



Príloha č. 1 - Opis predmetu zákazky

2 Základný opis predmetu zákazky: Agendový informačný systém REGISTRATÚRA

Verejný obstarávateľ požaduje dodať SW na správu registratúry (ďalej iba „Registratúra“), ktorý je certifikovaný Ministerstvom Vnútra SR na úroveň zhody „vysoká“. Informačný systém bude zabezpečovať kompletnú správu listinných aj elektronických dokumentov. Registratúra musí byť integrovaná na systém elektronických schránok ÚPVS tak, aby všetka komunikácia v zmysle zákona 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) bola zapísaná do registratúry. Registratúra musí byť integrovaná na Active directory obstarávateľa vrátane SSO a zároveň musí pri implementácii podporovať integráciu na MIDDLEWARE softvér ktorý bude poskytnutý zo strany verejného obstarávateľa na integráciu na budúce úložisko dát DMS a umožniť integráciu služieb registratúry tak, aby bola v súlade s platnými štandardami pre ISVS a to najmä v častiach „Štandardy pre webové služby“ a „Štandardy pre integráciu dát“. V prípade, že v čase realizácie projektu už uvedené komponenty budú nasadené do parlamentného informačného systému, ponúknuté riešenie ich musí využívať na integráciu, resp. ukladanie všetkých dát. Uchádzač sa svojou ponukou zaväzuje, že dodaný SW na registratúru bude podporovať verejným obstarávateľom zvolený MIDDLEWARE softvér a DMS. V prípade, že do nasadenia registratúry obstarávateľ nebude mať systém pre Middleware a pre DMS ešte nasadené, dodávateľ ich integráciu nasadí dodatočne, v dohodnutom termíne po ich nasadení do ostrej prevádzky.

Dodávateľ zabezpečí licenciu pre softvér REGISTRATÚRA **pre minimálne 250 konkurenčných používateľov**, ktorá pokryje všetky požadované parametre pre produkčné prostredie. Licencia musí zohľadňovať výkonnostné požiadavky a škálovateľnosť výkonu. Licencia musí pokrývať vysoko dostupné riešenie a musí byť rozšíriteľná až do 700 užívateľov.

2.1 Infraštruktúra

Platforma – obstarávateľ očakáva nasadenie komponentu v rámci svojej existujúcej infraštruktúry. Z tohoto dôvodu musí dodané riešenie podporovať architektúru procesora x86-64 AMD EPYC 7351P a nasadenie v prostredí MS Windows 2019 datacenter Hyper-V cluster a MS Virtual Machine Manager 2019. Obstarávateľ disponuje voľnými licenciami Windows 2019 server. V prípade využívania databázy musí podporovať MS SQL server 2019. Ak navrhované riešenie nie je možné nasadiť v existujúcom prostredí musí byť súčasťou cenovej ponuky aj kompletne hardvérové (hardvér musí byť nový, nepoužívaný s plnou technickou podporou výrobcu počas predpokladaného životného cyklu riešenia) a softvérové riešenie ktoré zabezpečí vysokú dostupnosť riešenia vrátane technickej podpory a technológie zálohovania.

Škálovateľnosť – dodané riešenie a jeho licenčný model musí umožňovať škálovateľnosť výkonu v súlade s rastúcimi požiadavkami na systémové zdroje.

Vysoká dostupnosť – komponent REGISTRATÚRA pre produkčné prostredie musí byť nasadený v konfigurácii pre vysokú dostupnosť.

Dodávateľ poskytne súčinnosť pri návrhu a implementácii výpočtovej a sieťovej infraštruktúry potrebnej k správne chodu softvéru REGISTRATÚRA v konfigurácii s vysokou dostupnosťou.



Dodávateľ realizuje inštaláciu a konfiguráciu softvéru REGISTRATÚRA a súvisiacich softvérových súčastí potrebných k správne mu chodu REGISTRATÚRY na definovanej infraštruktúre. V prípade dodania hardvéru zabezpečí aj kompletnú inštaláciu a konfiguráciu hardvéru.

2.2 Legislatívne požiadavky

Plnenie v súlade s platnou legislatívou (dopytovaný systém bude komponentom informačného systému, ktorý je základnou službou v zmysle zákona č. 69/2018)	- Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov. - Vyhláška Ministerstva vnútra Slovenskej republiky č. 628/2002 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov. - Výnos MV SR č. 525/2011 Z.z. o štandardoch pre elektronické informačné systémy na správu registratúry. - Vyhláška MV SR č. 410/2015 Z.z. o podrobnostiach výkonu správy registratúry orgánov verejnej moci a o tvorbe spisu. - Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov. - Zákon 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) - Zákon 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov - Vyhláška č. 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov - Vyhláška č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení - Zákon č. 95/2019 o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov - Vyhláška č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (KNR spadá do kategórie III.) - Vyhláška č. 78/2020 o štandardoch pre informačné technológie verejnej správy - Vyhláška č. 85/2020 o riadení projektov - Vyhláška NBÚ č. 48/2019 Z. z. o administratívnej bezpečnosti (platná od 1.1.2020 a zásadným spôsobom mení evidenciu utajovaných skutočností a tým sa mierne upraví aj registratúrny denník napr. o údaj stupňa utajenia)
--	---



	- Nariadenie rady EÚ č. 2016/269 (GDPR) - Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ošetriť registratúru tak, aby sa nemuseli vyhľadávať v dokumentoch osobné údaje a pri skenovaní ich prekryvať)
Dodržanie aktuálne platných štandardov ISVS	REGISTRATÚRA musí umožniť konfiguráciu služieb tak, aby boli v súlade s platnými štandardmi pre ISVS a to najmä v častiach „Štandardy pre webové služby“ a „Štandardy pre integráciu dát“

2.3 Minimálna funkčná špecifikácia REGISTRATÚRY

Podateľňa	- evidencia všetkej došlej pošty z vonkajšieho prostredia do organizácie/OVM/poslancom NR SR - evidencia všetkej odoslanej pošty smerom von z organizácie - evidencia a správa adresátov a odosielateľov (komplexná databáza osôb a organizácií) - podpora e-podacieho hárku - možnosť pripojiť naskenovaný dokument priamo k registratúrnemu záznamu - podpora integrácie na elektronické schránky uvedené v časti integrácie - možnosť vytvoriť registratúrny záznam priamo z emailu užívateľa registratúry - pridelenie pošty na vybavenie organizačného útvaru alebo spracovateľov - príjem, spracovanie a vytváranie elektronických formulárov (XML/eFormuláre) - evidencia stavu odosielania jednotlivých doručovacích úloh
Denník spisov a denník záznamov	- vytváranie spisov a stanovenie vecnej skupiny - vytváranie obsahu spisu, zakladanie záznamov v spise - prečíslovanie spisov pri prechode na nový rok - spracovanie záznamov spracovateľom alebo riadiacim pracovníkom organizačného útvaru - vybavenie/uzatvorenie spisu - automatické nastavenie agendy podľa vstupného elektronického formulára - vyhľadávanie a filtrovanie záznamov - tlač obsahu spisu a spisového obalu - export dát z tabuľkových prehľadov do tabuľkového procesora (MS Excel)



	a kompatibilné) - sledovanie lehôt pre vybavenie záznamov, emailová notifikácia a kontrola na blížiaci sa termín vybavenia, emailová notifikácia poslancom (prípadne asistentom) o doručenej pošte
Registratúrne stredisko	- správa ukladacích jednotiek - preberanie spisov z útvarov - tlač preberacích protokolov - ukladanie spisov do ukladacích jednotiek - lokalizácia ukladacích jednotiek - zapožičiavanie ukladacích jednotiek - tlač zoznamu prírastkov - podpora vyradovacieho konania (termíny na skartačné a vyradovacie konanie) - automatické vyradovacie konanie
Správa registratúry	- podpora správy vo všetkých oblastiach (podateľňa, registratúrne stredisko apod.) - správa číselníkov (organizačná štruktúra, organizácie, osoby a pod.) - správa používateľov a privilégii vrátane privilégii k dokumentom - možnosť zaraďovať používateľov do skupín - správa agend - správa ročníkov - správa ročnej uzávierky
Záznamy špecializovanej registratúry	- možnosť vytvárania rôznych evidencií v špecializovanej registratúre (vrátane inej agendy spracováanej v iných produkčných systémoch) - príjem, spracovanie a vytváranie elektronických formulárov (XML/eFormuláre) - vlastné číslovanie pre každú agendu (jednoznačný identifikátor) - možnosť kategorizácie podľa typov agendy prostredníctvom identifikátora - možnosť kategorizácie podľa typov záznamov prostredníctvom identifikátora - možnosť riadenia prístupu podľa typov zásielok/dokumentov - možnosť oddeliť proces evidencie rôznych typov zásielok a dokumentov podľa oprávnení k nim - možnosť nastavovania metadát pre riadenie bezpečnosti (napr. GDPR)



