriedkov, technológií a technických zariadení. Poskytovateľ bude o zmenách a požiadavkách z nich vyplývajúcich informovať objednávateľa.

6. Služby nezrealizovaná v aktuálnom roku budú zrealizované v nasledujúcom období, teda objednávateľovi nezaniká právo na ich dodanie dňom ukončenia príslušného kalendárneho roku a poskytovateľovi povinnosť ich dodať, a to aj po skončení príslušného obdobia, avšak najneskôr do doby trvania tejto zmluvy.

IV. ZMLUVNÁ CENA PREDMETU DIELA

Cena za poskytovanie predmetu zmluvy je stanovená dohodou zmluvných strán, v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov, vyhláškou MF SR č. 87/1996 Z. z., ktorou sa vykonáva zákon NR SR č. 18/1996 Z. z. o cenách v znení neskorších predpisov, cena jednotlivých poskytovaných služieb tvorí prílohu č. 1 tejto zmluvy. Takto dohodnutá cena je pre poskytovateľa nemenná a záväzná.

1. Cena predmetu plnenia na obdobie trvania zmluvy:

Cena spolu bez DPH:	**583 097,44 EUR**
DPH:	**116 619,49 EUR**
Cena spolu vrátane DPH:	**699 716,93 EUR**

2. Ceny poskytovaných služieb na kalendárny rok tvoria prílohu č.1 tejto zmluvy. Zmluvné strany môžu po 12 mesiacoch poskytovania služby písomným dodatkom k tejto zmluve v súlade s § 18 ods. 1 písm. a) Zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov upraviť raz ročne (do 28.2.) ceny poskytovaných služieb o násobok koeficientu (miery) inflácie meranej indexom spotrebiteľských cien za predchádzajúci kalendárny rok, vyhlásený Štatistickým úradom Slovenskej republiky. Ceny produktov a služieb navýšené o koeficient (mieru) inflácie budú zaokrúhlené na dve desatinné miesta.

2.1. V prípade zmeny sadzby DPH bude k cene služieb pripočítaná DPH vo výške platnej ku dňu zdaniteľného plnenia.

V. PLATOBNÉ PODMIENKY

1. Cena za predmet zmluvy bude poskytovateľovi uhradená na základe faktúr, ktoré poskytovateľ doručí objednávateľovi. Faktúry musia byť vystavené v zmysle platných právnych predpisov.

2. Platby za jednotlivé položky predmetu zmluvy budú realizované nasledovne:

2.1 Faktúra za predmet uvedený v časti 1. /údržba licencií dodaného licenčného softvéru/ bude vystavená vždy v I. štvrťroku prebiehajúceho roka. V prípade, že objednávateľ nebude mať záujem o obnovenie podpory, môže požiadať o jej zastavenie minimálne 3 mesiace pred uplynutím platnosti podpory.

2.2. Faktúra za predmet zmluvy uvedený v častiach 2 až 9 bude vystavená k 28.2.,30.4.,31.7. a 31.10. príslušného kalendárneho roka a to vo výške 1/4 ročnej ceny jednotlivých položiek príslušného roka.

3. Lehota splatnosti faktúr je 14 dní od jej vystavenia poskytovateľom.

4. Objednávateľ má právo vrátiť nesprávnu alebo neúplnú faktúru do 30 dní od jej doručenia, pričom vrátenie má odkladný účinok na jej splatnosť a nová splatnosť začína plynúť nasledujúcim dňom po dni, kedy bola opravená faktúra doručená objednávateľovi. Dĺžka splatnosti týmto nie je dotknutá.

5. Podpisom tejto zmluvy objednávateľ v zmysle zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov zároveň udeľuje poskytovateľovi súhlas na to, aby mu poskytovateľ vyúčtovával odmenu a iný nárok poskytovateľa Elektronickou faktúrou a poskytovateľ nadobúda oprávnenie vystavovať a zasielať objednávateľovi Elektronickú faktúru ako vyúčtovanie za plnenia poskytnuté objednávateľovi poskytovateľom na základe tejto zmluvy.

6. Doručovanie elektronickej faktúry:

6.1. Poskytovateľ sa zaväzuje doručovať Elektronickú faktúru objednávateľovi formou elektronickej pošty, a to na emailovú adresu Objednávateľa podatelna@msupoprad.sk (ďalej len „emailová adresa") ako dokument PDF (s príponou *.pdf). Prílohy k faktúram a oznamy môžu byť vystavené vo formáte súborov pdf, doc, docx, xls, xlsx, tif alebo jpg. Na zabezpečenie vierohodnosti a neporušenosti údajov elektronických dokumentov nie je oprávnená žiadna zmluvná strana zasahovať ani meniť obsah už odoslaných dokumentov. Objednávateľ vyhlasuje, že má prístup k uvedenej e-mailovej adrese.

6.2. Elektronická faktúra sa považuje za doručenú v deň nasledujúci po dni jej preukázateľného odoslania objednávateľovi poskytovateľom prostredníctvom elektronickej pošty na e-mailovú adresu.

VI. REALIZÁCIA – PODMIENKY VYKONANIA DIELA

1. Na splnenie predmetu plnenia v čase plnenia je nutná spolupráca objednávateľa s poskytovateľom. V prípade, že objednávateľ neposkytne primeranú súčinnosť poskytovateľovi, poskytovateľ nie je v omeškaní s plnením tejto zmluvy a nenesie zodpovednosť za prípadne škody ktoré môžu v tejto súvislosti vzniknúť. Za účelom predchádzaniu daným skutočnostiam, zmluvné stany stanovili podmienky pre vzájomnú spoluprácu:

1.1. Objednávateľ určí zodpovednú a kompetentnú osobu pre styk s poskytovateľom počas plnenia predmetu zmluvy do 10 pracovných dní od podpisu tejto zmluvy.

1.2. Objednávateľ zabezpečí požadovanú informačnú a organizačnú podporu a súčinnosť do 3 pracovných dní od vzniku požiadavky poskytovateľa vrátane požadovaného technického vybavenia, ak sa zmluvné strany nedohodli inak.

1.3. Objednávateľ určí zoznam kompetentných pracovníkov – odborných garantov objednávateľa do 10 pracovných dní od podpísania tejto zmluvy. Tento zoznam sa môže operatívne meniť a dopĺňať podľa potrieb a personálnych zmien u objednávateľa.

1.4. Objednávateľ je povinný zabezpečiť minimálne technické podmienky v zmysle minimálnej technickej špecifikácie podľa prílohy č. 5 tejto zmluvy a udržať ich počas platnosti tejto zmluvy.

1.5. Poskytovateľ je povinný oznámiť objednávateľovi prípadnú zmenu minimálnej technickej špecifikácie pre nasledujúce obdobie dostatočne včas, minimálne 6 mesiacov pred požadovaným termínom jej implementácie.

2. Za poskytovateľa sú za vykonanie predmetu plnenia zodpovední nasledovní pracovníci:

2.1. Za koordináciu činností a realizáciu tejto zmluvy: Ing. Ján Valko

2.2. Za sledovanie čerpania hotline podpory: Ing. Ján Valko

2.3. Za realizáciu technickej podpory: Ing. Emil Tomáš

3. Poskytovateľ bude bez meškania písomne informovať objednávateľa o vzniku akejkoľvek udalosti, ktorá bráni alebo sťažuje realizáciu predmetu tejto zmluvy.

4. Pri plnení predmetu zmluvy sa obe zmluvné strany zaväzujú dodržiavať zásady informačnej bezpečnosti.

4.1. V prípade, ak pri poskytovaní služieb zo strany poskytovateľa bude nevyhnutné, aby poskytovateľ spracovával v mene objednávateľa ako prevádzkovateľa osobných údajov osobné údaje fyzických osôb, zaväzuje sa objednávateľ o tejto skutočnosti s dostatočným časovým predstihom poskytovateľa informovať a súčasne sa zmluvné strany zaväzujú ešte pred tým ako dôjde k spracovaniu osobných údajov zo strany poskytovateľa ako sprostredkovateľa osobných údajov uzatvoriť zmluvu o spracovaní osobných údajov a to v súlade s čl. 28 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), ďalej len „Nariadenie" alebo "GDPR". Zmluvné strany sú následne povinné zabezpečiť splnenie všetkých povinností, ktoré citované Nariadenie pre spracovanie týchto osobných údajov dotknutých osôb objednávateľa zo strany poskytovateľa ako sprostredkovateľa vyžaduje a bez splnenia týchto osobitných podmienok stanovených Nariadením nie je poskytovateľ oprávnený a ani povinný takéto osobné údaje objednávateľa spracovávať.

4.2. Napriek vyššie uvedenému pri plnení predmetu plnenia sa obe zmluvné strany vo všeobecnosti zaväzujú dodržiavať zásady informačnej bezpečnosti podľa medzinárodných štandardov. Poskytovateľ prehlasuje, že prijal technické a organizačné opatrenia na:

- kontrolu prístupu k zariadeniam, aby sa zabránilo neoprávnenému prístupu k zariadeniam na prístup k osobným údajom z informačného systému objednávateľa,
- kontrolu nosičov osobných údajov, aby sa zabránilo neoprávnenému čítaniu nosičov osobných údajov, kopírovaniu nosičov osobných údajov, pozmeňovaniu nosičov osobných údajov alebo odstráneniu nosičov osobných údajov,
- kontrolu postupov a technických zariadení, aby sa zabránilo neoprávnenému vkladaniu osobných údajov do informačného systému a neoprávnenému prehliadaniu osobných údajov, pozmeňovaniu osobných údajov v informačnom systéme alebo vymazaniu osobných údajov z informačného systému objednávateľa zo strany poskytovateľa,

- kontrolu užívateľa informačného systému poskytovateľa, aby sa zabránilo použitiu systémov automatizovaného spracúvania neoprávnenými osobami pomocou zariadenia na prenos osobných údajov,
- kontrolu prístupu k osobným údajom, aby sa zabezpečilo, že osoby oprávnené používať systém poskytovateľa budú mať prístup iba k tým osobným údajom, na ktoré sa vzťahuje ich oprávnenie na prístup,
- kontrolu prenosu údajov, aby sa zabezpečila možnosť overiť a zistiť subjekty, ktorým sa preniesli osobné údaje alebo poskytli osobné údaje, alebo overiť a zistiť subjekty, ktorým sa môžu preniesť osobné údaje, alebo poskytnúť osobné údaje prostredníctvom zariadenia na prenos osobných údajov,
- kontrolu vkladania údajov do informačného systému, aby sa zabezpečilo, že bude možné overiť a zistiť, aké osobné údaje sa vložili do systému automatizovaného spracúvania, a kedy a kto ich tam vložil,
- kontrolu prepravy osobných údajov, aby sa zabránilo neoprávnenému čítaniu osobných údajov, kopírovaniu osobných údajov, pozmeňovaniu osobných údajov alebo vymazaniu osobných údajov počas ich prenosu alebo počas prepravy nosiča osobných údajov,
- zabezpečenie spoľahlivosti informačného systému, aby sa zabezpečilo, že funkcie tohto systému fungujú a hlási sa výskyt chýb v jeho funkciách.