	a pod.) ktoré umožnia zvláštny režim riadenia prístupu k záznamu - evidencia a správa viacerých špecializovaných registratúrnych stredísk - v rámci špecializovaného registratúrneho strediska diferenčné nastavenie umiestnení a ukladacích jednotiek - automatické postúpenie záznamu špecializovanej registratúry do produkčného systému
Reporting	Odchádzajúca pošta - report za ľubovoľné časové obdobie - report za ľubovoľné oddelenie alebo organizačnú zložku - report na doporučené, obyčajné a prioritné zásielky - report na typy zásielok Prichádzajúca pošta - report za ľubovoľné časové obdobie - report za ľubovoľné oddelenie alebo organizačnú zložku - report na spôsob doručenia zásielok do spoločnosti - report na typy prijatých listov - report na počet prijatých zásielok za obdobie Reporty k záznamom a spisom - report za ľubovoľné časové obdobie - report vybavených / nevybavených - report nevybavených v stanovenom termíne - nevybavených a neuzatvorených spisov z predchádzajúceho kalendárneho roka (prechodová tabuľka) - report pridelených záznamov na jednotlivých správcov záznamov / spracovateľov - report histórie - report - so znakom hodnoty „A“, bez znaku hodnoty „A“ - report archívnych dokumentov presunutých po vypočítaní konaní do archívu + ich umiestnenie v škatuli - odovzdávací protokol do RS - registratúrny plán - návrh na odovzdanie spisov do registratúrneho strediska - odovzdanie spisov do registratúrneho strediska



	- návrh na vyradenie spisov so znakom hodnoty A - návrh na vyradenie spisov bez znaku hodnoty - protokol o vyradení spisov bez znaku hodnoty - protokol o vyradení spisov so znakom hodnoty A Vypožičiavanie spisov - report za ľubovoľné časové obdobie - vybavené - požičané / nevybavené + stav - vrátený / nevrátený (aj s informáciou o dodržaní stanovenej lehoty)
Skenovanie	- Možnosť označovať dokumenty čiarovým kódom - Párovanie skenovaných dokumentov so záznamom v registratúre na základe čiarového kódu
Logovanie	- aktivity administrátorov a používateľov musia byť zaznamenávané

2.4 Integrácie na ÚPVS

Integrácia registratúry na ÚPVS	- Ústredný portál verejnej správy, - Modul dlhodobého ukladania registratúrnych záznamov – ÚPVS, - Centrálné úradné doručovanie – ÚPVS, - ovládacie rozhranie REGISTRATÚRY ktoré umožní integráciu na integračnú platformu MIDDLEWARE objednávateľa v rozsahu ktorý umožní obojsmernú dátovú výmenu
Integrácia na ÚPVS umožní	- automatické prijatie podania z eDesku (elektronickej schránky) do systému pre správu registratúry, - zobrazenie prijatých podaní z eDesk pre podateľňu, - celé podanie existuje iba v elektronickej forme, papierový dokument nie je k dispozícii, - rozbalenie správy do čitateľnej formy - transformáciu elektronických správ na registratúrne záznamy - pridelenie na spracovateľský útvar - odoslanie rozhodnutia prípadne iného odoslaného záznamu do eDesku príjemcu zo systému pre správu registratúry - transformáciu registratúrnych záznamov na elektronické správy - odoslaný záznam existuje iba v elektronickej forme, papierový dokument nie je k dispozícii - podpisovanie je realizované prostredníctvom kvalifikovaného



	elektronického podpisu, zaručenej elektronickej pečate a časovej pečiatky alebo elektronického podpisu - automatické pečatenie odosielaných správ - automatický monitoring doručenia správy a priloženie doručanky k záznamu - proces sprístupnenia spisu - proces spracovania spisu - schvaľovací proces - proces vyvedenia spisov do osobitnej evidencie a prenos dát - proces pripomienkového konania - proces pre neformálne vyjadrenie, vzatie záznamu na vedomie - proces presunu spisov do špecializovanej registratúry a registratúrneho strediska - SW musí podporovať elektronický schvaľovací proces nad každým dokumentom s uchovaním kompletnej histórie (kto, kedy, čo so spisom urobil) - SW musí kontrolovať termíny uložené jednotlivými osobami na jednotlivých úrovniach - SW musí umožňovať zasielanie mailových notifikácií - Treba zvážiť možnosť, či by firma nebola schopná dodať aj elektronický archív, t. j. možnosť trvalého uloženia vyradených elektronických dokumentov z registratúry – aby sme si všetky elektronické dokumenty mohli archivovať sami - overovanie elektronických podpisov
Centrálné úradné doručovanie – ÚPVS	- registratúra zabezpečí prostredníctvom integrácie na ÚPVS doručovanie úradných dokumentov v elektronickej forme prostredníctvom modulu centrálného úradného doručovania (CÚD)
Modul dlhodobého ukladania registratúrnych záznamov – ÚPVS	- Systém musí byť pripravený na dlhodobé uchovávanie elektronických dokumentov
Požadujeme implementáciu pre nasledovné elektronické schránky NRSR	- Kancelária Národnej rady SR - Mandátový a imunitný výbor NR SR - Výbor NR SR na preskúmavanie rozhodnutí NBÚ - Výbor NR SR pre nezlučiteľnosť funkcií



	- Národná rada SR
--	-------------------

2.5 Integračné rozhranie

Ovládacie rozhranie REGISTRATÚRY musí umožniť integráciu na integračnú platformu MIDDLEWARE objednávateľa v rozsahu ktorý umožní obojsmernú dátovú výmenu tak, aby bola v súlade s platnými štandardami pre ISVS a to najmä v častiach „Štandardy pre webové služby“ a „Štandardy pre integráciu dát“.

Všetky neštruktúrované dokumenty musia byť ukladané prostredníctvom MIDDLEWARE v informačnom systéme DMS obstarávateľa s definovanými metadátami.

REGISTRATÚRA musí obsahovať minimálne:

- pole „typ dokumentu“, ktorý sa bude načítavať z informačného zdroja „typy dokumentov v DMS“ v informačnom systéme „Digitálny archív“ cez webové služby
- pole „volebné obdobie“, ktoré si bude načítavať z webservisu z informačného zdroja „volebné obdobia“
- musí umožňovať pri založení (aplikačnej funkcii Uložiť, alebo Publikovať) zvoleného typu dokumentu spustiť požadovaný webservis (napr. pre založenie záznamu v agendovom informačnom systéme)
- musí umožňovať označovať záznamy v štádiu:
 - rozpracovaný, alebo pripravovaný – ešte nebude poskytovaný webservisom cez MIDDLEWARE do externých informačných systémov
 - publikovaný – záznam je poskytnutý webservisom cez MIDDLEWARE do externých informačných systémov

REGISTRATÚRA musí poskytovať cez MIDDLEWARE do externých informačných systémov, minimálne nasledovné údaje:

- Webservis pre načítanie záznamov zvoleného typu dokumentu v zvolenom volebnom období
- Webservis pre načítanie metadát zvoleného dokumentu aj s linkou na jeho zobrazenie v DMS
- Webservis pre založenie nového záznamu do Registratúry, pričom webservis vráti jednoznačný identifikátor záznamu (ktorý založil) – pre prípad, že záznamy sú zakladané z agendových informačných systémov
- Webservis pre vrátenie identifikátora dokumentu v DMS, prípadne funkciu na jeho otvorenie
- Webservis pre návrat dokumentov podľa zvoleného filtra (filter bude súčasťou rokovania s víťazným uchádzačom po podpise zmluvy)

Uvedená špecifikácia je minimálna, počas analýzy cieľového stavu je možné špecifikáciu upraviť podľa potreby.

**2.6 Implementácia formulárov a schvaľovacích procesov**

Obstarávateľ požaduje vytvoriť 3 formuláre so schvaľovaním prostredníctvom elektronického podpisu. Špecifikácia formulárov uvedená nižšie je minimálna, počas analýzy cieľového stavu je možné špecifikáciu po dohode s obstarávateľom upraviť podľa potreby.

Ovládacie rozhranie REGISTRATÚRY musí umožniť integráciu na integračnú platformu MIDDLEWARE objednávateľa v rozsahu ktorý umožní obojsmernú dátovú výmenu pre tieto agendy. (Vytvorenie žiadanky a prístup ku žiadankám z iného informačného systému)

Formulár 1 pre schvaľovanie zámerov verejného obstarávania

Vstupný formulár – polia, ktoré je možné vyplniť používateľom

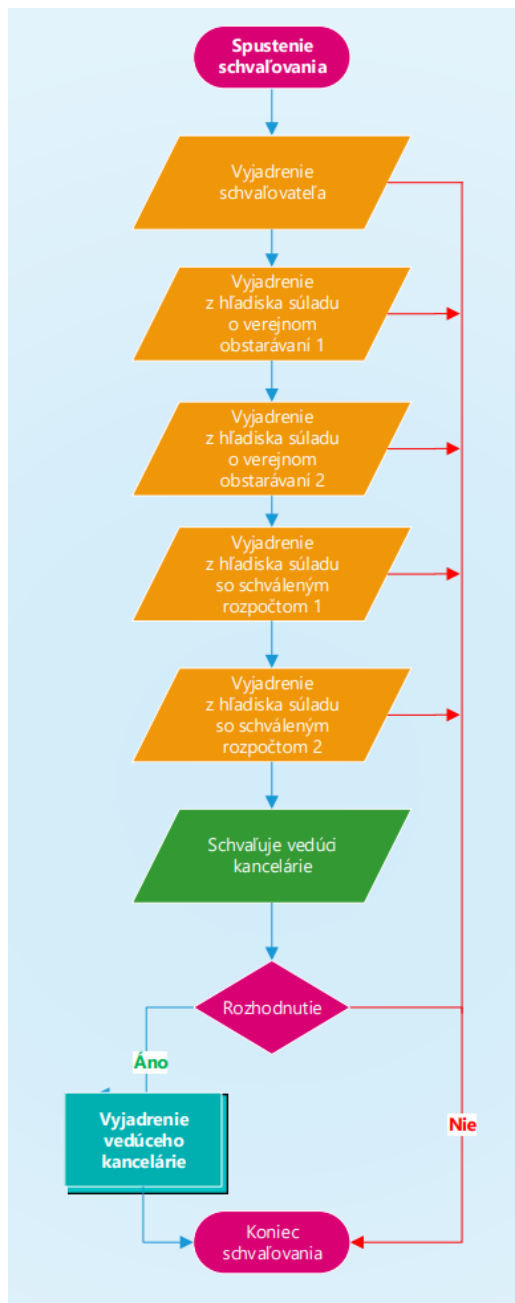
Číslo zámeru	Automaticky generovaný identifikátor
Žiadateľ	Meno priezvisko žiadateľa
Názov	pole s názvom
Opis predmetu	pole s opisom predmetu obstarávania
Trvanie zmluvného vzťahu	Pole s dĺžkou trvania
Postup vo VO	Výberové pole
Predpokladaná hodnota (bez DPH)	Suma
Požadovaný termín ukončenia VO	Dátum

Polia, ktoré nie sú viditeľné – vyplňa ich systém

Rola Schvalovateľ	Skupina/používateľ
Rola Súhlas verejného obstarávateľa 1	Skupina/používateľ
Rola Súhlas verejného obstarávateľa 2	Skupina/používateľ
Rola Súhlas súladu so schváleným rozpočtom 1	Skupina/používateľ
Rola Súhlas súladu so schváleným rozpočtom 2	Skupina/používateľ
Rola Súhlas vedúceho kancelárie	Skupina/používateľ

Schvaľovací algoritmus

Každý krok v schvaľovaní môže schváliť používateľ ktorý má pridelenú príslušnú rolu (je členom skupiny alebo priamo pridelený)





KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

ODBOR PRÁVNÝCH SLUŽIEB A VEREJNÉHO OBSTARÁVANIA

Zobrazenie pre tlač



KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

SYSTÉMOV, POSKYTOVANÝCH ELEKTRON.SLUŽIEB A BEZPEČNOSTI INFOR.-KOMUNIK.TE

ZÁMER VEREJNÉHO OBSTARÁVANIA č. ZAM2020171

Názov zákazky: Nákup telefónu	
Predpokladaná hodnota zákazky bez DPH v €:	1 245,00
Opis predmetu zákazky: Apple iPhone 11 Pro, 512 GB, Space Grey	
Trvanie zmluvného vzťahu v mesiacoch: 24 Navrhovaná forma obstarania: Priame zadanie – do 5 000 eur, ak ide o zákazku na dodanie tovaru (okrem potravín), poskytnutie služby alebo uskutočnenie stavebných prác – výnimka zo zákona (neformálny prieskum)	
Požadovaný termín ukončenia VO: 23. 3. 2020	
Priezvisko/dátum/podpis: Martin, Mgr. / 23.03.2020 / podpísané el. podpisom	
Vykonanie základnej finančnej kontroly podľa zákona o finančnej kontrole a audite:	
a): overujem, že zámer je v súlade s hospodárnosťou, efektívnosťou, účinnosťou, účelnosťou a v súlade so všeobecne platnými predpismi, internými aktmi riadenia, uzatvorenou zmluvou a súhlasím s jej pokračovaním: gestor, vedúci zamestnanec, resp. poverený zamestnanec Priezvisko/dátum/podpis: Karol, Ing. / 23.03.2020 / podpísané el. podpisom	
b) potvrdzujem, že zámer VO je v súlade so schváleným rozpočtom a zákonom o rozpočtových pravidlách: EO/Priezvisko/dátum/podpis: Ľubica, Ing. / 24. 3. 2020 8:48:05 / podpísané el. podpisom EO2/Priezvisko/dátum/podpis: Daniela, Ing. / 24. 3. 2020 8:52:57 / podpísané el. podpisom	
c) potvrdzujem, že zámer VO je v súlade so zákonom o verejnom obstarávaní: OPSVO/Priezvisko/dátum/podpis: Martin, Mgr. / 23. 3. 2020 16:38:53 / podpísané el. podpisom OPSVO2/Priezvisko/dátum/podpis: , JUDr. / 23. 3. 2020 16:42:10 / podpísané el. podpisom	
Vedúci kancelárie Priezvisko/dátum/podpis: Daniel, Ing. / 24. 3. 2020 13:51:16 / podpísané el. podpisom	

Formulár 2 pre schvaľovanie finančných operácií

Vstupný formulár – polia, ktoré je možné vyplniť používateľom

Číslo finančnej operácie	Automaticky generovaný identifikátor
Zamestnanec	Meno priezvisko žiadateľa
Predmet	pole s názvom



KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

ODBOR PRÁVNÝCH SLUŽIEB A VEREJNÉHO OBSTARÁVANIA

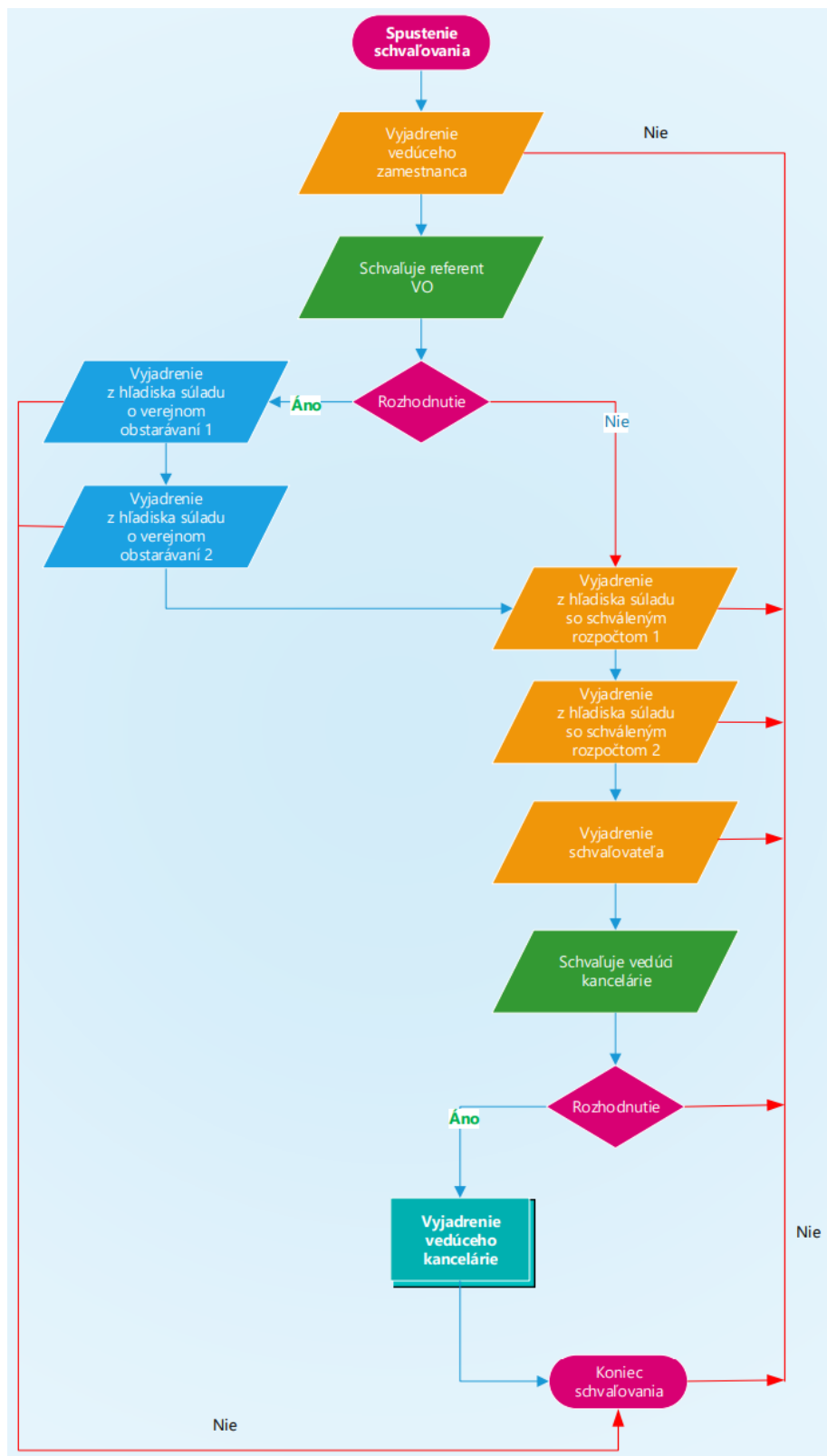
Predpokladaná cena bez DPH	Suma
DPH	Percento
Predpokladaná cena s DPH	Suma
Zdôvodnenie	Pole so zdôvodnením
Forma obstarávania	Výberové pole
Zmluva	Pole s číslom zmluvy
Zámer	Pole s číslom zámeru
Iné rozhodnutie	Pole s inou referenciou
Žiadanka	Pole s číslom žiadanky

Polia, ktoré nie sú viditeľné – vyplňa ich systém

Rola Súhlas vedúceho zamestnanca	Skupina/používateľ
Rola Súhlas verejného obstarávateľa 1	Skupina/používateľ
Rola Súhlas verejného obstarávateľa 2	Skupina/používateľ
Rola Súhlas súladu so schváleným rozpočtom 1	Skupina/používateľ
Rola Súhlas súladu so schváleným rozpočtom 2	Skupina/používateľ
Rola Súhlas vedúceho kancelárie	Skupina/používateľ

Schvaľovací algoritmus

Každý krok v schvaľovaní môže schváliť používateľ ktorý má pridelenú príslušnú rolu (je členom skupiny alebo priamo pridelený)





KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

ODBOR PRÁVNÝCH SLUŽIEB A VEREJNÉHO OBSTARÁVANIA

Zobrazenie pre tlač



KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

.SYSTÉMOV, POSKYTOVANÝCH ELEKTRON.SLUŽIEB A BEZPEČNOSTI INFOR.-KOMUNIK.TE

NÁVRH FINANČNEJ OPERÁCIE č. FO00282/20 - VÝDAVKY

Predmet finančnej operácie: Nákup telefónu
Predpokladaná cena s DPH v €: 1 494,00 Predpokladaná cena bez DPH v €: 1 245,00
Zdôvodnenie: Apple iPhone 11 Pro, 512 GB, Space Grey
Navrhovaná forma obstarania: Priame zadanie – do 5 000 eur, ak ide o zákazku na dodanie tovaru (okrem potravín), poskytnutie služby alebo uskutočnenie stavebných prác – výnimka zo zákona (neformálny prieskum)
Návrh finančnej operácie predkladá v súlade: a) s uzatvorenou zmluvou č.: b) iným rozhodnutím: Zámer: ZAM2020171 c) internými aktmi riadenia: d) inými podmienkami poskytnutia:
meno a priezvisko/dátum/podpis: Martin , Mgr. / 23. 3. 2020 14:37:41 / Schválené pri zámere
Vykonanie základnej finančnej kontroly podľa zákona o finančnej kontrole a audite :
a) vecné plnenie - súlad s hospodárnosťou, efektívnosťou, účinnosťou, účelnosťou a súlad so všeobecne platnými predpismi, internými aktmi riadenia a uzatvorenou zmluvou: Vo finančnej operácii alebo jej časti je / nie-je* možné pokračovať: vedúci zamestnanec, resp. poverený zamestnanec zodpovedný za vecné plnenie/meno a priezvisko/dátum/podpis: Karol , Ing. / 23.03.2020 / Schválené pri zámere
b) súlad so schváleným rozpočtom a zákonom o rozpočtových pravidlách: Vo finančnej operácii alebo jej časti je / nie-je* možné pokračovať: EO/zamestnanec zodpovedný za rozpočet/meno a priezvisko/dátum/podpis: Ľubica , Ing. / 24. 3. 2020 / Schválené pri zámere
Vo finančnej operácii alebo jej časti je / nie-je* možné pokračovať: EO/vedúci zamestnanec, resp. poverený zamestnanec zodpovedný za rozpočet/meno a priezvisko /dátum/podpis: Daniela , Ing. / 24. 3. 2020 / Schválené pri zámere
c) súlad so zákonom o verejnom obstarávaní: Vo finančnej operácii alebo jej časti je / nie-je* možné pokračovať: OPSVO/zamestnanec zodpovedný za verejné obstarávanie/meno a priezvisko/dátum/podpis: Martin , Mgr./23.03.2020/Schválené pri zámere
Vo finančnej operácii alebo jej časti je / nie-je* možné pokračovať: OPSVO/vedúci zamestnanec, resp. poverený zamestnanec zodpovedný za verejné obstarávanie/meno a priezvisko/dátum/podpis: Martina , JUDr./23.03.2020/Schválené pri zámere
Finančnú operáciu schválil v súlade s podpisovým oprávnením**: meno a priezvisko/dátum/podpis: Daniel , Ing. / 24. 3. 2020 / Schválené pri zámere

* Nehodiace sa prečiarknite

** Rozhodnutie vedúceho Kancelárie Národnej rady Slovenskej republiky o priznaní poukazovacieho a dispozičného práva v platnom znení

Formulár 3 žiadanka o dovolenku alebo iné prerušenie

Vstupný formulár – polia, ktoré je možné vyplniť používateľom

Žiadateľ	Meno priezvisko žiadateľa
----------	---------------------------

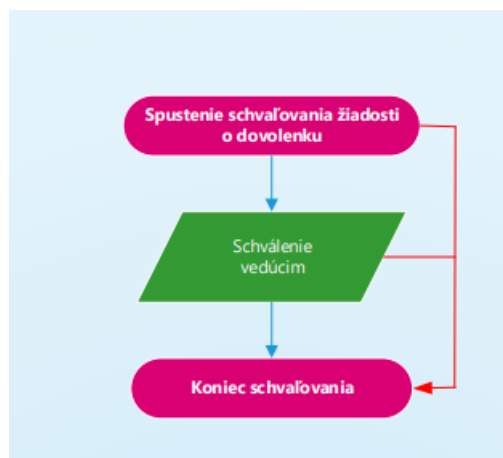


Typ prerušenia	Výberové polia
Dátum od	Dátum/čas
Dátum do	Dátum/čas
Počet dní	Výpočtové pole
Sobota, Nedeľa, Sviatok	áno / nie
Miesto	Textové pole
Poznámka	Textové pole

Polia, ktoré nie sú viditeľné – vyplňa ich systém

Rola Schvalovateľ	Skupina/používateľ
-------------------	--------------------

Schvaľovací algoritmus



Každý krok v schvaľovaní môže schváliť používateľ ktorý má pridelenú príslušnú rolu (je členom skupiny alebo priamo pridelený) pre daný organizačný útvar.