4.3. Zamestnanec poskytovateľa realizujúci podporu (akoukoľvek formou) u objednávateľa je povinný najmä zachovávať mlčanlivosť o osobných údajoch v súlade s ustanoveniami zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a Nariadenia, s ktorými príde do styku pri prácach na informačných systémoch objednávateľa. Tie nesmie využiť ani pre osobnú potrebu a bez súhlasu objednávateľa informačného systému ich nesmie zverejniť a nikomu poskytnúť, ani sprístupniť.

4.4. Poskytovateľ zabezpečí pre svojich zamestnancov poučenie o tom, ako zachovávať ustanovenia zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov Nariadenia a zaviaže ich povinnosťou mlčanlivosti podľa §79 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov, ktorá bude trvať aj po zániku prístupu k podpore objednávateľa alebo po zmene pozície či ukončení pracovného pomeru.

4.5. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov, pri plnení jeho úloh v súlade s výnimkami podľa §79 zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov.

4.6. Poskytovateľ prehlasuje, že všetky jemu poskytnuté osobné údaje informačného systému objednávateľa vráti objednávateľovi bezodkladne po splnení zmluvy a všetky ich kópie zlikviduje, pokiaľ nie je medzi zmluvnými stranami dohodnuté inak.

5. Pre zabezpečenie ochrany údajov objednávateľa sa zmluvné strany dohodli, že:

5.1. Prevzatie a následné odovzdanie akýchkoľvek dát resp. podkladov objednávateľa zo strany poskytovateľa bude realizované po udelení súhlasu písomnou alebo emailovou formou.

5.2. Poskytovateľ je oprávnený dáta objednávateľa získané počas realizácie predmetu plnenia používať výlučne v súlade s účelom za ktorým boli poskytnuté.

5.3. Poskytovateľ nemôže poskytnúť dáta objednávateľa alebo ich časť žiadnej tretej osobe ani publikovať dáta alebo jej časť akýmkoľvek verejne dostupným spôsobom bez písomného súhlasu objednávateľa.

5.4. Poskytovateľ musí vynaložiť primerané úsilie na zabezpečenie dát objednávateľa pred stratou, znehodnotením alebo poškodením.

5.5. Zmluvné strany sa dohodli, že osobné údaje môže poskytovateľ spracúvať aj prostredníctvom subdodávateľa, ktorý ich bude spracúvať a zabezpečovať ich ochranu na zodpovednosť poskytovateľa.

6. Pre realizáciu vzdialeného prístupu poskytovateľa k informačným systémom objednávateľa sa zmluvné strany dohodli, že:

6.1. Zamestnanci poskytovateľa v spolupráci s objednávateľom zabezpečia všetky potrebné technické náležitosti tak, aby bolo možné bezpečne využívať službu vzdialenej správy u objednávateľa, ako na samotnú technickú podporu, tak i pre potreby realizácie predmetu plnenia.

6.2. Poskytovateľ zabezpečí internú evidenciu parametrov pripojenia pre vzdialenú správu v samostatnom súbore s riadeným prístupom výhradne pre pracovníkov, ktorí toto pripojenie realizujú.

6.3. Poskytovateľ zabezpečí internú evidenciu účtov pre vzdialenú správu v samostatnom súbore prístupnom výhradne pre administrátorov pripojenia a poverených zamestnancov poskytovateľa.

6.4. Na realizáciu vzdialenej správy sa v zásade vytvára jeden účet s privilégiami administrátor, ktorý je pridelený oddeleniu technickej podpory poskytovateľa a za jeho používanie a evidenciu použitia je zodpovedný vedúci oddelenia.

6.5. Pre potreby projektu je možné vytvoriť ďalšie účty (bez administrátorských privilégií) na požiadanie povereného zamestnanca poskytovateľa na základe súhlasu povereného zamestnanca objednávateľa.

6.6. Počas práce na zariadeniach objednávateľa prostredníctvom vzdialenej správy sa poskytovateľ zaväzuje dodržiavať všetky zásady ochrany údajov a zariadení objednávateľa. Pre potreby spätného dohľadania a monitorovania činností, zabezpečí poskytovateľ vytvorenie záznamov (log súborov) o použití vzdialenej správy.

6.7. Zamestnanec poskytovateľa realizujúci podporu (akoukoľvek formou) u objednávateľa je povinný najmä zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku pri prácach na informačných systémoch objednávateľa. Tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa informačného systému a zamestnávateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.

6.8. Poskytovateľ zabezpečí formou interného predpisu povinnosť mlčanlivosti jeho zamestnancov, ktorá bude trvať aj po zániku prístupu k podpore objednávateľa alebo po zmene pozície či ukončení pracovného pomeru.

6.9. Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh orgánov činných v trestnom konaní a vo vzťahu k Úradu pre ochranu osobných údajov, pri plnení jeho úloh.

7. Zmluvné strany si dohodli nasledujúce postupy pri aktualizácii existujúcich riešení v prostredí informačných systémov (ďalej IS) objednávateľa vrátane riešenia požiadaviek a chýb:

7.1. Všetky aktualizácie ASW vo forme verzií a kumulatívnych zmien (ďalej KZ) budú realizované sprístupnením príslušných aktualizačných súborov. Samotnú aktualizáciu vykoná správca IS objednávateľa alebo osoba ním poverená.

7.2. Zmeny v databáze ASW budú vykonávané zaslaním SQL dávky, ktorá tieto zmeny realizuje. Spustenie dávky bude realizovať správca IS alebo osoba ním poverená.

7.3. V mimoriadnych prípadoch je možné po vzájomnej dohode určiť pre body VI.7.1 a VI.7.2. iný postup. Tento postup musí byť presne definovaný a obmedzený na daný mimoriadny prípad.

7.4. Pre účely tejto zmluvy – odseku VI.7.3 sa mimoriadnym prípadom rozumie stav keď objednávateľ nie je schopný zabezpečiť aktualizáciu ASW a hrozí jeho nedostupnosť alebo nesprávna funkčnosť.

8. Žiadna zo zmluvných strán nesmie sprístupniť tretej osobe, alebo pre seba či iného využiť dôverné informácie, ktoré pri plnení tejto zmluvy získala od druhej zmluvnej strany. Zmluvné strany môžu sprístupniť dôverné informácie za účelom plnenia tejto zmluvy zamestnancom podieľajúcim sa na plnení podľa tejto zmluvy za rovnakých podmienok, aké sú stanovené zmluvným stranám v tomto článku, a to len v rozsahu nevyhnutnom pre riadne plnenie tejto zmluvy. Ďalej ich môžu sprístupniť tretím osobám za účelom uskutočnenia právneho, účtovného alebo daňového auditu niektorej zo zmluvných strán, ak sú tieto osoby viazané povinnosťou ochrany informácií najmenej v rozsahu, aký je stanovený v tomto článku. Dôverné informácie sú považované zmluvnými stranami za obchodné tajomstvo a obidve zmluvné strany sa ho zaväzujú takto chrániť.

8.1. Za dôverné informácie sú na základe tejto zmluvy stranami považované všetky informácie vzájomne poskytnuté v ústnej alebo v písomnej forme, najmä informácie, ktoré sa zmluvné strany dozvedeli v súvislosti s touto zmluvou, ako aj know-how, ktorým sa rozumejú všetky poznatky obchodnej, výrobnej, technickej či ekonomickej povahy súvisiace s činnosťou zmluvnej strany, ktoré majú skutočnú alebo aspoň potenciálnu hodnotu a ktoré nie sú v príslušných obchodných kruhoch bežne dostupné a majú byť utajené.

8.2. Zmluvné strany sa zaväzujú zachovávať mlčanlivosť o informáciách, o ktorých sa dozvedeli pri realizácii predmetu zmluvy. Žiadne informácie spojené s predmetom zmluvy nesmú byť použité na iné účely ako je definované v tejto zmluve a nesmú byť poskytnuté tretej osobe, a to ani po skončení právneho vzťahu založeného touto zmluvou. Zmluvné strany sú si zároveň vedomé právnych následkov porušenia tejto povinnosti.

8.3. Zmluvné strany do 10 pracovných dní od prvého stretnutia k realizácií predmetu tejto zmluvy, tzv. otvorenia projektu špecifikujú osoby oprávnené rokovať so zástupcami druhej zmluvnej strany a oboznámia ich s príslušnými článkami tejto zmluvy.

8.4. Za objednávateľa sú tieto osoby oprávnené požadovať realizáciu HotLine podpory a sú súčasne zodpovedné za čistotu a správnosť dát týkajúcich sa príslušných modulov, pre ktoré boli stanovení ako odborní garanti.

8.5. Za poskytovateľa sú tieto osoby zodpovedné za funkčnosť príslušných modulov, pre ktoré boli stanovení ako odborní garanti.

8.6. Zoznam zodpovedných osôb za obe zmluvné strany bude vedený písomne. Každá ďalšia zmena zodpovedných osôb – odborných garantov sa oznámi druhej zmluvnej strane vo forme listu, ktorý bude zaslaný do 10 pracovných dní odo dňa vykonania zmeny a podpísaný oprávnenou osobou.

8.7. V prípade porušenia tejto dohody o mlčanlivosti je strana, ktorá porušila túto dohodu o mlčanlivosti povinná nahradiť druhej strane všetku škodu, ktorá jej z toho porušenia a v príčinnej súvislosti s ním vznikne.

9. Zmluvné strany budú mať pri plnení tejto zmluvy prístup k informáciám týkajúcim sa druhej zmluvnej strany (ďalej len „dotknutá zmluvná strana“) a jej podnikania, najmä k akýmkoľvek informáciám obchodnej, výrobnej, prevádzkovej, marketingovej, finančnej, majetkovej, organizačnej, personálnej, hospodárskej a/alebo technickej povahy, vrátane analýzy a opisu činnosti modulov. Tieto informácie alebo akékoľvek iné informácie verejne neprístupné a súvisiace s činnosťou dotknutej zmluvnej strany, ktoré druhá zmluvná strana získa ústne, písomne alebo v akejkoľvek inej forme pri plnení tejto zmluvy alebo v jej súvislosti, sú predmetom obchodného tajomstva dotknutej zmluvnej strany, alebo ich dotknutá zmluvná strana týmto označuje ako

dôverné v zmysle ustanovenia § 271 Obchodného zákonníka (ďalej len „dôverné informácie").

10. Zmluvné strany budú zachovávať mlčanlivosť o dôverných informáciách, najmä sa zaväzujú s dôvernými informáciami zaobchádzať ako s prísne tajnými, tieto dôverné informácie bez výslovného predchádzajúceho písomného súhlasu dotknutej zmluvnej strany priamo alebo nepriamo tretej osobe neoznámiť, nesprístupniť, nezverejniť alebo pre seba alebo iného nevyužiť.

11. Zmluvné strany písomne oznámia dotknutej zmluvnej strane akékoľvek okolnosti, ktoré by mohli viesť k vzniku konfliktu záujmov s dotknutou zmluvou stranou.

12. Zmluvné strany použijú dôverné informácie iba v súvislosti s plnením predmetu tejto zmluvy a na dosiahnutie účelu podľa tejto zmluvy.

13. Zmluvné strany obmedzia zverenie dôverných informácií iba tým svojim zamestnancom, ktorí sú určení na plnenie predmetu tejto zmluvy a u ktorých zabezpečujú dodržiavanie dôvernosti týchto informácií a povinností s tým súvisiacich.