2.7 Ostatné požiadavky

V rámci implementácie požadujeme	- v spolupráci s obstarávateľom dodávateľ zabezpečí vytvorenie nového registratúrneho poriadku optimalizovaného pre softvér REGISTRATÚRA - dodávateľ zabezpečí prvotné naplnenie dát z pôvodnej registratúry - dodávateľ sa zaväzuje vykonať právnu analýzu súladu spracúvania osobných údajov v dodávanom informačnom systéme voči požiadavkám platnej legislatívy SR a EÚ na ochranu osobných údajov - Dodávateľ sa zaväzuje dodať ku informačnému systému dokument Analýza bezpečnosti, ktorý bude súčasťou Bezpečnostného projektu podľa prílohy
----------------------------------	--



	č. 3 Vyhlášky č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy - Dodávateľ sa zaväzuje, že pri dodávke informačného systému zabezpečí vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí
Implementácia a integrácia	- inštalácia a konfigurácia REGISTRATÚRY v prostredí obstarávateľa - školenie administrátorov a používateľov
dokumentácia	- používateľská dokumentácia - administrátorská dokumentácia - prevádzková dokumentácia
technická podpora	- očakávaný životný cyklus produktu je 6 rokov - zapracovanie všetkých legislatívnych zmien - softvérové a bezpečnostné aktualizácie produktu - servisná podpora 24x7x365 garantovaná výrobcom SW

2.8 Požiadavky na dodanie dokumentácie

- administrátorská dokumentácia
 - Inštalčná a konfiguračná príručka musí obsahovať dokumentáciu inštalčného a konfiguračného postupu softvéru REGISTRATÚRA v minimálne takom rozsahu, aby bolo možné podľa nej inštaláciu a konfiguráciu systému zopakovať
 - Príručka zálohovania a obnovy musí obsahovať dokumentáciu procesu zálohovania a obnovy softvéru REGISTRATÚRA v takom rozsahu, aby podľa nej bolo možné nastaviť riadenie kontinuity prevádzky. Pri procese obnovy musí byť uvedený čas v ktorom je možné systém REGISTRATÚRA obnoviť do pôvodného stavu za predpokladu že podporná infraštruktúra Obstarávateľa je funkčná.
 - prevádzková dokumentácia pre administrátorov
- Používateľská dokumentácia v elektronickej forme
 - manuál na ovládanie IS používateľmi a existuje v takom rozsahu, aby používateľ vedel použiť všetky ponúkané funkcie, vrátane správneho použitia bezpečnostných mechanizmov
 - musí obsahovať používateľskú dokumentáciu softvéru s popisom štandardných postupov použiteľnú na zaškolenie nových zamestnancov
- Prevádzková dokumentácia
 - Obsahom prevádzkovej dokumentácie je najmä popis architektúry, konfigurácií, integračných väzieb a rozhraní.



2.9 Školenie administrátorov a používateľov

Poskytovateľ zabezpečí školenie administrátorov v priestoroch Kancelárie Národnej rady SR v nasledovnom rozsahu:

- školenie administrátorov – do 5 ks
 - Inštalačný a konfiguračný postup
 - Postup zálohovania a obnovy
 - Administráciu systému v plnom rozsahu funkcionality softvéru REGISTRATÚRA
- školenie sekretárook – do 30 ks
- školenie užívateľov – do 250 ks

2.10 Požadované termíny

Verejný obstarávateľ požaduje od dátumu účinnosti zmluvy dodať:

Fáza I.

- implementáciu SW na testovanie do 2 mesiacov.
- verejný obstarávateľ si vyhradzuje právo testovať SW do troch mesiacov, počas ktorých požadujeme vyškoliť požadované počty užívateľov.
- do produkčnej prevádzky požadujeme dodať REGISTRATÚRU do 3 mesiacov

Fáza II.

- migráciu starých dát požadujeme dokončiť do 6 mesiacov

Fáza III.

- integrácie na ÚPVS dokončiť do 9 mesiacov

Jednotlivé fázy projektu je možné fakturovať individuálne.

3 Požiadavky na systémovú podporu a údržbu

Verejný obstarávateľ požaduje, aby po ukončení implementácie a odovzdaní Diela dodávateľ zabezpečoval servisnú podporu pre REGISTRATÚRA softvér v nasledovnom rozsahu:

- Systémová podpora a údržba počas 6 rokov (plánovaný životný cyklus je 6 rokov)
- Aktualizácie softvéru tak, aby bol vždy vo verzii oficiálne podporovanej výrobcom vrátane:
 - poskytnutie nových verzií so zapracovanými legislatívnymi zmenami
 - poskytnutie nových verzií s optimalizovanými funkciami
 - poskytnutie nových verzií s rozšírenou funkcionalitou všeobecného charakteru
 - poskytnutie nových verzií RK v dôsledku zmien v informačných technológiách



- distribúciu nových verzií RK v zmysle predchádzajúceho bodu
- Upozorňuje na potrebu inštalácie nových verzií a zabezpečí aktualizáciu komponentov softvéru REGISTRATÚRA tak, aby nedošlo k výpadkom poskytovaných služieb v čase prevádzky (verejný obstarávateľ zabezpečí súčinnosť).
- poskytnutie odpovede cez telefónnu linku na otázky týkajúce sa problémových situácií vzniknutých pri používaní REGISTRATÚRY, tzn. k obsluhu RK, k problémovým stavom RK a k správaniu sa RK v rozpore s opisom v používateľskej dokumentácii
- Zabezpečí nepretržitú servisnú podporu v rozsahu 24x7x365 s nasledovnými parametrami (kritickosť nahlásenej servisnej udalosti určuje výrobca REGISTRATÚRA komponentu v zmysle nižšie uvedenej tabuľky - definícia úrovni kritickosti nahláseného problému):

Kritickosť nahláseného problému	Potvrdenie prijatia servisnej udalosti	Doba odozvy	Vyriešenie servisnej udalosti
Kritická	Ihneď	2,5 hodiny	2 dni
Vysoká	Ihneď	4,5 hodiny	4 dni
Nízka	1 deň	1 deň	10 dní

Definícia úrovni kritickosti nahláseného problému:

Kritická	- Softvér REGISTRATÚRA alebo jeho podstatná časť je nefunkčná. - Funkčnosť softvéru REGISTRATÚRA zlyháva alebo hrozí úplné zlyhanie systému alebo hrozí neobnoviteľná strata dát.
Vysoká	- Softvér REGISTRATÚRA je použiteľný, ale je funkčne degradovaný - Funkčnosť softvéru REGISTRATÚRA je obmedzená a narušuje normálnu prevádzku systému alebo sa dotýka významnej časti systému
Nízka	softvér REGISTRATÚRA je použiteľný, ale jedna alebo viac funkcií nefunguje podľa očakávania. Ide o nekritickú situáciu.

- Zabezpečí možnosť online nahlasovania servisných udalostí s možnosťou sledovania ich stavu riešenia
- Zabezpečí analýzu požiadavky a identifikáciu problému
- Zabezpečí riadenie servisných udalostí, požadovanú dobu odozvy od nahlásenia servisnej udalosti a riešenie servisnej udalosti v požadovanom hraničnom čase
- Zabezpečí pre verejného obstarávateľa prístup k evidencii nahlásených servisných udalostí

V prípade ak dodávateľ nedodá dielo včas, má objednávatel nárok na zmluvnú pokutu vo výške 20 % z ceny plnenia.



Pri plnení služby servisná podpora je stanovená zmluvná pokuta nasledovne:

- a. pri nedodržaní časového limitu na odstránenie problému s kritického problému: 1500 eur
 - b. pri nedodržaní časového limitu na odstránenie problému s vysokou kritickosťou: 1000 eur
 - c. pri nedodržaní časového limitu na odstránenie problému s nízkou kritickosťou: 500 eur
- za každé individuálne porušenie povinnosti.

4 Ostatné zmluvné podmienky

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení
niektorých zákonov v znení neskorších predpisov
(ďalej len „**zákon o kybernetickej bezpečnosti**“)
(ďalej len „**zmluva**“)

medzi zmluvnými stranami:

Prevádzkovateľ:	Kancelária Národnej rady Slovenskej republiky
Sídlo:	Námestie Alexandra Dubčeka 1, 812 80 Bratislava 1
IČO:	XXXXXX
Zastúpený:	XXXXXX, vedúci Kancelárie NR SR

(ďalej len „**Prevádzkovateľ základnej služby**“)

a

Dodávateľ:	
Sídlo:	
IČO:	
IČ DPH:	
Zastúpený:	
Zapísaný:	

(ďalej len „**Dodávateľ**“)

(Prevádzkovateľ základnej služby a Dodávateľ spolu ďalej len „**zmluvné strany**“)



Článok I.