14. Zmluvné strany o každom sprístupnení dôverných informácií tretej strane v prípadoch stanovených všeobecne záväznými právnymi predpismi budú informovať dotknutú zmluvnú stranu.

15. Poskytovateľ je povinný dodržiavať bezpečnostné opatrenia a povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v nadväznosti na vyhlášku národného bezpečnostného úradu č. 362/2018 Z. z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Bezpečnostné opatrenia a povinnosti tvoria prílohu č. 4 tejto zmluvy.

VII. ZODPOVEDNOSŤ ZA VADY, ZÁRUKY

1. V súvislosti s chybami ASW je určená nasledovná kategorizácia chýb ASW:

1.1. Kritická chyba – chyba ktorá má vplyv na podstatné činnosti ASW, pričom ASW nie je možné používať na zabezpečenie činností a objednávateľ nemôže použiť iné moduly ASW na realizáciu činností.

1.2. Hlavná chyba – chyba ktorá neumožňuje prácu s ASW bez použitia iných metodických a technologických postupov.

1.3. Malá chyba – chyba ktorá nemá vplyv na spoľahlivosť a spôsob používania ASW v plynulej prevádzke.

2. Reklamácia chyby predmetu zmluvy bude uplatnená písomne.

2.1. Objednávateľ sa zaväzuje, že prípadnú reklamáciu chyby dodaného ASW uplatní bezodkladne po jej zistení formou helpdesk alebo emailom.

2.2. V reklamácií objednávateľ čo najpresnejšie opíše charakter reklamovanej chyby a zaradí chybu do kategórie chýb podľa bodu VII.1. Potvrdenie prijatia reklamácie zo strany poskytovateľa bude realizované podľa spôsobu jej ohlásenia.

2.3. Poskytovateľ je povinný reagovať - potvrdiť prijatie - na každú reklamáciu do 18 hodín od jej doručenia (helpdesk, email) pričom do reakčnej doby je zahrnutá iba pracovná doba od 8:00 do 16:00 hod. a počas pracovných dní. V prípade doručenia reklamácie na konci pracovného času/ pracovnej doby sa čas reakcie na reklamáciu počíta v príslušnom zostatku do pracovného času nasledujúceho pracovného dňa.

3. Poskytovateľ sa zaväzuje začať činnosti potrebné na odstránenie chyby do 24 hodín od potvrdenia jej prijatia (reakčná doba) pričom do reakčnej doby je zahrnutá iba pracovná doba od 8:00 do 16:00 hod. počas pracovných dní. Pričom prvotne zaradí reklamáciu/ chybu do kategórie chýb a dané oznámi objednávateľovi spolu s časom na jej odstránenie. Čas na odstránenie chyby začína plynúť od potvrdenia reklamácie u poskytovateľa a zaradenia chyby do kategórie chýb v zmysle ods. VII.1 tohto článku.

4. Poskytovateľ sa zaväzuje odstrániť chyby nasledovne:

4.1. chybu podľa ods.VII.1.1. do 2 pracovných dní od uplynutia reakčnej doby, ak sa strany nedohodnú inak.

4.2. chybu podľa ods. VII.1.2. do 30 dní pracovných dní od uplynutia reakčnej doby, ak sa strany nedohodnú inak.

4.3. chybu podľa ods. VII.4.3. do 30 dní pracovných dní od uplynutia reakčnej doby, ak sa strany nedohodnú inak.

5. Za odstránenie chyby sa považuje aj jej preradenie do novej kategórie chýb na základe čiastočného odstránenia chyby. Po jej preradení začína plynúť nový čas na odstránenie chyby príslušný pre novú kategóriu chyby do ktorej bola chyba preradená.

6. Poskytovateľ nezodpovedá objednávateľovi za nedostatky spôsobené konaním alebo opomenutím tretích strán, napr. výpadok el. siete, resp. chyby spôsobené v dôsledku výpadku el. siete, výpadok internetového spojenia, resp. chyby spôsobené v dôsledku výpadku internetového spojenia a pod, resp. za nedodržanie podmienok užívania informačných systémov, resp. softvéru.

VIII. DÔSLEDKY NEPLNENIA ZMLUVY, ZMLUVNÉ POKUTY

1. Zmluvné strany si pre prípad porušenia povinností vyplývajúcich z tejto zmluvy dohodli nasledovné zmluvné pokuty :

1.1. Ak poskytovateľ nedodrží ustanovenia zmluvy týkajúce sa poskytnutia služby v jednotlivých častiach predmetu zmluvy alebo odstránenia vady, zaplatí zmluvnú pokutu vo výške 0,05 % z ceny príslušnej časti predmetu zmluvy s ktorej vykonaním je v omeškaní za každý aj začatý kalendárny deň omeškania.

1.2. Ak objednávateľ nezaplatí vyfakturovanú zmluvnú cenu v lehote splatnosti, zaplatí zmluvnú pokutu vo výške 0,05 % z ceny s ktorou je v omeškaní a to za každý aj začatý kalendárnych deň omeškania.

1.3. Odhliadnuc od znenia bodu VIII.1.2 je poskytovateľ v prípade omeškania objednávateľa s úhradou jednotlivých faktúr poskytovateľa, oprávnený prerušiť poskytovanie plnenia na základe tejto zmluvy až do riadnej úhrady faktúr objednávateľom, pričom takéto prerušenie poskytovania plnenia sa nepovažuje za omeškanie na strane poskytovateľa, resp. porušenie ustanovení tejto zmluvy.

2. Lehota splatnosti faktúr, ktorými sa uplatňujú zmluvné pokuty je do 14 kalendárnych dní odo dňa ich doručenia.

3. Dojednaním zmluvnej pokuty nie je dotknutý nárok na náhradu skutočnej priamej škody, ktorá vznikla porušením zmluvnej povinnosti, na ktorú sa vzťahuje zmluvná pokuta vo výške presahujúcu zmluvnú pokutu.

4. Celkové finančné záväzky, ktoré bude Poskytovateľ znášať v súvislosti so všetkými nárokmi vznesenými v súvislosti s touto Zmluvou, nepresiahnu hodnotu skutočných priamych škôd, ktoré vzniknú Objednávateľovi.

IX. ZÁVEREČNÉ USTANOVENIA

1. Táto Zmluva patrí medzi povinne zverejňované zmluvy (vrátane jej dodatkov) v centrálnom registri zmlúv vedenom na Úrade vlády SR podľa ustanovenia § 5a zákona č. 211/2000 Z. z., o slobodnom prístupe k informáciám v znení neskorších predpisov v spojení s ustanoveniami § 1 ods. 2 Obchodného zákonníka a § 47a ods.1 zákona č. 40/1964 Zb. Občianskeho zákonníka v znení neskorších predpisov (ďalej len „Občiansky zákonník"). Zmluva nadobúda platnosť dňom jej podpísania oboma zmluvnými stranami a účinnosť dňa 1.1.2023.

2. Ostatné náležitosti neupravené touto zmluvou sa primerane riadia ustanoveniami Obchodného zákonníka a Autorského zákona.

3. Zmluva môže zaniknúť:

3.1. Dohodou zmluvných strán.

3.2. Odstúpením od zmluvy ktorejkoľvek zmluvnej strany, ak druhá strana poruší ustanovenia tejto zmluvy podstatným spôsobom. Zmluvné strany sa dohodli, že za podstatné porušenie tejto zmluvy sa považuje okrem prípadu podľa § 345 ObZ konkrétne aj porušenie záväzkov objednávateľa týkajúcich sa riadnej úhrady faktúr.

4. Neoddeliteľnou súčasťou tejto zmluvy sú prílohy:

- Príloha č. 1 - Ceny poskytovaných služieb
- Príloha č. 2 - Špecifikácia IKT infraštruktúry
- Príloha č. 3 - Zoznam modulov aplikačného softvéru a počet licencií
- Príloha č. 4 - Bezpečnostné opatrenia a povinnosti
- Príloha č. 5 - Minimálna technická špecifikácia
- Príloha č. 6 - Vyhlásenie uchádzača o subdodávateľoch

5. Táto zmluva je vyhotovená v 5 (piatich) exemplároch, z ktorých 3 (tri) obdrží objednávateľ a 2 (dva) poskytovateľ.

6. Túto zmluvu je možné meniť a dopĺňať výlučne formou písomných dodatkov podpísaných zmluvnými stranami, ak nie je v tejto zmluve výslovne upravené inak.

7. V prípade rozporu medzi ustanoveniami zmluvy a dispozitívnymi ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, platia ustanovenia zmluvy. V prípade rozporu medzi ustanoveniami zmluvy a ustanoveniami všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky, ktoré je možné dohodou zmluvných strán vylúčiť, platia ustanovenia zmluvy a uvedené ustanovenia všeobecne záväzných právnych predpisov právneho poriadku Slovenskej republiky sa považujú za výslovne vylúčené.

8. Objednávateľ nie je oprávnený bez výslovného písomného súhlasu poskytovateľa postúpiť pohľadávky voči poskytovateľovi z tejto zmluvy. Postúpenie pohľadávky v rozpore s týmto článkom sa považuje za postúpenie pohľadávky v rozpore s dohodou s dlžníkom podľa § 525 ods. 2 zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ako takéto bude neplatné.

9. Zhotoviteľ najneskôr v čase uzavretia tejto zmluvy v súlade s § 41 ods. 3 uvedie údaje o všetkých známych subdodávateľoch (Príloha č. 6), údaje o osobe konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia. Zmenu údajov akéhokoľvek aktuálneho subdodávateľa je poskytovateľ povinný bezodkladne písomne oznámiť objednávateľovi v súlade s § 41 ods. 4 ZVO (s výnimkou dodávateľa/dodávateľov tovaru podľa § 41 ods. 6 ZVO).

10. Objednávateľ nesmie v zmysle § 11 ods. 1 ZVO uzavrieť zmluvu, koncesnú zmluvu alebo rámcovú dohodu s uchádzačom alebo uchádzačmi, ktorí majú povinnosť

zapisovať sa do registra partnerov verejného sektora a nie sú zapísaní v registri partnerov verejného sektora alebo ktorých subdodávatelia alebo subdodávatelia podľa osobitného predpisu, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora a nie sú zapísaní v registri partnerov verejného sektora. Taktiež podľa § 11 ods. 1 písm. d) zákona o verejnom obstarávaní verejný obstarávateľ nesmie uzavrieť zmluvu, koncesnú zmluvu alebo rámcovú dohodu s uchádzačom, ktorého subdodávateľ a subdodávateľ podľa osobitného predpisu, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora majú v registri partnerov verejného sektora zapísaného konečného užívateľa výhod, ktorým je osoba podľa písm. c) § 11 zákona o verejnom obstarávaní.

11. Ak niektoré ustanovenia tejto zmluvy sú neplatné alebo po jej podpise stratia platnosť, nie je tým dotknutá platnosť a účinnosť ostatných ustanovení tejto zmluvy. Namiesto neplatných alebo neúčinných ustanovení tejto zmluvy alebo na úpravu právnych vzťahov, ktoré nie sú touto zmluvou upravené, sa použijú ustanovenia zákona č. 513/1991 Zb. Obchodný zákonník, ktoré sú obsahom a účelom najbližšie obsahu a účelu tejto zmluvy.