ÚVODNÉ USTANOVENIA

1. **Kancelária Národnej rady Slovenskej republiky** je Prevádzkovateľom základnej služby podľa zákona o kybernetickej bezpečnosti.
2. Identifikovanými základnými službami Prevádzkovateľa základnej služby sú:
 - a)
 - b)
3. Dodávateľ uzatvára s Prevádzkovateľom základnej služby zmluvu o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore č. xxxxxxxx (ďalej len „**zmluva o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore**“), ktorej predmet má vplyv na prevádzku, alebo priamo súvisí s prevádzkou sietí a informačných systémov ako sú definované v zákone o kybernetickej bezpečnosti pre Prevádzkovateľa základnej služby.
4. Prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti.
5. Zmluva stanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa základnej služby, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany prevádzkovateľa základnej služby (ďalej len „**ciele**“), a to aj v spolupráci s dodávateľom.
6. Plnenie povinností podľa tejto zmluvy zmluvnými stranami sa vyžaduje počas celej doby trvania zmluvy.

Článok II.

ZÁKLADNÉ POJMY

Na účely tejto zmluvy sa rozumie:

- a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,
- b) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktívované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,
- c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,
- d) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
- e) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,
- f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,



- g) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernú uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,
- h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,
- i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,
- j) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je
 - strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
 - vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
 - ohrozenie bezpečnosti informácií,
- k) základnou službou služba, ktorá je zaradená v zozname základných služieb a
 - závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona o kybernetickej bezpečnosti,
 - je informačným systémom verejnej správy, alebo
 - je prvkom kritickej infraštruktúry,
- l) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k),
- m) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2 zákona o kybernetickej bezpečnosti,
- n) manažér informačnej bezpečnosti (MIB) je osoba poverená riadením informačnej a kybernetickej bezpečnosti, ktorá má právomoci a povinnosti definované v Politike informačnej bezpečnosti a ďalších smerniciach Prevádzkovateľa základnej služby. Ide najmä o kontrolné činnosti, riešenie bezpečnostných a kybernetických incidentov, riadenie implementácie bezpečnostných opatrení, konzultačné a metodické činnosti pre oblasť informačnej a kybernetickej bezpečnosti a ďalšie,
- o) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

Článok III.

PREDMET ZMLUVY

1. V zmysle § 19 ods. 2 zákona o kybernetickej bezpečnosti a s ohľadom na zmluvu o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore je predmetom tejto zmluvy stanovenie práv a povinností zmluvných strán pri zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.

Článok IV.

POVINNOSTI DODÁVATEĽA

1. Dodávateľ sa zaväzuje prijímať a dodržiavať bezpečnostné opatrenia Prevádzkovateľa základnej služby na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam bezpečnostných opatrení Prevádzkovateľa základnej služby



a súvisiace nastavenie procesov riadenia kybernetickej bezpečnosti je uvedený v prílohe č. 2 tejto zmluvy.

2. Dodávateľ vyhlasuje, že súhlasí so stanovenými bezpečnostnými opatreniami v tejto zmluve.
3. Dodávateľ je zároveň povinný dodržiavať bezpečnostné politiky Prevádzkovateľa základnej služby, s ktorými ho Prevádzkovateľ základnej služby písomne oboznámil. Dodávateľ vyhlasuje, že súhlasí s bezpečnostnými politikami Prevádzkovateľa základnej služby.
4. Dodávateľ súhlasí s tým, že bezpečnostné politiky Prevádzkovateľa základnej služby sa môžu priebežne meniť a dopĺňať tak, aby zodpovedali aktuálnym bezpečnostným opatreniam, aktuálnemu stavu sietí a informačných systémov Prevádzkovateľa základnej služby a aktuálnym hrozbám dotýkajúcim sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby.
5. Dodávateľ sa zaväzuje plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto zmluve tak, aby boli naplnené ciele tejto zmluvy. Zoznam kontaktov zmluvných strán je uvedený v prílohe č. 1 tejto zmluvy.
6. Dodávateľ vyhlasuje, že má všetko potrebné technické, technologické a personálne vybavenie, ktoré je potrebné na plnenie úloh vyplývajúcich z tejto zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie cieľov tejto zmluvy.
7. Odplata za plnenie povinností Dodávateľa podľa tejto zmluvy a náhrada všetkých nákladov vynaložených Dodávateľom v súvislosti s plnením povinností Dodávateľa podľa tejto zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom Prevádzkovateľom základnej služby Dodávateľovi podľa zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore a na žiadne ďalšie peňažné plnenia Dodávateľ za plnenie povinností podľa tejto zmluvy od Prevádzkovateľa základnej služby nemá nárok.
8. Dodávateľ sa zaväzuje, že nezapojí ďalšieho dodávateľa (ďalej len „**subdodávateľ**“) úplne alebo čiastočne zabezpečujúceho plnenie tejto zmluvy predtým, než dostane písomný súhlas Prevádzkovateľa základnej služby. Zoznam subdodávateľov tvorí prílohu č. 3 tejto zmluvy. Dodávateľ sa zaväzuje, že pri výbere subdodávateľa preverí, či tento disponuje primeraným technickým a organizačným zabezpečením. Na subdodávateľa sa primerane vzťahujú povinnosti Dodávateľa uvedené v tejto zmluve. Dodávateľ je plne zodpovedný voči Prevádzkovateľovi základnej služby za plnenie povinností subdodávateľa.
9. Plnenie povinností podľa tejto zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa základnej služby podľa zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto zmluvy po celú dobu trvania zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore.

Článok V. BEZPEČNOSTNÉ OPATRENIA



1. Dodávateľ sa zaväzuje, že má zavedené a implementované bezpečnostné opatrenia minimálne v rozsahu:
 - Organizácie informačnej bezpečnosti,
 - Riadenia aktív, hrozieb a rizík,
 - Personálnej bezpečnosti,
 - Riadenia dodávateľských služieb, akvizície, vývoj a údržby informačných systémov,
 - Technických zraniteľností systémov a zariadení,
 - Riadenia bezpečnosti sietí a informačných systémov,
 - Riadenia prevádzky,
 - Riadenia prístupov,
 - Kryptografických opatrení,
 - Riešenia kybernetických bezpečnostných incidentov,
 - Monitorovania, testovania bezpečnosti a bezpečnostných auditov,
 - Fyzickej bezpečnosti a bezpečnosti prostredia,
 - Riadenia kontinuity procesov.
2. Bezpečnostné opatrenia musia zahŕňať najmenej:
 - Detekciu kybernetických bezpečnostných incidentov,
 - Evidenciu kybernetických bezpečnostných incidentov,
 - Postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
 - Určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
 - Prepojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálného systému včasného varovania.
3. Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu v organizácii.
4. Obsah a štruktúra bezpečnostnej dokumentácie:
 - Schválená bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
 - Klasifikácia informácií a kategorizácia sietí a informačných systémov,
 - Zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
 - Vykonaná analýza rizík kybernetickej bezpečnosti,
 - Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti (§ 29 zákona o kybernetickej bezpečnosti).

Článok VI.

PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

1. Dodávateľ sa zaväzuje v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby (ďalej len „**incidenty**“):
 - a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez Dodávateľa nebolo možné zasiahnuť siete a informačné systémy Prevádzkovateľa základnej služby,
 - b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému /



- o podpore a tejto zmluvy alebo budú mať prístup k informáciám Prevádzkovateľa základnej služby,
- c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,
 - d) sledovať hrozby dotýkajúce sa Dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
 - e) predchádzať vzniku incidentov,
 - f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,
 - g) prijímať od Prevádzkovateľa základnej služby varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu Prevádzkovateľa základnej služby,
 - h) zasielať Prevádzkovateľovi základnej služby včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto zmluvy alebo inak a
 - i) spolupracovať s Prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby.
2. Dodávateľ sa zaväzuje počas trvania tejto zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto zmluvy.
3. Zoznam pracovných rolí Dodávateľa a zoznam jeho zamestnancov, ktorí sa budú podieľať na plnení zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore a tejto zmluvy a/alebo budú mať prístup k informáciám a údajom Prevádzkovateľa základnej služby, je uvedený v prílohe č. 1. tejto zmluvy. Dodávateľ je povinný písomne oznámiť Prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení a to bezodkladne po tom, ako táto zmena v personálnom obsadení nastane; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Dodávateľ je povinný zaviazat povinnosťou mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti osoby, ktoré sa budú podieľať na plnení podľa tohto bodu.
4. Dodávateľ sa zaväzuje stanoviť postupy plnenia svojich povinností podľa tejto zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť Prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.
5. Dodávateľ sa zaväzuje prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN 150/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti.) v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.
6. Dodávateľ sa zaväzuje prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa §8, 10, 12, 14 a 15 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.



7. Dodávateľ sa zaväzuje prijať a dodržiavať sektorové bezpečnostné opatrenia v rozsahu špecifikovanom v bezpečnostných politikách Prevádzkovateľa základnej služby.

Článok VII. POSTUP PRI RIEŠENÍ INCIDENTOV

1. Dodávateľ sa zaväzuje bezodkladne hlásiť každý incident Prevádzkovateľovi základnej služby spôsobom určeným Prevádzkovateľom základnej služby, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, Dodávateľ sa zaväzuje odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ sa zaväzuje riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraňovaním incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „**reaktívne opatrenie**“). Pri riešení incidentov je Dodávateľ povinný na žiadosť Prevádzkovateľa základnej služby spolupracovať s Prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom hospodárstva Slovenskej republiky a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.
3. Dodávateľ sa zaväzuje v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní a poskytnúť ho Prevádzkovateľovi základnej služby.
4. Dodávateľ sa zaväzuje oznámiť Prevádzkovateľovi základnej služby skutočnosť, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ sa zaväzuje bezodkladne oznámiť a preukázať Prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.
6. Po vyriešení incidentu je Dodávateľ na výzvu Prevádzkovateľa základnej služby v určenej lehote povinný predložiť Prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „**ochranné opatrenia**“) na schválenie. Ak Dodávateľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je Dodávateľ povinný spolupracovať s Prevádzkovateľom základnej služby na jeho návrhu.
7. Po schválení ochranného opatrenia Prevádzkovateľom základnej služby, je Dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať. Po vykonaní ochranného opatrenia Dodávateľom, je Dodávateľ povinný preveriť jeho účinnosť.

Článok VIII. ZÁVÄZOK MLČANLIVOSTI

1. Dodávateľ sa zaväzuje zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore a



tejto zmluvy, a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka oblasti kybernetickej bezpečnosti. Dodávateľ je povinný chrániť najmä informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby. Dodávateľ je zároveň povinný chrániť všetky informácie poskytnuté Prevádzkovateľom základnej služby Dodávateľovi.

2. Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto zmluvy.
3. Výnimky z povinnosti mlčanlivosti podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.
4. Dodávateľ sa zaväzuje zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávného vzťahu, obchodného vzťahu alebo iného vzťahu.
5. Po ukončení tejto zmluvy je Dodávateľ povinný vrátiť alebo previesť na Prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto zmluvy prístup, resp. tieto podľa pokynu Prevádzkovateľa základnej služby zničiť.

Článok IX.

KONTAKTNÉ OSOBY NA ÚSEKU KYBERNETICKEJ BEZPEČNOSTI

1. Dodávateľ sa zaväzuje komunikovať pri plnení povinností podľa tejto zmluvy s Prevádzkovateľom základnej služby spôsobom určeným Prevádzkovateľom základnej služby, pričom Dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Prevádzkovateľ základnej služby určuje kontaktné osoby pre komunikáciu s Dodávateľom na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
3. Dodávateľ určuje kontaktné osoby pre komunikáciu s Prevádzkovateľom základnej služby na úseku kybernetickej bezpečnosti v prílohe č. 1 tejto zmluvy.
4. Kontaktné osoby podľa prílohy č. 1 tejto zmluvy môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme; na platnosť takejto zmeny sa nevyžaduje uzatvorenie dodatku k tejto zmluve. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia tejto zmluvy o doručovaní (článok X. bod 9., 10. a 11.).

Článok X.

SPOLOČNÉ USTANOVENIA

1. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení,



bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

2. Dodávateľ je ďalej povinný plniť povinnosti podľa tejto zmluvy v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo hospodárstva Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.
3. Dodávateľ sa zaväzuje spracovávať informácie, ktoré by mohli mať vplyv na základnú službu Prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov Prevádzkovateľa základnej služby tak, aby nebola narušená ich dostupnosť, dôverynosť, autentickosť a integrita.
4. Dodávateľ sa zaväzuje mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto zmluvy na zabezpečenom priestore tak, aby nebola narušená ich dôverynosť, autentickosť a integrita.
5. Dodávateľ sa zaväzuje dokumentovať svoju činnosť podľa tejto zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť Prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.
6. Dodávateľ sa zaväzuje plniť povinnosti podľa tejto zmluvy bezodkladne, pokiaľ to nie je v tejto zmluve alebo požiadavkách platnej legislatívy SR a EÚ stanovené inak.
7. V prípade, ak Dodávateľ plní zmluvu prostredníctvom subdodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre Prevádzkovateľa základnej služby, alebo toto plnenie priamo súvisí s prevádzkou sietí a informačných systémov Prevádzkovateľa základnej služby, Dodávateľ sa zaväzuje zabezpečiť plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tejto zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto zmluvy. Dodávateľ sa zaväzuje zabezpečiť, aby Prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto zmluvy aj u týchto subdodávateľov.
8. V prípade, ak Dodávateľ spôsobí Prevádzkovateľovi základnej služby porušením svojich povinností vyplývajúcich mu z príslušných právnych predpisov a/alebo zmluvy akúkoľvek škodu, zodpovednosť za škodu a povinnosť na náhradu takto spôsobenej škody sa bude riadiť a spravovať ustanoveniami § 373 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov. Pre odstránenie právnych pochybností, zodpovednosť Dodávateľa nevylučuje prekážka, ktorá vznikla až v čase, keď bol Dodávateľ v omeškaní s plnením svojej povinnosti alebo prekážka, ktorá vznikla z jeho hospodárskych pomerov. Za škodu sa považuje tiež ujma, ktorá vznikla Prevádzkovateľovi základnej služby tým, že musel vynaložiť náklady v dôsledku porušenia povinnosti Dodávateľom.
9. Všetky dokumenty, oznámenia, žiadosti, správy, výzvy, požiadavky a ostatné písomnosti určené druhej zmluvnej strane (ďalej len „písomnosti“) musia byť doručené, ak zmluva neustanovuje inak:



- a) v písomnej forme prostredníctvom pošty doporučené s doručenkou; za deň doručenia sa považuje dátum prevzatia zásielky alebo
- b) osobne do sídla druhej zmluvnej strany.

10. Miestom pre doručovanie písomností sú adresy zmluvných strán uvedené v záhlaví tejto zmluvy. Každá zo zmluvných strán je povinná písomne oznámiť druhej zmluvnej strane akúkoľvek zmenu ohľadne doručovania, a to najneskôr do 5 pracovných dní po tom, čo k takejto zmene dôjde. Pokiaľ sa z dôvodu oneskoreného alebo nevykonaného oznámenia o zmene miesta doručovania nepodarí včas a riadne doručiť písomnosť druhej zmluvnej strane, považuje sa deň neúspešného pokusu o opakované doručenie písomnosti za deň doručenia písomnosti druhej zmluvnej strane so všetkými právnymi dôsledkami pre dotknutú zmluvnú stranu.
11. Dodávateľ sa zaväzuje oznamovať všetky skutočnosti majúce vplyv na zmluvu, ako aj hlásiť ďalšie informácie požadované Prevádzkovateľom základnej služby, písomne na adresu sídla Prevádzkovateľa základnej služby.

Článok XI. AUDIT KYBERNETICKEJ BEZPEČNOSTI

1. Prevádzkovateľ základnej služby je oprávnený vykonať u Dodávateľa audit zameraný na overenie plnenia povinností Dodávateľa podľa tejto zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia Dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, pracovných rolí a technológií v organizačnej, personálnej a technickej oblasti u Dodávateľa pre plnenie cieľov tejto zmluvy.
2. Dodávateľ je povinný predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.
3. Prípadné nedostatky zistené auditom je Dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.
4. Prevádzkovateľ základnej služby môže audit u Dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti Prevádzkovateľa základnej služby pri výkone auditu realizuje Prevádzkovateľom základnej služby poverená tretia osoba.
5. Dodávateľ sa zaväzuje pri audite spolupracovať s 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, prípadne poskytnúť ďalšiu potrebnú súčinnosť.
6. Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom Dodávateľa, ktorí sa podieľajú na plnení úloh na úseku kybernetickej bezpečnosti podľa tejto zmluvy.