12. Zmluvné strany vyhlasujú, že ustanoveniam tejto zmluvy porozumeli, že táto zmluva bola uzavretá určite, vážne a zrozumiteľne, na základe ich vážnej a slobodnej vôle, nie v tiesni a za nápadne nevýhodných podmienok, na znak čoho ju podpisujú.

V Poprade , dňa .....

V Poprade, dňa .....

Ing. Anton Danko
primátor mesta

Ing. Jozef Habiňák
konateľ spoločnosti

PRÍLOHA Č. 1 - Ceny poskytovaných služieb

Ceny služieb na obdobie 12 mesiacov

Počet jednotiek	Jednotka	Cena za jednotku bez DPH	Cena spolu bez DPH	Cena spolu vrátane DPH
Časť 1. Údržba licencií dodaného licenčného softvéru				
1	celok	1 100,00 €	1 100,00 €	1 320,00 €
Časť 2. UPDATE – Údržba licencií dodaného aplikačného softvéru				
1	celok	87 804,36 €	87 804,36 €	105 365,23 €
Časť 3. UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru				
300	ČH	79,00 €	23 700,00 €	28 440,00 €
Časť 4. Hotline podpora				
150	ČH	75,00 €	11 250,00 €	13 500,00 €
Časť 5. Riadenie projektu				
40	ČH	92,00 €	3 680,00 €	4 416,00 €
Časť 6. Technická podpora				
8	ČD	970,00 €	7 760,00 €	9 312,00 €
Časť 7. Metodická podpora				
12	ČD	696,00 €	8 352,00 €	10 022,40 €
Časť 8. Školenia/metodické dni				
20	osôb	87,00 €	1 740,00 €	2 088,00 €
Časť 9. Bezpečnostná politika				
1	celok	388,00€	388,00 €	465,60 €

Ceny služieb na obdobie trvania zmluvy 48 mesiacov

Poskytovaná služba	Cena bez DPH	Cena vrátane DPH
Časť 1. Údržba licencií dodaného licenčného softvéru	4 400,00 €	5 280,00 €
Časť 2. UPDATE – Údržba licencií dodaného aplikačného softvéru	351 217,44 €	421 460,93 €
Časť 3. UPGRADE – Technické zhodnotenie dodaného aplikačného softvéru	94 800,00 €	113 760,00 €
Časť 4. Hotline podpora	45 000,00 €	54 000,00 €
Časť 5. Riadenie projektu	14 720,00 €	17 664,00 €
Časť 6. Technická podpora	31 040,00 €	37 248,00 €
Časť 7. Metodická podpora	33 408,00 €	40 089,60 €
Časť 8. Školenia/metodické dni	6 960,00 €	8 352,00 €
Časť 9. Bezpečnostná politika	1 552,00 €	1 862,40 €

FS (file sharing), OracleDB 11gR2 CG ISS *Virtuálny server*	Windows Server 2019 Datacenter
	Oracle RDBMS 11g R2 64-bit
	Oracle klient 11gR2 32-bit
	Runtime IS 3.2
	Runtime VFP 6.0 SP3
	MS SOAP Toolkit SDK 3.0

IIS, FS CG GISAM CG DISS CG eGOV *Virtuálny server*	Windows Server 2019 Datacenter
	Oracle klient 11gR2 32-bit
	Microsoft IIS + .NET Framework 3.5 SP1 + 4.5
	Runtime IS 3.2
	Oracle GlassFish 3.1.2
	Oracle Mapviewer ps6
	MS SOAP Toolkit SDK 3.0
	CoraCoreService, CoraCoreWebService, CommISS, Cora eDESK service

IIS, OracleDB CG WEBGIS CG eGOV *Virtuálny server*	Windows Server 2019 Datacenter
	Oracle RDBMS 11g R2 64-bit
	Oracle klient 11g R2 32-bit
	Oracle GlassFish 3.1.2 + Oracle Mapviewer 11g

FS, Oracle DB CG ISS *Virtuálny server*	Windows Server 2012 R2 Standard Edition EN x64
	Oracle RDBMS 11g R2 64-bit
	Oracle klient 11gR2 32-bit
	Runtime IS 3.2

IIS, FS CG DISS CG eGOV *Virtuálny server*	Windows Server 2012 R2 Standard Edition EN x64
	Oracle klient 11gR2 32-bit
	Microsoft IIS + .NET Framework 3.5 SP1 + 4.5
	Runtime IS 3.2
	CoraCoreService, CommISS

IIS, Oracle DB CG eGOV *Virtuálny server*	Windows Server 2012 R2 Standard Edition EN x64
	Oracle RDBMS 11g R2 64-bit
	Oracle klient 11g R2 32-bit

Príloha č. 3 – Zoznam modulov aplikačného softvéru a počet licencií

Podsystém	Predmet / Názov	Rozsah	Jednotka
BASE	Dokumenty	1	150 NU
	Domy a byty	1	150 NU
	Kataster nehnuteľností	1	150 NU
	Kataster nehnuteľností - archív importov	1	150 NU
	Obyvatelia	1	150 NU
	Podnikatelia a prevádzky	1	150 NU
	Správa údajov	1	150 NU
	Súpisné a orientačné čísla	1	150 NU
	Správa CG ISS	1	150 NU
	BASE CG_ISS	1	150 NU
	Voľby	1	150 NU
	Elektronická komunikácia	1	multilicencia
CG GISAM	Doprava	1	multilicencia
	Názvoslovie a orientácia	1	multilicencia
	Reklamné zariadenia	1	multilicencia
	Územný plán	1	multilicencia
	Zeleň	1	multilicencia
	Správa CG GISAM	1	multilicencia
	Kataster nehnuteľností (CG GISAM)	1	multilicencia
	Majetok mesta (CG GISAM)	1	multilicencia
	Reklamné zariadenia - vizualizácia	1	multilicencia
DISS	Registratúra	1	multilicencia
	Zelená pošta	1	multilicencia
	ORG_Registratúra	1	50 NU
EKON	Banka a Homebanking	1	50 NU
	BAR CODE (Čiarový kód) - čítanie v module EP Pokladňa	1	multilicencia
	Dotácie	1	50 NU
	Exekúcie	1	55 NU
	Fakturácia	1	150 NU
	Miestne dane - Daň z nehnuteľností	1	150 NU
	Miestne dane a poplatok za KO	1	50 NU
	Objednávky	1	150 NU
	Platobné poukazy	1	50 NU
	Pokladňa	1	55 NU
	Poštové poukážky	1	5 NU
	Rozpočet a prístupové práva	1	150 NU
	Sklad	1	50 NU
	Správne poplatky	1	multilicencia
	Účtovníctvo	1	55 NU
	Zmluvy	1	50 NU

	Majetok	1	55 NU
	EKONOMIKA CG_ISS	1	150 NU
	ORG_Ekonomika	1	50 NU
EVID	Trhové miesta	1	50 NU
	Porovnanie MM,DN a KN dát v CG ISS s dátami katastra	1	multilicencia
	Import grafických údajov katastra do databázy	1	multilicencia
ISS	ORG_Správa prístupov	1	50 NU
KANC	Mestské zastupiteľstvo	1	5 NU
PaM	Integrácia Personalistika a mzdy - Dochádzkový systém	1	multilicencia
	Personalistika a mzdy	1	50 NU
	Dôvera - kontroly a export	1	multilicencia
	MZDY CG_ISS	1	50 NU
WEB	CG eGOVernment - Všeobecná zóna	1	multilicencia
	CG eGOVernment - Privátna zóna	1	multilicencia
	CG Portál ISS (Ročná podpora)	1	multilicencia
	CG eGOVernment - eFORMs	1	multilicencia
	GDPR - Evidencia výskytu a prístupu	1	multilicencia
	CG WebGIS	1	150 NU
MZDY	ORG_Personalistika a mzdy	1	50 NU
MsP_Park	Mestská polícia	1	50 NU
	Priestupky	1	5 NU
	MsP_Park CG_ISS	1	50 NU
	Integrácia s EVO - evidencia vozidiel	1	multilicencia
	CG MAMP - Mobilná aplikácia Mestskej polície	1	multilicencia
eMesto	Document management system (DMS)	1	multilicencia
	FormFiller	1	multilicencia
	Workflow manažment (WFM)	1	multilicencia
	Riadenie podaní	1	multilicencia
	Integračný modul na eDesk	1	multilicencia
	Integračný modul na IAM	1	multilicencia
	Zaručená konverzia	1	multilicencia
	Listinný rovnopis	1	multilicencia
	UET,CUET zverejňovanie	1	multilicencia
	ORG Integračný modul na eDesk (na každú organizáciu)	13	multilicencia

Príloha č. 4 – Bezpečnostné opatrenia a povinnosti

Bezpečnostné opatrenia a iné povinnosti vyplývajúce zmluvným stranám zo zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „Zákon") v nadväznosti na vyhlášku národného bezpečnostného úradu č. 362/2018 Z. z. z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „Vyhláška").

Pojmy aplikované v tejto Prílohe sú pojmami tak ako sú definované v § 3 na účely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

1. Povinnosť poskytovateľa dodržiavať bezpečnostnú politiku objednávateľa ako prevádzkovateľa základnej služby a povinnosť poskytovateľa dodržiavať a prijať bezpečnostné opatrenia.

1.1. Poskytovateľ sa zaväzuje dodržiavať platné bezpečnostné politiky objednávateľa ako prevádzkovateľa základnej služby, ktoré sú normatívne upravené v dokumentoch objednávateľa ako prevádzkovateľa základnej služby a to od momentu kedy bude s nimi poskytovateľ riadne oboznámený. Riadnym oboznámením sa s obsahom bezpečnostných politík podľa predchádzajúcej vety sa rozumie protokolárne odovzdanie dokumentov, ktoré má poskytovateľ dodržiavať, nie však skôr ako dňom účinnosti tejto zmluvy.

1.2. Poskytovateľ vyhlasuje, že sa s bezpečnostnou politikou objednávateľa ako prevádzkovateľa základnej služby oboznámil a vyjadruje súhlas s bezpečnostnou politikou prevádzkovateľa základnej služby.

1.3. Poskytovateľ sa zaväzuje dodržiavať a prijať bezpečnostné opatrenia vo vzťahu k dodaným Informačným systémom definovaných v článku II. tejto Zmluvy, vo vzťahu ku ktorým poskytovateľ poskytuje prevádzkovateľovi základnej služby Ročnú podporu v súlade s ustanoveniami tejto zmluvy a súčasne výlučne vo vzťahu k informačným systémom, ktoré sú predmetom tejto zmluvy prostredníctvom, ktorých poskytovateľ poskytuje objednávateľovi ako prevádzkovateľovi základnej služby Ročnú podporu pre Informačné systémy definovaných v článku II. a to pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) Zákona. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

1.4. Zmluvné strany sa dohodli, že objednávateľ ako prevádzkovateľ základnej služby prehlasuje, že s výnimkou dodanej služby Ročnej podpory v termínoch stanovených prevádzkovateľom základnej služby Informačné systémy definované v článku II. prevádzkuje a spravuje prevádzkovateľ základnej služby samostatne na vlastných sieťach (serveroch) bez toho, aby k nim mal poskytovateľ osobitný prístup. Pre vylúčenie pochybností sa ustanovenia tejto Prílohy č. 4 a tejto zmluvy vzťahujú len po dobu (v čase) realizácie služby Ročná podpora prostredníctvom vzdialenej správy zo strany poskytovateľa a vo vzťahu k samotnej funkčnosti dodaných Informačných systémov.

2. Špecifikácia a rozsah bezpečnostných opatrení, ktoré prijíma poskytovateľ a vyjadrenie súhlasu s nimi.

2.1. Bezpečnostné opatrenia pre oblasť riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s Poskytovateľom ako treťou stranou:

Poskytovateľ identifikuje technické zraniteľností informačných systémov a zariadení vo vzťahu k poskytovanej Ročnej podpore najmä identifikuje technické zraniteľnosti informačných systémov, ktoré využíva pri poskytovaní služieb Objednávateľovi ako prevádzkovateľovi základnej služby prostredníctvom nasledujúcich opatrení, ak sú relevantné:

a) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
b) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
c) využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

2.2. Bezpečnostné opatrenia pre oblasť riadenia bezpečnosti sietí a informačných systémov vo vzťahu k poskytovanej Ročnej podpore:

Poskytovateľ realizuje nasledovné opatrenia, ak sú relevantné:

a) Riadenie bezpečného prístupu medzi informačnými systémami prevádzkovateľa základnej služby, a to najmä využitím nástrojov na ochranu informačných systémov, ktoré sú zabezpečené segmentáciou informačných systémov.
b) Povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií.
c) Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov.
d) Spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov.
e) Servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu.
f) Udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave.
g) Neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty.
h) Vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete.

2.3. Bezpečnostné opatrenia pre oblasť ochrany proti škodlivému kódu a pre oblasť riadenia prístupov vo vzťahu k poskytovanej Ročnej podpore realizuje poskytovateľ nasledovné opatrenia:

a) Riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci Informačných systémov, ktoré sú nevyhnutné na plnenie zverených úloh používateľa.
b) Riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.
c) Riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej (i) vypracovanie zásad riadenia prístupu k informáciám; (ii) riadenia prístupu používateľov; (iii) zodpovednosti používateľov; (iv) riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; (v) prístupu k aplikáciám; (vi) monitorovania prístupu a používania informačného systému a (vii) riadenia vzdialeného prístupu.
d) Pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému.
e) Zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov.
f) Výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch.
g) Určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových

záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

2.4. Bezpečnostné opatrenia pre oblasť akvizície, vývoja a údržby informačných sietí a informačných systémov a pre oblasť riešenia kybernetických bezpečnostných incidentov vo vzťahu k zabezpečeniu služieb Ročnej podpory a počas povoleného času prístupu do siete objednávateľa ako prevádzkovateľa základnej služby realizuje poskytovateľ nasledovné opatrenia: Poskytovateľ najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať priamy dopad na výkon činnosti pre objednávateľa ako prevádzkovateľa základnej služby, ak sú relevantné:

a) Oboznámenie sa s postupmi prevádzkovateľa základnej služby pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči prevádzkovateľovi základnej služby.

2.5. Bezpečnostné opatrenia pre oblasť zaznamenávania udalostí a monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje poskytovateľ: opatrenia podľa § 15 Vyhlášky najmä implementuje centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú využívané pri poskytovaní služieb objednávateľa ako prevádzkovateľa základnej služby.

2.6. Špecifikácia a rozsah bezpečnostných opatrení vymedzených v tomto článku Prílohy č. 4 je dohodnutý zmluvnými stranami len rámcovo. Zmluvné strany sa zaväzujú dodatočne doplniť konkrétne bezpečnostné opatrenia, ktoré bude musieť tá-ktorá Zmluvná strana plniť, podľa záverov, ktorý vyplynú z Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2 k tejto Prílohe č. 4/, v ktorej budú popri rizikách identifikovaný aj príslušný vlastníci rizík, a teda subjekty povinné na plnenie konkrétnych bezpečnostných opatrení.

2.7. Zmluvné strany si prostredníctvom technických zástupcov dohodnú a potvrdia presné technické špecifikácie, ktoré budú vyplývať z interných bezpečnostných opatrení objednávateľa ako prevádzkovateľa základnej infraštruktúry a to na základe zrealizovanej Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2 k tejto Prílohe č. 4/ Servisnej zmluve. Do predloženia Analýzy rizík zo strany prevádzkovateľa základnej služby, ktorá je uvedená v Doložke č. 2 k tejto Prílohe č. 4/ Servisnej zmluve nie je poskytovateľ v omeškaní s plnením opatrení špecifikovaných v tomto článku. Bezpečnostné opatrenia v súlade s týmto článkom prijíma samotný poskytovateľ v primeranom rozsahu podľa vlastného rozhodnutia, tak aby bol naplnený účel zákona č. 69/2018 Z.z.. Objednávateľ ako prevádzkovateľ základnej služby do bezpečnostných opatrení poskytovateľa nijako nezasahuje.

2.8. Objednávateľ ako prevádzkovateľ základnej služby berie na vedomie, že aplikácia bezpečnostných opatrení bude aplikovaná len na Informačné systémy definované v článku II. a na tie časti siete, na ktoré má poskytovateľ reálny dosah.

3. Rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu objednávateľom ako prevádzkovateľom základnej služby u poskytovateľa.

3.1. Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonávať kontrolnú činnosť a audit u poskytovateľa, a to v rozsahu a za účelom kontroly plnenia povinnosti poskytovateľa v zmysle Zákona a tejto zmluvy.

3.2. Objednávateľ ako prevádzkovateľ základnej služby je oprávnený vykonať kontrolnú činnosť a/alebo audit u poskytovateľa prostredníctvom poverenej osoby, ktorej identifikačné údaje je objednávateľ ako prevádzkovateľ základnej služby povinný poskytovateľovi vopred oznámiť (ďalej len „Poverená osoba“). Poverená osoba sa v čase realizácie kontrolnej činnosti a/alebo auditu u poskytovateľa musí preukázať

písomným poverením vystaveným objednávateľom ako prevádzkovateľom základnej služby na jeho vykonanie. Zmluvné strany sa dohodli, že náklady na realizáciu kontrolnej činnosti a/alebo auditu u poskytovateľa tak na strane objednávateľa ako prevádzkovateľa základnej služby ako aj na strane poskytovateľa znáša v celom rozsahu objednávateľ ako prevádzkovateľ základnej služby.

3.3. Prevádzkovateľ základnej služby je oprávnený vykonať audit prijatých bezpečnostných opatrení a kontrolu pravidelne raz za kalendárny rok; v prípade preukázaného podozrenia z porušenia tejto Zmluvy alebo zákona; v prípade nedodržania bezpečnostných opatrení a v prípade žiadosti dozorného orgánu podľa zákona.

3.4. Prevádzkovateľ základnej služby informuje o termíne vykonania auditu alebo kontroly poskytovateľa oznámením zaslaným emailom uvedeným v záhlaví tejto Zmluvy, a to minimálne 7 pracovných dní pred vykonaním auditu alebo kontroly. Poskytovateľ je povinný bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 pracovných dní odo dňa zaslania oznámenia. Pokiaľ poskytovateľ termín auditu alebo kontroly nepotvrdí, má sa za to, že s termínom súhlasí.

3.5. Prevádzkovateľ základnej služby je oprávnený vykonávať audit u poskytovateľa nasledovne, pričom zmluvné strany majú pri výkone kontrolných činností a auditu nasledovné práva a povinnosti:

a) Prevádzkovateľ základnej služby je oprávnený vykonať u poskytovateľa audit zameraný na overenie plnenia povinností poskytovateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia poskytovateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u poskytovateľa pre plnenie cieľov tejto Zmluvy.
b) Prípadné nedostatky zistené auditom je poskytovateľ povinný odstrániť bez zbytočného odkladu.
c) Prevádzkovateľ základnej služby môže audit u poskytovateľa realizovať sám alebo prostredníctvom tretej osoby; v prípade ak objednávateľ realizuje audit prostredníctvom tretej osoby, tak je táto tretia osoba pred začatím realizácie auditu povinná uzatvoriť s poskytovateľom dohodu o mlčanlivosti tzv. NDA, následne práva a povinnosti objednávateľa ako prevádzkovateľa základnej služby pri výkone auditu realizuje objednávateľom ako prevádzkovateľom základnej služby poverená tretia osoba.
d) Poskytovateľ je povinný pri audite spolupracovať s objednávateľom ako prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy vo vzťahu k Informačným systémom definovaných v článku II. a výkonu Ročnej podpory. Objednávateľ ako prevádzkovateľ základnej služby je povinný minimálne 7 pracovných dní pred samotným auditom zaslať poskytovateľovi predmet auditu s menovitým zoznamom tém a oblastí, ktorých sa audit bude týkať.
e) Objednávateľ ako prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom poskytovateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy za prítomnosti osoby poverenej poskytovateľom, na ktorú sa sťahuje bod c) tohto článku.
f) V rámci auditu je poskytovateľ povinný preukázať objednávateľovi ako prevádzkovateľovi základnej služby súlad jeho postupov s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, záväzok a poučenie svojich zamestnancov, o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.

g) Ak poskytovateľ, napriek splneniu podmienky podľa pís. c) a d) tohto článku objednávateľom ako prevádzkovateľom základnej služby, neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, to neplatí ak možnosť realizácie auditu oznámil poskytovateľ objednávateľovi ako prevádzkovateľovi základnej služby v náhradnom termíne a tento termín prevádzkovateľ základnej služby odmietol akceptovať.

h) Prevádzkovateľ základnej služby, resp. ním poverená tretia osoba je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

i) Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov poskytovateľa v rámci výkonu auditu musia dodržiavať pokyny poskytovateľa týkajúce sa uvedených priestorov na úseku BOZP a ochrany pred požiarmi na účely predchádzania vzniku požiarov a zabezpečenia podmienok na účinné zdolávanie požiarov (ďalej len „PO"), s ktorými boli oboznámení podľa tretej vety tohto odseku, pričom zodpovednosť za to, že tieto osoby budú dodržiavať uvedené pokyny, nesie prevádzkovateľ základnej služby. Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov poskytovateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne poskytovateľ. Poskytovateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch poskytovateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal poskytovateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru, záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory poskytovateľa.

3.6. Poskytovateľ je povinný poskytnúť všetky informácie a potrebnú súčinnosť prevádzkovateľovi základnej služby na účely kontroly a auditu v zmysle ust. § 28 a 29 zákona.

3.7. Poskytovateľ je povinný v lehote určenej prevádzkovateľom základnej služby, nie však skôr ako v lehote 90 dní odo dňa ich oznámenia prijať opatrenia na nápravu nedostatkov zistených auditom u prevádzkovateľa základnej služby a poskytnúť potrebnú súčinnosť prevádzkovateľovi základnej služby na ich odstránenie.

4. Vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre objednávateľa ako prevádzkovateľa základnej služby namiesto poskytovateľa

4.1. Poskytovateľ je povinný dodržiavať podmienky zapojenia nového dodávateľa do poskytovania služieb tak, ako sú upravené v tejto zmluve

4.2. Poskytovateľ je povinný vopred informovať objednávateľa ako prevádzkovateľa základnej služby o zapojení nového dodávateľa, a to zaslaním žiadosti o zapojenie nového dodávateľa prostredníctvom emailu na kontakt uvedeného v tejto zmluve.

4.3. Poskytovateľ nesmie poveriť výkonom akýchkoľvek činností majúcich dopad na poskytovanie služieb objednávateľa ako prevádzkovateľovi základnej služby nového dodávateľa bez predchádzajúceho výslovného písomného súhlasu objednávateľa ako prevádzkovateľa základnej služby.

4.4. Ak poskytovateľ zapojí do vykonávania činností spojených s poskytovaním služieb objednávateľovi ako prevádzkovateľovi základnej služby nového dodávateľa, tomuto novému dodávateľovi je povinný uložiť rovnaké povinnosti týkajúce sa aplikácie bezpečnostných opatrení, ako sú ustanovené v tejto zmluve. Zodpovednosť voči objednávateľovi ako prevádzkovateľovi základnej služby nesie poskytovateľ, ak nový

dodávateľ nesplní svoje povinnosti týkajúce sa aplikácie bezpečnostných opatrení, alebo hlásenia bezpečnostných incidentov.

5. Povinnosti poskytovateľa informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti

5.1. Objednávateľ ako prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu poskytovateľa o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie tejto Zmluvy stalo nemožným, ak Národný bezpečnostný úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

5.2. Poskytovateľ je povinný bezodkladne riešiť kybernetický bezpečnostný incident týkajúci sa predmetu tejto zmluvy a v zmysle Zákona a informovať objednávateľa ako prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečenie kybernetickej bezpečnosti.

5.3. V prípade, ak počas vykonávania Ročnej podpory poskytovateľ zaznamená kybernetický bezpečnostný incident je povinný bezodkladne informovať objednávateľa ako prevádzkovateľa základnej služby podľa bodu 5.2 tohto článku tejto Prílohy č. 4 hlásením kybernetického bezpečnostného incidentu prostredníctvom zaslania hlásenia na e-mailovú adresu uvedenú v tejto zmluve v rozsahu nasledovných informácií:

a) informácie o tom, kto hlási kybernetický bezpečnostný incident:
- identifikačné údaje dodávateľa,
- funkcia a pracovné zaradenie osoby dodávateľa, ktorá hlási kybernetický bezpečnostný incident,
- identifikačné údaje ďalších organizácií dotknutých kybernetickým bezpečnostným incidentom,

b) informácie o kybernetickom bezpečnostnom incidente v rozsahu potrebnom na jeho riadnu identifikáciu, ak sú dostupné a známe:
- kategória kybernetického bezpečnostného incidentu (bezpečnostný incident I. stupňa, bezpečnostný incident II. stupňa, bezpečnostný incident III. stupňa),
- typ závažného kybernetického bezpečnostného incidentu
  - nežiaduci obsah (Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd),
  - škodlivý kód (vírus, malvér, ransomvér),
  - získavanie informácií (skenovanie site, odpočúvanie, sociálne inžinierstvo),
  - pokus o prienik do systému,
  - podozrenie na úspešný prienik do systému vrátane APT,
  - nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby),
  - neoprávnený prístup k informáciám, únik informácií, poškodenie informácií,
  - podvod (neautorizované využitie prostriedkov, porušenia autorských práv),
  - zraniteľnosť (ich existencia),
  - iné,
- časové údaje zistenia a vzniku závažného kybernetického bezpečnostného incidentu
  - čas začiatku incidentu (ak je známy), čas a spôsob zistenia incidentu, informácia, či ide o prebiehajúci kybernetický bezpečnostný incident,
- detailný opis priebehu závažného kybernetického bezpečnostného incidentu a jeho prvotná príčina,
- popis rozsahu škôd,
- odhad závažnosti dopadu závažného kybernetického bezpečnostného incidentu na užívateľov základnej služby,

c) informácie o službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
- prvotne zasiahnuté aktíva (Host/IP, vrátane identifikácie informačného systému a prevádzkových parametrov služby),
- informácia, či ide o kritické aktíva z pohľadu zabezpečenia kontinuity služby alebo činnosti, a či je zariadenie v čase podávania hlásenia v prevádzke,

d) informácie o riešení závažného kybernetického bezpečnostného incidentu:
- stav riešenia závažného kybernetického bezpečnostného incidentu,
- informácia o vykonaní nápravných opatrení smerujúcich k riešeniu hláseného závažného kybernetického bezpečnostného incidentu,
- opatrenia na zamedzenie opakovania závažného kybernetického bezpečnostného incidentu,
- popis možných negatívnych dopadov, opatrení a možných dôsledkov závažného kybernetického bezpečnostného incidentu,
- výsledok opatrení,
- dátum a čas realizácie opatrení.

5.4. Poskytovateľ je povinný na vyžiadanie nahlásiť objednávateľovi ako prevádzkovateľovi základnej služby ďalšie informácie požadované objednávateľom na plnenie jeho povinnosti vyplývajúcich zo Zákona, najmä je povinný poskytnúť objednávateľovi ako prevádzkovateľovi základnej služby:

a) informácie dôležité a potrebné pri riešení hláseného kybernetického bezpečnostného incidentu požadované prevádzkovateľom základnej služby alebo Národným bezpečnostným úradom a ústredným orgánom od prevádzkovateľa základnej služby za účelom splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods. 6 písm. c) Zákona,
b) informácie dôležité pre zabezpečenie dôkazu ako dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
c) informácie potrebné na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 19 ods.6 písm. e) Zákona oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie,
d) informácie v potrebnom rozsahu na účely splnenia povinnosti prevádzkovateľa základnej služby v zmysle ust. § 27 ods.10 Zákona.

5.5. Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa vykonanie reaktívneho opatrenia a poskytovateľ je povinný vykonať reaktívne opatrenie v prípadoch, kedy bola objednávateľovi ako prevádzkovateľovi základnej služby uložená povinnosť vykonať reaktívne opatrenie Národným bezpečnostným úradom v zmysle Zákona vo vzťahu k prevádzkovaniu Informačných systémov definovaných v článku II. a vo vzťahu informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy.

5.6. Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok a poskytnúť prevádzkovateľovi základnej služby všetku potrebnú súčinnosť pri splnení povinnosti objednávateľa ako prevádzkovateľa základnej služby oznámiť a preukázať vykonanie reaktívneho opatrenia a ich výsledok pred Národným bezpečnostným úradom vo vzťahu k prevádzkovaniu Informačných systémov CG dodaných zo strany dodávateľa a vo vzťahu informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy.

5.7. Objednávateľ ako prevádzkovateľ základnej služby je oprávnený požadovať od poskytovateľa návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu, a to najmä v prípadoch, kedy Národný bezpečnostný úrad požaduje od prevádzkovateľa základnej služby návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu vo vzťahu k prevádzkovaniu Informačných systémov a vo vzťahu k informačným systémom dodávateľa prostredníctvom, ktorých dodávateľ poskytuje prevádzkovateľovi základnej služby Podporu pre Informačné systémy (ďalej aj len „ochranné opatrenie"). Ochranné opatrenie sú prijímané na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

5.8. Poskytovateľ je povinný bezodkladne objednávateľovi ako prevádzkovateľovi základnej služby predložiť navrhované ochranné opatrenie na schválenie.

5.9. V prípade, ak poskytovateľ nenavrhne ochranné opatrenie v lehote určenej objednávateľom ako prevádzkovateľom základnej služby alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je poskytovateľ povinný poskytnúť všetku potrebné súčinnosť objednávateľovi, ktorý je povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

5.10. Bez ohľadu na ustanovenia Prílohy č. 4 , povinnosti poskytovateľa majú len podporný charakter, táto zmluva/ Príloha nezbavuje objednávateľa ako prevádzkovateľ základnej služby plniť povinnosti v zmysle Zákona, okrem iného § 19 ods. 6 a § 24 Zákona.

6. Ostatné dojednania súvisiace s povinnosťami zmluvných strán vyplývajúcich zo Zákona a Vyhlášky

6.1. Zmluvné strany sa dohodli, že hlásenia ďalších informácií požadovaných objednávateľom ako prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo Zákona sa uskutoční hlásením na e-mailové adresy uvedené v tejto zmluve.

6.2. Zmluvné strany sa dohodli, že hlásenia všetkých/akýchkoľvek informácií majúcich vplyv na túto zmluvu sa uskutoční hlásením na e-mailové adresy uvedené v tejto zmluve.

6.3. Poskytovateľ sa zaväzuje, že po ukončení zmluvného vzťahu vráti, prevedie alebo zničí všetky informácie, ku ktorým mal prístup počas trvania zmluvného vzťahu s Objednávateľom ako prevádzkovateľovi základnej služby.

6.4. Poskytovateľ prehlasuje, že Zákonom ustanovenú povinnosť po ukončení tejto zmluvy udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné práva na používanie softvéru licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby špecifikovanú v tejto zmluve na objednávateľa ako prevádzkovateľa základnej služby bola splnená a to samotným dodaním Informačných systémov CG.

6.5. Poskytovateľ prehlasuje, že sa zaväzuje chrániť všetky informácie poskytnuté Objednávateľom ako prevádzkovateľom základnej služby.

Systémové požiadavky pre klienta aplikácie CG ISS

V prípade použitia základného klienta CG ISS na terminálovom serveri Microsoft je možné použiť ako terminálový server serverový operačný systém Windows Server 2008, 2008 R2, 2012, 2012 R2 v edíciách Standard, Datacenter, prípadne Enterprise pre 2008 a 2008 R2. Pri použití iného typu terminálového servera, nás pre potvrdenie funkčnosti kontaktujte.

Hardvér, softvér	Klient CG ISS minimálna konfigurácia	Klient CG ISS odporúčaná konfigurácia
procesor	2,0 GHz a vyšší	2,8 GHz a vyšší
RAM	1 GB pre Windows 7	2 GB pre Windows 7
HDD	40 GB viac	80 GB a viac
LAN	100 Mbit	1 Gbit
VGA	min. 64 MB VRAM	min. 128 MB VRAM
monitor	17" LCD alebo CRT rozlíšenie 1024 x 768	19" LCD rozlíšenie 1024 x 768 alebo 1920 x1080
*Platforma	Windows 7 Professional Windows 8 Pro, Windows 8.1 Pro Windows 10 Pro	Windows 7 Professional SP1 (x64)
**Internetový prehliadač	MS Internet Explorer 9.x alebo vyšší	MS Internet Explorer 11.x
Software	Oracle klient 11gR2 32-bit Runtime IS 3.2	Oracle klient 11gR2 32-bit Runtime IS 3.2
Software pre prepojenie na CG GISAM	MS SOAP Toolkit 3.0 SDK	MS SOAP Toolkit 3.0 SDK
Software pre prepojenie na REGOB	MS SOAP Toolkit 3.0 SDK Microsoft .NET Framework 3.5 SP1	MS SOAP Toolkit 3.0 SDK Microsoft .NET Framework 3.5 SP1
Software pre prepojenie na eDOC	Microsoft .NET Framework 3.5 SP1	Microsoft .NET Framework 3.5 SP1
Software pre elektronické formuláre	CG Infopath viewer 2.0 alebo MS Office Infopath 2007/2010/2013	CG Infopath viewer 2.0 alebo MS Office Infopath 2007/2010/2013
**Kancelársky softvér	MS Office 2007, 2010, 2013	MS Office 2007, 2010, 2013
Iný software	Microsoft .NET Framework 3.5 SP1 Acrobat Reader 7.x alebo noší MS XML 4.0, 6.0	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.5 SP1 Acrobat Reader 9.x alebo novší MS XML 4.0, 6.0

** V prípade požiadaviek na použitie 64 bitového systému, nás pre potvrdenie funkčnosti kontaktujte. Môžu byť použité aj iné edície vhodné pre firemné prostredie (Ultimate, Enterprise).*
*** V prípade požiadaviek na použitie iného softvéru (prehliadač Mozilla Firefox, Opera, Google Chrome, kancelársky softvér MS Office 2016, OpenOffice a pod.) nás pre potvrdenie funkčnosti kontaktujte.*

Systémové požiadavky pre klientov aplikácií CG Portál ISS, CG GISAM, CG DISS

V prípade použitia základného klienta CG ISS na terminálovom serveri Microsoft je možné použiť ako terminálový server serverový operačný systém Windows Server 2008, 2008 R2, 2012, 2012 R2 v edíciách Standard, Datacenter, prípadne Enterprise pre 2008 a 2008 R2.

Hardvér, softvér	Klient CG Portál ISS Klient CG GISAM Klient CG DISS minimálna konfigurácia	Klient CG Portál ISS Klient CG GISAM Klient CG DISS odporúčaná konfigurácia
procesor	2,0 GHz a vyšší	2,8 GHz a vyšší
RAM	1 GB	2 GB
HDD	40 GB viac	80 GB a viac
LAN	100 Mbit	1 Gbit
VGA	min. 128 MB VRAM	min. 128 MB VRAM
monitor	17" LCD alebo CRT rozlíšenie 1024 x 768	19" LCD rozlíšenie 1024 x 768 alebo vyššie
*Platforma	Windows 7 Professional Windows 8 Pro, Windows 8.1 Pro Windows 10 Pro	Windows 7 Professional SP1 (x64)
*Internetový prehliadač	MS Internet Explorer 9.x alebo novší alebo iný prehliadač kompatibilný pre aktuálnu verziu aplikácie	MS Internet Explorer 11.x alebo iný prehliadač kompatibilný pre aktuálnu verziu aplikácie
*Kancelársky softvér	MS Office 2007, 2010, 2013	MS Office 2007, 2010, 2013
Iný software	Acrobat Reader 7.x alebo novší	Acrobat Reader 9.x alebo novší

* V prípade požiadaviek na použitie 64 bitového systému, nás pre potvrdenie funkčnosti kontaktujte. Môžu byť použité aj iné edície vhodné pre firemné prostredie (Ultimate, Enterprise).
** V prípade požiadaviek na použitie iného softvéru (prehliadač Mozilla Firefox, Opera, Google Chrome, kancelársky softvér MS Office 2016, OpenOffice a pod.) nás pre potvrdenie funkčnosti kontaktujte.

Hardvér, softvér	Klient CG DISS minimálna konfigurácia	Klient CG DISS odporúčaná konfigurácia
procesor	2,4 GHz a vyšší	2,8 GHz a vyšší
RAM	1 GB	2 GB
HDD	60 GB a viac	80 GB a viac
LAN	100 Mbit	1 Gbit
VGA	min. 128 MB VRAM	min. 128 MB VRAM
monitor	17" LCD alebo CRT rozlíšenie 1024 x 768	19" LCD rozlíšenie 1024 x 768 alebo vyššie
*Platforma	Windows 7 Professional Windows 8 Pro, Windows 8.1 Pro Windows 10 Pro	Windows 7 Professional SP1 (x64)
**Internetový prehliadač	MS Internet Explorer 9.x alebo novší alebo iný prehliadač kompatibilný pre aktuálnu verziu aplikácie	MS Internet Explorer 11.x alebo iný prehliadač kompatibilný pre aktuálnu verziu aplikácie
**Kancelársky softvér	MS Office 2007, 2010, 2013	MS Office 2007, 2010, 2013
Software pre skener	Software dodaný výrobcom skenera	Software dodaný výrobcom skenera
Iný software	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.0 / 4.5 Acrobat Reader 7.x alebo novší MS XML 4.0 a vyšší	Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4.0 / 4.5 Acrobat Reader 9.x alebo novší MS XML 4.0

* V prípade požiadaviek na použitie 64 bitového systému, nás pre potvrdenie funkčnosti kontaktujte. Môžu byť použité aj iné edície vhodné pre firemné prostredie (Ultimate, Enterprise).

** V prípade požiadaviek na použitie iného softvéru (prehliadač Mozilla Firefox, Opera, Google Chrome, kancelársky softvér MS Office 2016, OpenOffice a pod.) nás pre potvrdenie funkčnosti kontaktujte.

Skener pre CG DISS	
Parameter	Hodnota
Optické rozlíšenie skenovania	4 800 dpi a viac
Rozlíšenie pri hardvérovom skenovaní	800 x 4 800 DPI
Bitová hĺbka	48-bitov a viac
Skenovacie režimy	farebný, odtiene šedej, čiernobiely
Skenované formáty	A5, A4, prípadne menšie rozmery Bezokrajové
*OCR	Možnosť rozpoznávania slovenského jazyka v texte
Iné požiadavky	Prechodové snímanie, Obojstranné snímanie Podpora ukladania výstupu do PDF, JPG/PNG Možnosť ukladania preddefinovaných skenovacích profilov
Pripojiteľnosť	USB, LPT, LAN
Kapacita automatického podávača dokumentov	Štandardná, 50 listov

* Len v prípade, že sa plánuje využívať.

Systémové požiadavky pre server aplikácie CG ISS

Server pre CG ISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Požiadavky na sieťové prostredie pre CG ISS:

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,
- na serveri s projektom a databázou CG ISS
  - povolené porty pre komunikáciu klient/server pre projekt CG ISS (zdieľanie),
  - povolená komunikácia klient/server na Oracle databázový server (štandardne port TCP 1521),
- na klientoch povolený prístup k projektu a databáze CG ISS (firewall, Internet Explorer).

1. Hardvérové a softvérové požiadavky pre server CG ISS

Hardvér/ softvér	Server CG ISS minimálne požiadavky	Server CG ISS odporúčané požiadavky
*procesor	2 x CPU Dual Core 3,0 GHz a viac alebo 2 x CPU Quad/Hexa Core	2 x CPU Quad Core s možnosťou rozšírenia na viac CPU
**RAM	8 GB s max. kapacitou aspoň 32 GB	12 GB a viac s max. kapacitou aspoň 32 GB
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	Integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS pre projekt CG ISS a databázu SAS/SATA pre zálohy otáčky 10k alebo 15k	SAS pre projekt CG ISS a databázu SAS/SATA pre zálohy otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***100 - 300 GB v RAID1/10/5/6 pre údaje ***200 - 300 GB v RAID1/5/6 pre zálohy	60 GB v RAID1/10/5/6 pre OS ***100 - 300 GB v RAID1/10/5/6 pre údaje ***200 - 300 GB v RAID1/5/6 pre zálohy
LAN	1 Gbps	2 x 1 Gbps
Zálohovacie zariadenie	Pásková mechanika LTO4 a viac sieťový disk, externý USB disk, a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
Databáza	Oracle RDBMS 11gR2 x64	Oracle RDBMS 11gR2 x64
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Softvér	Internet Explorer 9.x alebo novší Runtime IS Oracle klient 11gR2 32-bit	Internet Explorer 11.x Runtime IS Oracle klient 11gR2 32-bit

* Môžu byť použité ekvivalenty virtuálnych CPU.

** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.

*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.

**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

2. Požiadavky pre súčasnú prevádzku CG Portál ISS a CG GISAM

Odporúča sa aplikácie CG Portál ISS a CG GISAM prevádzkovať na samostatnom serveri, nie spoločne na serveri s CG ISS.

Softvér/hardvér	Server CG ISS + CG Portál ISS	Server CG ISS + CG GISAM
RAM	-	+ 4 GB
Webový server	Microsoft IIS 7.x / 8.x	Microsoft IIS 7.x / 8.x
Oracle AS	-	Oracle GlassFish 3.2, Oracle mapviewer 11g
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.5	MS .NET Framework 3.5 MS .NET Framework 4.5 MS SOAP Toolkit 3.0, Java JDK 1.7 x64

3. Požiadavky pre súčasnú prevádzku s CG DISS

Odporúča sa aplikácie CG DISS prevádzkovať na samostatnom serveri, nie spoločne na serveri s CG ISS, môže byť použitý server CG Portál ISS a CG GISAM.

Softvér/hardvér	Server CG ISS + CG DISS
RAM	+ 1 GB
Webový server	Microsoft IIS 7.x / 8.x
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.5

Systémové požiadavky pre server CG Portál ISS

Server CG Portál ISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Hardvérové a softvérové požiadavky pre server CG Portál ISS

Hardvér/ softvér	Server CG Portál minimálne požiadavky	Server CG Portál odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	2 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Oracle klient	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS 7.x / 8.x	Microsoft IIS 7.x / 8.x
Softvér	MS .NET Framework 3.5 + 4.5 Internet Explorer 9.x alebo novší Acrobat Reader 7.x alebo novší	MS .NET Framework 3.5 + 4.5 Internet Explorer 11.x Acrobat Reader 9.x alebo novší

* Môžu byť použité ekvivalenty virtuálnych CPU.

** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.

*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.

**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

Požiadavky na sieťové prostredie pre CG Portál ISS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,
- mailové konto s povolením zasielania mailov cez SMTP aj mimo lokálnu poštovú doménu spravidla portal@domena.sk pre účely zasielania servisných správ,
- na serveri s CG Portál ISS
  - povolené porty pre komunikáciu aplikačného servera CG Portál ISS,
  - povolené porty pre komunikáciu webového servera Microsoft IIS (http) aj z LAN,
  - povolená komunikácia na Oracle databázový server (TCP 1521),
  - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
  - na klientoch povolený a nakonfigurovaný prístup k intranetovej webovej aplikácii CG Portál ISS (firewall, Internet Explorer, proxy server).

Systémové požiadavky pre CG GISAM

Server pre CG GISAM môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Hardvérové a softvérové požiadavky pre server CG GISAM

Hardvér/ softvér	Server CG GISAM minimálne požiadavky	Server CG GISAM odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Softvér Oracle	Oracle GlasFish 3.2 Oracle Mapviewer 11g, Mapbuilder 11g Oracle klient 11gR2 32-bit	Oracle GlasFish 3.2 Oracle Mapviewer 11g, Mapbuilder 11g Oracle klient 11gR2 32-bit
Web server	Microsoft IIS 7.x / 8.x	Microsoft IIS 8.x
Softvér	Java JDK 1.7 x64 MS SOAP Toolkit 3.0 MS .NET Framework 3.5 MS .NET Framework 4.5 Internet Explorer 9.x alebo novší Acrobat Reader 7.x alebo novší	Java JDK 1.7 x64 MS SOAP Toolkit 3.0 MS .NET Framework 3.5 MS .NET Framework 4.5 Internet Explorer 11.x Acrobat Reader 9.x alebo novší

* Môžu byť použité ekvivalenty virtuálnych CPU.
** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.
*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.
**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

Požiadavky na sieťové prostredie pre CG GISAM

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený na 1 Gpbs,
- doména Windows alebo pracovná skupina,
- používateľské účty pre správu a implementáciu produktov,
- administrátorský prístup na server,
- na serveri s CG GISAM
  - povolené porty pre aplikačný server Oracle (TCP 9200-9202),
  - povolená komunikácia klientov na aplikačný server Oracle (TCP 9200) v LAN,
  - povolené porty pre komunikáciu webového servera Microsoft IIS (http, TCP 80),
  - povolené porty pre komunikáciu s aplikačným serverom CG Portál ISS,
  - povolená komunikácia na Oracle databázový server (TCP 1521),
- na klientoch povolený a nakonfigurovaný prístup k intranetovej webovej aplikácii CG GISAM (firewall, Internet Explorer, proxy server).

Systémové požiadavky pre server CG DISS

Server CG DISS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Hardvérové a softvérové požiadavky pre server CG DISS

Hardvér/ softvér	Server CG DISS minimálne požiadavky	Server CG DISS odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	1 Gbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Oracle klient	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS 7.x / 8.x	Microsoft IIS 7.x / 8.x
Softvér	MS .NET Framework 3.5 + 4.5 Internet Explorer 9.x alebo novší Acrobat Reader 7.x alebo novší	MS .NET Framework 3.5 + 4.5 Internet Explorer 11.x Acrobat Reader 9.x alebo novší

* Môžu byť použité ekvivalenty virtuálnych CPU.
** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.
*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.
**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

Požiadavky na sieťové prostredie pre CG DISS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený na 1 Gpbs,
- doména Windows,
- administrátorský prístup na server,
- používateľské účty pre správu a implementáciu produktov,
- v prípade využívania notifikácie mailové konto s povolením zasielania mailov cez SMTP aj mimo lokálnu poštovú doménu spravidla edis@domena.sk,
- na serveri s CG DISS
  - povolené porty pre komunikáciu webového servera Microsoft IIS (http) aj z LAN,
  - povolená komunikácia na Oracle databázový server (TCP 1521),
  - pre aplikáciu prevádzkovanú na protokole https vystavený SSL certifikát na meno servera a dôveryhodný v prostredí domény Windows,
- na klientoch povolený a nakonfigurovaný prístup k intranetovej webovej aplikácii CG DISS (firewall, Internet Explorer, proxy server).

Systémové požiadavky pre CG WEBGIS

Server pre CG WEBGIS môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Hardvérové a softvérové požiadavky pre server CG WEBGIS

Hardvér/ softvér	Server CG WEBGIS minimálne požiadavky	Server CG WEBGIS odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	2x 100 Mbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Zálohovacie zariadenie	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Databáza	Oracle RDBMS 11gR2 x86/x64	Oracle RDBMS 11gR2 x64
Softvér Oracle	Oracle GlasFish 3.2 Oracle Mapviewer 11g, Mapbuilder 11g Oracle klient 11gR2 32-bit	Oracle GlasFish 3.2 Oracle Mapviewer 11g, Mapbuilder 11g Oracle klient 11gR2 32-bit
Web server	Microsoft IIS 7.x / 8.x	Microsoft IIS 8.x
Softvér	Java JDK 1.7 x64 MS SOAP Toolkit 3.0 MS .NET Framework 3.5 MS .NET Framework 4.5 Acrobat Reader 7.x alebo novší Internet Explorer 9.x alebo vyšší alebo iný kompatibilný prehliadač	Java JDK 1.7 x64 MS SOAP Toolkit 3.0 MS .NET Framework 3.5 MS .NET Framework 4.5 Acrobat Reader 9.x alebo novší Internet Explorer 11.x alebo iný kompatibilný prehliadač

* Môžu byť použité ekvivalenty virtuálnych CPU.
** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.
*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.
**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

Požiadavky na sieťové prostredie pre CG WEBGIS

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený 1 Gpbs v DMZ, prípadne 1 x LAN 1 Gbps, 1 x Internet 100 Mbps,
- POZN: Možnosti reálneho zapojenia závisia od sieťovej infraštruktúry a použitých prvkov (firewall, proxy servera pod.) na úrade a je možné ich čiastočne prispôsobiť.
- pevná internetová adresa,
- registrované internetové DNS záznamy typu A napr. gis.domena.sk a syncgis.domena.sk,
- na firewalle a proxy serveri zabezpečiť smerovania dotazov z LAN a Internetu na http://gis.domena.sk resp https://gis.domena.sk. na vnútornú adresu servera bez zmeny hlavičky s použitím host header,
- na serveri s CG WEBGIS
    - povolené porty pre aplikačný server Oracle (TCP 9200-9202),

- povolené porty pre komunikáciu webového servera Microsoft IIS (http, https, TCP 80, 443),
- povolená komunikácia na Oracle databázový server (TCP 1521),
- povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
- v prípade využitia SSL zakúpený SSL certifitkát typu SHA256 od dôveryhodnej internetovej certifikačnej autority pre daný internetový DNS, resp iný napr. typu wildcard (*.domena.sk),

- povolená komunikácia servera do siete Internet (80, 443).

Systémové požiadavky pre CG EGOV

Server pre CG EGOV môže byť fyzický alebo prevádzkovaný vo virtuálnom prostredí, pokiaľ hardvér spĺňa základné požiadavky na virtualizáciu a výkon.

Hardvérové a softvérové požiadavky pre server CG EGOV

Hardvér/ softvér	Server CG EGOV minimálne požiadavky	Server CG EGOV odporúčané požiadavky
*procesor	1 x CPU Dual Core 3,0 GHz a viac alebo 1x CPU Quad Core/ Hexa Core	2 x CPU Dual Core 3,0 GHz a viac alebo 1 x CPU Quad Core
**RAM	4 GB	4 GB a viac
Radič HDD	integrovaný HW radič diskového poľa RAID SAS s 512MB cache	integrovaný HW radič diskového poľa RAID SAS s 512MB cache
Typ HDD	SAS, otáčky 10k alebo 15k	SAS, otáčky 10k alebo 15k
kapacita HDD	50 až 60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje	60 GB v RAID1/10/5/6 pre OS ***50 až 100 GB v RAID1/10/5/6 pre údaje
LAN	2 x 100 Mbps	2 x 1 Gbps
UPS	Riadený záložný zdroj na 15-30 min.	Riadený záložný zdroj na 15-30 min.
Zálohovacie zariadenie	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.	Sieťový disk, externý USB disk, pásková mechanika LTO4 a viac a pod.
Iné	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia	DVD ROM, monitor, klávesnica, myš, garancia doby na odstránenie poruchy, redundantné prvky hardvéru, klimatizácia
****Operačný systém	Windows Server 2008, 2008 R2 (x64) Windows Server 2012, 2012 R2 (x64)	Windows Server 2012 R2
Databáza	Oracle RDBMS 11gR2 x86/x64	Oracle RDBMS 11gR2 x64
Softvér Oracle	Oracle klient 11gR2 32-bit	Oracle klient 11gR2 32-bit
Web server	Microsoft IIS 7.x / 8.x	Microsoft IIS 8.x
Softvér	MS .NET Framework 3.5 MS .NET Framework 4.5 Acrobat Reader 7.x alebo novší Internet Explorer 9.x alebo vyšší alebo iný kompatibilný prehliadač	MS .NET Framework 3.5 MS .NET Framework 4.5 Acrobat Reader 9.x alebo novší Internet Explorer 11.x alebo iný kompatibilný prehliadač

* Môžu byť použité ekvivalenty virtuálnych CPU.

** Skutočné požiadavky vyplývajú z počtu klientov a súčasne využívaných aplikácii a služieb.

*** Skutočná kapacita a požiadavky vyplývajú z množstva údajov, odhadu rastu a režimu prevádzky databázy a ďalších kritérií. Je možné použiť interné disky serverov alebo externé diskové pole.

**** Podporované edície operačných systémov Standard, Enterprise (2008, 2008 R2), Datacenter.

Požiadavky na sieťové prostredie pre CG EGOV

- sieť typu Ethernet Cat 5E a vyššia, priepustnosť aspoň 100 Mbps,
- server pripojený 1 Gpbs v DMZ, prípadne 1 x LAN 1 Gbps, 1 x Internet 100 Mbps,
- POZN: Možnosti reálneho zapojenia závisia od sieťovej infraštruktúry a použitých prvkov (firewall, proxy servera pod.) na úrade a je možné ich čiastočne prispôsobiť.
- pevná internetová adresa,
- registrované internetové DNS záznamy typu A napr. egov.domena.sk a sync.domena.sk,
- na firewalle a proxy serveri zabezpečiť smerovania dotazov z LAN a Internetu na http://egov.domena.sk resp. https://egov.domena.sk na vnútornú adresu servera bez zmeny hlavičky s použitím host header,
- používateľské účty pre správu a implementáciu produktov,
- administrátorský prístup na server,

- na serveri s CG EGOV
    - povolené porty pre aplikačný server CG EGOV (napr. TCP 9085),,
    - povolené porty pre komunikáciu webového servera Microsoft IIS (http, https, TCP 80, 443),
    - povolená komunikácia na Oracle databázový server (TCP 1521),
    - povolená vzdialená správa, povolený prístup na FTP server CORA GEO,
    - povolená komunikácia servera do siete Internet (80, 443),
    - v prípade využitia SSL zakúpený SSL certifitkát typu SHA256 od dôveryhodnej internetovej certifikačnej autority pre daný internetový DNS, resp iný napr. typu wildcard (*.domena.sk),
    - povolená komunikácia pre synchronizáciu údajov z vnútorného servera, obyčajne port TCP 81, prípadne komunikácia na http://sync.domena.sk na porte 80,
- mailové konto s povolením zasielania mailov cez SMTP mimo lokálnu doménu spravidla portal@domena.sk pre účely zasielania servisných správ zo servera CG ISS / CG Portál ISS.

Príloha č. 6 - Vyhlásenie uchádzača o subdodávateľoch

VYHLÁSENIE UCHÁDZAČA O SUBDODÁVATEĽOCH

Obchodné meno, názov uchádzača: CORA GEO, s.r.o.
Adresa, sídlo: A.Kmeťa 5397/23, 036 01 Martin
IČO: 31612989

Ako štatutárny orgán vyššie uvedeného uchádzača týmto čestne vyhlasujem(e), že na dodanie predmetu zákazky „Poskytovanie služieb pre prevádzku a údržbu informačných systémov " na základe Oznámenia o vyhlásení verejného obstarávania vyhlásenej v Úradnom vestníku EÚ

a) sa nebudú podieľať subdodávatelia a celý predmet uskutočním(e) vlastnými kapacitami*

~~b) sa budú podieľať títo subdodávatelia*:~~

*(*nehodiace sa preškrtnúť)*

P.č.	Obchodné meno a sídlo subdodávateľa**	IČO	Predmet/rozsah a podiel subdodávok
x	x	x	x
x	x	x	x
x	x	x	x

Zároveň týmto čestne vyhlasujem(e), že na dodanie predmetnej zákazky ako uchádzač, prípadne subdodávatelia a subdodávatelia podľa osobitného predpisu, ktorí majú povinnosť zapisovať sa do registra partnerov verejného sektora, nemajú v registri partnerov verejného sektora zapísaného konečného užívateľa výhod, ktorým je osoba podľa § 11 ods. 1 písm. c) zákona o verejnom obstarávaní.

V Poprade, dňa 17. augusta 2022

Ing. Jozef Habiňák
konateľ spoločnosti CORA GEO s.r.o.

Pozn.: POVINNÉ