7. V rámci auditu je Dodávateľ povinný preukázať Prevádzkovateľovi základnej služby súlad s touto zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzkov a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
8. Prevádzkovateľ základnej služby sa zaväzuje oznámiť Dodávateľovi najmenej desať pracovných dní vopred svoj zámer realizovať u Dodávateľa audit. Vykonanie alebo nevykonanie auditu Prevádzkovateľom základnej služby nezaväzuje Dodávateľa zodpovednosti za plnenie povinností Dodávateľa vyplývajúcich z tejto zmluvy. Ak Dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto zmluvy.
9. Dodávateľ sa zaväzuje písomne informovať Prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované Dodávateľom.
10. Prevádzkovateľ základnej služby sa zaväzuje zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu, a ktoré nie sú verejne známe. Ustanovenia článku VIII. ods. 2, 3 a 4 tejto zmluvy sa uplatňujú primerane.
11. Prevádzkovateľ základnej služby a jeho zamestnanci pri návšteve priestorov Dodávateľa v rámci výkonu auditu musia dodržiavať pokyny Dodávateľa týkajúce sa uvedených priestorov na úseku bezpečnosti a ochrany zdravia pri práci (ďalej len „BOZP“) a ochrany pred požiarom 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 Dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne Dodávateľ. Dodávateľ sa zaväzuje preukázateľne informovať zamestnancov Prevádzkovateľa základnej služby o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch Dodávateľa môžu vyskytnúť a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal Dodávateľ 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 Dodávateľa.

Článok XII. ZÁVEREČNÉ USTANOVENIA

1. Táto zmluva sa uzatvára na dobu určitú, a to na dobu trvania zmluvy o dielo / o poskytovaní služieb / o prevádzke informačného systému / o podpore alebo iného jej ukončenia.
2. Prevádzkovateľ základnej služby je oprávnený od tejto zmluvy písomne odstúpiť v prípadoch:
 - a) podstatného porušenia tejto zmluvy zo strany Dodávateľa;
 - b) ak je na Dodávateľa vyhlásený konkurz, alebo bola povolená reštrukturalizácia, alebo ak bolo vyhlásenie konkurzu odmietnuté alebo zrušené pre nedostatok majetku;
 - c) ak je Dodávateľ v likvidácii.



Odstúpenie od tejto zmluvy je platné a účinné dňom preukázateľného doručenia písomného odstúpenia od tejto zmluvy Dodávateľovi.

3. Za podstatné porušenie zmluvy sa považuje:

- a) porušenie povinností dodávateľom uvedených v čl. IV ods. 1, 8, čl. VI. ods. 3, 4, čl. VII a čl. VIII tejto zmluvy;
- b) konanie Dodávateľa, ktorý už v čase uzavretia zmluvy vedel alebo v tomto čase mohol predvídať s prihliadnutím na účel zmluvy, ktorý vyplynul z jej obsahu alebo z okolností, za ktorých bola zmluva uzavretá, že nedodrží, poruší a/alebo nebude plniť zmluvnú povinnosť dojednanú touto zmluvou a to bez ohľadu na to, či ide o zmluvnú povinnosť uvedenú v predchádzajúcom písm. a) a je zrejmé, že Prevádzkovateľ základnej služby by nemal záujem uzatvoriť túto zmluvu pri takom porušení zmluvy;
- c) Dodávateľ neposkytne potrebnú súčinnosť v zmysle tejto zmluvy.

4. Túto zmluvu je možné vypovedať Prevádzkovateľom základnej služby písomnou výpoveďou, aj bez uvedenia dôvodu s výpovednou dobou 1 mesiac, ktorá začína plynúť prvým dňom mesiaca nasledujúceho po mesiaci, v ktorom bola výpoveď doručená Dodávateľovi.

5. Zmluvné strany sa dohodli, že túto zmluvu je možné ukončiť aj písomnou dohodou zmluvných strán. V tomto prípade zmluva zaniká ku dňu, ktorý bude v tejto dohode určený ako deň zániku zmluvy. Ak takýto deň určený nie je, táto zmluva zaniká ku dňu nadobudnutia účinnosti takejto dohody.

6. Zrušenie tejto zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zrušení tejto zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto zmluvy.

7. Po ukončení tejto zmluvy je Dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na Prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby Prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto zmluvy.

8. Táto zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy výslovne neupravené touto zmluvou sa riadia príslušnými ustanoveniami Obchodného zákonníka a ostatnými súvisiacimi všeobecne záväznými právnymi predpismi.

9. Prípadné spory vyplývajúce z tejto zmluvy budú riešené predovšetkým mimosúdne. Podpisom tejto zmluvy zmluvné strany potvrdzujú, že na riešenie prípadných sporov z tejto zmluvy sú príslušné súdy Slovenskej republiky.

10. Táto zmluva sa môže meniť, dopĺňať alebo ukončiť iba dohodou zmluvných strán v písomnej forme, ak zo zmluvy nevyplýva niečo iné.

11. Žiadna zo zmluvných strán nie je oprávnená postúpiť svoje práva a povinnosti podľa tejto zmluvy na inú osobu bez predchádzajúceho písomného súhlasu druhej zmluvnej strany.

12. Ak niektoré ustanovenia tejto zmluvy budú zmluvné strany, súd alebo iné kompetentné orgány považovať za neplatné alebo nevymáhateľné, potom takéto ustanovenie bude neplatné iba v



dotknutom a v najužšom možnom rozsahu, pričom jeho zvyšná časť, význam a dopady, ako aj ostatné ustanovenia tejto zmluvy zostávajú v platnosti. Zmluvné strany budú v takom prípade postupovať tak, aby účel ustanovení považovaných za nevymáhateľné alebo neplatné bol v maximálne možnej miere rešpektovaný a pre zmluvné strany právne záväzný vo forme umožňujúcej jeho právnu vymáhateľnosť.

13. Táto zmluva tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto zmluvy zanikajú všetky predchádzajúce písomné a ústne zmluvy súvisiace s predmetom tejto zmluvy a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych, v tejto zmluve neuvedených, ústnych alebo písomných dojednaní a dohôd.
14. Táto zmluva bola vyhotovená v šiestich rovnopisoch, a to v štyroch rovnopisoch pre Prevádzkovateľa základnej služby a vo dvoch rovnopisoch pre Dodávateľa.
15. Zmluvné strany berú na vedomie, že Prevádzkovateľ základnej služby je v zmysle § 2 ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou, a preto je táto zmluva v zmysle § 5a tohto zákona v spojení s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov povinne zverejňovanou zmluvou.
16. Táto zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády SR.
17. Neoddeliteľnou súčasťou tejto zmluvy sú jej prílohy:
 - Príloha č. 1 – Zoznam pracovných rolí a kontaktov Prevádzkovateľa základnej služby a Dodávateľa
 - Príloha č. 2 - Bezpečnostné opatrenia v organizácii Prevádzkovateľa základnej služby, ktoré sa vzťahujú na Dodávateľa,
 - Príloha č. 3 – Zoznam subdodávateľov
18. Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah zmluvy dôkladne prečítali, a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu a na znak súhlasu ju podpisujú.

V Bratislave dňa ____.

V

dňa

____.

Prevádzkovateľ základnej služby:

Dodávateľ:



KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

ODBOR PRÁVNÝCH SLUŽIEB A VEREJNÉHO OBSTARÁVANIA

***Kancelária Národnej
rady SR***

(obchodné meno)

(štatutár)

(funkcia)



Príloha 1: Zoznam pracovných rolí a kontaktov prevádzkovateľa základnej služby a dodávateľa - VZOR

Prevádzkovateľ základnej služby:

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
	GB	Riadenie informačnej bezpečnosti		
	Riaditeľ OIT	Riadenie procesov		
	Vedúci oddelenia BASS	Zodpovednosť sa chod projektu / implementáciu projektu		

Meno a priezvisko	Rola	Proces súvisiaci s prevádzkou ZS	Telefónny kontakt	Email
	DB administrátor	Správa DB systému		
	NET administrátor	Administrácia časti siete, konfigurácia sieťových prvkov		
	Security operátor	Správa a konfigurácia bezpečnostných prvkov (firewall, VPN koncentrátor)		
	Helpdesk operátor	Riešenie problémov používateľov PC, problémov s funkčnosťou aplikácie		



Príloha č. 2:

Bezpečnostné opatrenia v organizácii Prevádzkovateľa základnej služby, ktoré sa vzťahujú na Dodávateľa:



KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

ODBOR PRÁVNÝCH SLUŽIEB A VEREJNÉHO OBSTARÁVANIA

Príloha č. 3:

Zoznam subdodávateľov: