

Príloha č. 1 – Parametre a podmienky poskytovania Služieb

Obsah prílohy

1. Opis súčasného stavu
2. Služby podpory prevádzky
 - 2.1. Zoznam činností vykonávaných v rámci Služieb podpory prevádzky
 - 2.2. Helpdesk
 - 2.3. Postup pri riešení problémov/požiadaviek
 - 2.4. Parametre kvality poskytovanej služby
 - 2.5. Akceptačné konanie
3. Služby rozvoja
 - 3.1. Postup objednania Služby rozvoja
 - 3.2. Parametre kvality poskytovanej služby
 - 3.3. Akceptačné konanie
 - 3.4. Hodnotenie kvality poskytnutej služby

1. Opis súčasného stavu

IS ESS v súčasnosti zabezpečuje základné funkcionality potrebné pre poskytovanie, správu a archiváciu spisu v plne elektronickej podobe. V jeho bezpečnom úložisku na báze produktu DS-LTA sú aktuálne uložené všetky elektronické dokumenty vznikajúce počas životného cyklu spisu. Dokumenty vznikajú v Súdnom manažmente, môžu byť doručené cez elektronické schránky UPVS alebo byť doručené ako papierové podania na podateľňu. Tieto sú následne skenované v centrálnom skenovacom module Ephesoft, je z nich vyťažený text a následne sú uložené do vo forme metadát do modulu ESS a ako binárny dokument do modulu DS-LTA. Posledným vstupom do systému je externý IS MonoReCourt, ktorý zabezpečuje aby audio nahrávky súdnych pojednávaní boli v štandardizovanej podobe takisto uložené v ESS a DS-LTA. Systém zároveň zabezpečuje integračné rozhrania, ktoré je možné použiť na integráciu s ďalšími systémami v rámci domény súdnictva.

Organizačný pohľad (Business architektúra)

Používatelia systému IS ESS

Súdy

Sudcovia a oprávnení súdni úradníci môžu pristupovať do IS ESS priamo z ich prostredia agendového systému Súdny manažment. Sudcovia majú prístup ku všetkým dokumentom, ktoré sa dostali z vyššie popísaných zdrojov do spisu. Riadenie prístupu k jednotlivým spisom je na strane Súdneho manažmentu, IS ESS overuje len identitu prihláseného používateľa v AD a porovnáva s identitou zaslanou Súdny manažmentom.

Administrátori

Správcovia môžu po úspešnom s doménovým účtom pristupovať k správcovskému prostrediu, ktoré je rozdelené na 3 sekcie:

- Správa prístupov
- Správa číselníkov
- Prezeranie logov.

Verejnosť a iné prístupy

Verejnosť nemá prístup do IS ESS. Do IS ESS nie je možné vstupovať len v internom LAN prostredí MS SR a okresných a krajských súdov.

Používatelia systému Ephesoft

Aplikácia Ephesoft je určená pre zamestnancov skenovacieho pracoviska a administrátorom. Prístupové oprávnenia a zodpovednosti jednotlivých používateľov sú definované podľa rolí.

Používateľ v roli „Súdny operátor“ je zodpovedný za obsluhu skenera a následnú validáciu spracovávanej dávky v systéme Ephesoft. Po ukončení validácie systém odošle dávku do aplikácie IS ESS.

Používateľ v roli administrátor (na úrovni okresného, krajského súdu alebo centrálny administrátor) je zodpovedný za prvotné pripojenie skenera, kontrolu spracovania dávok a odstraňovanie chýb. Takisto majú možnosť vidieť a riešiť skenované dávky na podriadených jednotkách, reporty a na vyžiadanie zamestnanca môže administrátor nastaviť vyššiu prioritu pre spracovanie konkrétnej dávky.

Moduly IS ESS

IS ESS poskytuje v jednotlivých moduloch nasledovné služby:

MODUL IS ESS

Informačný systém ESS je realizovaný ako čiastočne distribuovaný, pričom na krajskej úrovni je umiestnený ESS Kraj, ktorý zabezpečuje replikáciu metadát spisov, dokumentov ako aj samotných uložených dokumentov na ESS Centrála a v prípade požiadavky z iného kraja z ESS Centrála na ESS kraj.

ESS na úrovni ESS Kraj využíva služby:

- DIG Digitalizácia papierových dokumentov
- DS LTA Elektronický archív súdov
- Antivírusová kontrola - v prípade dostupnosti
- Adresárové služby – v prípade dostupnosti
- PKI – v prípade dostupnosti

ESS poskytuje nasledovné služby:

- Prístup k spisu a uloženým dokumentom
- Uloženie spisu a dokumentu
- Správa prístupových práv
- Správa číselníkov
- Replikácia metadát Spisu, Dokumentu a Dokumentov medzi Krajom a Centrálou

Primárny prístup k informačnému systému ESS je realizovaný prostredníctvom volania z informačného systému Súdny manažment. Informačný systém súdny manažment volá IS ESS prostredníctvom dohodnutých webových služieb, pričom IS ESS vráti IS Súdny manažment URL slúžiacu pre zobrazenie požadovaných dát (Spisu, Skenovaných dokumentov, ...).

Pri zasielaní požiadavky prostredníctvom webových služieb, zašle IS Súdny manažment aj informáciu o prihlásenom používateľovi a jeho právach v rámci príslušnej požadovanej operácie. Túto pre účely auditu operácií ako aj práva prístupu IS ESS považuje za dôveryhodnú s ohľadom na aktuálne technologické riešenie IS Súdny manažment.

Priamy prístup prostredníctvom web rozhrania pre účely administrácie, správy číselníkov, prezeranie logov a žurnálu, predpokladaná autentifikácia používateľa voči MS Active Directory, resp. službám LDAP.

Informačný systém ESS je podľa zadania vyvinutý s použitím technológie ASP.NET. Verzia platformy .NET použitá pre vývoj bude 4.5. Pri vývoji bola použitá architektúra ASP.NET MVC 4, ako ORM vrstva je použitý Microsoft Entity Framework. Implementácia webových služieb je realizovaná s technológiou Windows Communication Foundation (WCF) a modulu Microsoft AppFabric s použitím protokolu SOAP 1.2 a SOAP 1.1. Aktuálne nasadená verzia ma implementované rozšírenie, ktoré všetky nové dokumenty, skeny alebo audionahrávky, ktoré sú zreplikované na centrálu, automaticky odošle do úložiska UBUS (externý systém v rámci MS SR).

MODUL DS-LTA

Cieľom systému DS-LTA je poskytnúť systému Elektronického súdneho spisu (ESS) službu centrálného a dočasného úložiska elektronických dokumentov, ktoré sú neoddeliteľnou súčasťou

elektronického súdneho spisu. Systém DS-LTA zavádza základné procesy pre dlhodobé uchovanie dokumentov s možnosťou ich overenia a kontroly.

Kľúčové vlastnosti systému DS-LTA

- **Centrálne ukladanie dokumentov elektronického súdneho spisu.**
Systém DS-LTA zabezpečuje uloženie všetkých elektronických dokumentov elektronického súdneho spisu v centrálnej lokalite MS SR. Dokumenty do systému vstupujú zo systému ESS z centrálnej lokality.
- **Centrálny prístup k dokumentom elektronického súdneho spisu**
Systém DS-LTA zabezpečuje dostupnosť elektronických dokumentov v centrálnej lokalite MS SR. Dokumenty sú prístupné pre systém ESS v centrálnej lokalite.
- **Dočasné ukladanie dokumentov elektronického súdneho spisu**
Systém DS-LTA zabezpečuje ukladanie elektronických dokumentov elektronického súdneho spisu v lokalite krajov MS SR. Dokumenty do systému vstupujú iba zo systému ESS v tej istej lokalite kraja.
- **Dočasný prístup k dokumentom elektronického súdneho spisu**
Systém DS-LTA zabezpečuje dostupnosť elektronických dokumentov v lokalite kraja MS SR. Dokumenty sú prístupné iba pre systém ESS v tej istej lokalite kraja.
- **Archivovanie elektronických dokumentov**
Z dokumentov uložených v centrálnej lokalite MS SR, na základe požiadavky ESS, sú vytvorené archivne balíky AIP (OAIS) tak, aby mohli byť dlhodobo archivované v externých systémoch. Po archivovaní dokumenty budú naďalej on-line dostupné pre systém ESS v centrálnej lokalite MS SR.
AIP Exchange nie je súčasťou tohto riešenia.
- **Ukladanie metadát** - Ku každému elektronickému dokumentu je možné uložiť vopred definované doplnkové údaje vo forme metadát.
- **Kontrola prístupu** - Systém zabezpečuje dostupnosť dokumentov iba pre systém ESS pomocou zabezpečeného spojenia tak, aby bol vylúčený neautorizovaný prístup k elektronickému dokumentu zo strany iných systémov, ako aj zo strany neoprávnených osôb. Zároveň je zabezpečený prístup k službám DS-LTA iba zo systému ESS v tej istej lokalite. Zabezpečenie prístupu je na infraštruktúrnej úrovni a aj na aplikačnej úrovni.

Kontrola prístupu spĺňa požiadavky na uloženie elektronických dokumentov obsahujúce:

- Osobné údaje
- Citlivé údaje (nie utajované skutočnosti)
- Elektronické dokumenty podpísané EP (ZEP)
- Kontrola integrity

V systéme DS-LTA sú byť mechanizmy na zabezpečenie integrity uložených elektronických dokumentov a metadát. Systém ESS pri každej operácii nad dokumentom overuje integritu uloženého dokumentu voči centrálnemu DS-LTA.

- **Ochrana uložených informácií**

Informácie sú uložené v nečitateľnej podobe. Sú zavedené príslušné kryptografické operácie, aby sa zabránilo zneužitiu ako citlivých tak osobných údajov.

- **Škodlivý SW**

V systéme DS-LTA sú zavedené procesy na kontrolu obsahu škodlivého SW. Výsledok kontroly je zaznamenaný v žurnále.

- **Auditovateľnosť**

Všetky informácie o operáciách a stave systému sú v čase vysledovateľné a dostupné pre kontrolné činnosti.

- Sledovanie systému

Systém umožňuje cez UI sledovanie kritických parametrov ako napríklad:

- Kapacita systému
 - o Obsadená
 - o Dostupná
- Zaťaženie systému

Priama integrácia so systém ESS (jeho službami) je vytvorená pomocou zabezpečeného komunikačného kanála tak aby sa dala overiť ako identita systému DS-LTA v systéme ESS tak aj systému ESS v systéme DS-LTA. V opačnom prípade je komunikácia odmietnutá a vytvorená príslušná notifikácia. Údaje prenášané v infraštruktúre sú v nečitateľnej podobe (kryptograficky).

MODUL Ephesoft

Modul Ephesoft je centrálné riešenie, určené na skenovanie a vyťažovanie dokumentov, ktoré k jednotlivým spisom boli doručené na súd v papierovej podobe. Riešenie je na báze produktu Ephesoft Transact, aktuálne je inštalovaná verzia ročného subscription pre 16 cores.

Implementácia je nasadená ako centralizované riešenie, ktoré nevyžaduje žiadne lokálne okresné, ani krajské inštalácie skenovacích klientov. Spracovanie dokumentov pre potreby MS SR a súdov sa realizuje lokálne, cez tenkého webového klienta.

MODUL MonoReCourt

Aplikácia MonoReCourt Klient slúži na spracovanie multimediálnych nahrávok, ktoré vzniknú pri pojednávaní v jednotlivých súdnych miestnostiach. Celá aplikácia je preto navrhnutá ako sled obrazoviek, ktoré predstavujú jednotlivé kroky spracovania multimediálnych nahrávok. V každom kroku je používateľovi krátkym popisom naznačené, čo sa od neho očakáva a aplikácia nepokračuje ďalej pokiaľ nie sú splnené všetky podmienky na pokračovanie.

Klientska aplikácia úzko spolupracuje so serverom na lokálnom súde aj s centrálnym serverom na ministerstve, preto je nutné pripojenie na obidva servery počas práce. Nie je možná práca bez pripojenia, pretože nahrávky spolu s metadáta musia byť odoslané na server pre ďalšie spracovanie, aby bol celkový proces spracovania korektne ukončený.

Aplikácia je taktiež úzko naviazaná na externý systém, od ktorého čerpá dáta ku konkrétnemu pojednávaniu. Preto nie je možné aplikáciu používať bez spustenia z tohto externého systému.

Architektúra je podobne ako pri IS ESS decentralizovaná, t.j. každý kraj ma jeden server, na ktorom sa zhromažďujú audionahrávky z jednotlivých klientov a posielajú sa do IS ESS.

2. Služby podpory prevádzky

Služby podpory prevádzky zahŕňajú zabezpečovanie bežnej servisnej podpory, ako aj poskytovanie podpory pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky IS Obstarávateľa v súlade s aktuálnymi platnými požiadavkami, vrátane riešenia Problémov.

Rozšírený popis Služby:

- a) odstraňovanie Problémov, resp. poskytnutie dočasného náhradného riešenia pri ich riešení,

- b) poskytnutie služieb v súvislosti s posudzovaním a riešením Problémov IS Objednávateľa, ktoré boli spôsobené nesprávnym fungovaním IS Objednávateľa,
- c) pravidelná kontrola funkčnosti IS Objednávateľa a jeho častí (monitorovanie systému),
- d) pravidelná kontrola nastavenia IS Objednávateľa podľa posledného odsúhlaseného stavu konfigurácie IS Objednávateľa,
- e) profylaktické práce v rozsahu definovanom prevádzkovou dokumentáciou IS Objednávateľa,
- f) kontrola a vyhodnocovanie záznamov z aplikačných logov,
- g) proaktívne upozorňovanie Objednávateľa Poskytovateľom na vhodné úpravy a zmeny IS Objednávateľa,
- h) proaktívne upozorňovanie Objednávateľa Poskytovateľom na vzniknuté Problémy, ako aj stavy IS Objednávateľa, pri ktorých môže dôjsť, resp. ktoré môžu viesť k vzniku Problémov,
- i) drobné požiadavky na zmenu.

2.1. Zoznam činností vykonávaných v rámci Služieb podpory prevádzky

Služby podpory prevádzky zahŕňajú nasledovné činnosti:

- a) riadenie a poskytovanie servisných služieb a činností Helpdesku, prostredníctvom ESSP
- b) zber a vedenie evidencie a štatistiky nahlásených Problémov,
- c) prevádzka hot-line a strediska Helpdesku za účelom garantovania parametrov SLA,
- d) identifikácia Problému, jeho analýza a samotné riešenie/neutralizácia;
 - i. analýza a poskytovanie súčinnosti pri riešení problému – t.j. podpora poskytnutá Objednávateľovi pri neutralizácii identifikovateľného Problému; Poskytnutie podpory a odporúčaní na predchádzanie Problémom pre prevádzkové účely v rozsahu IS Objednávateľa,
 - ii. neutralizácia Problému znamená odstránenie stavu obmedzujúceho alebo znemožňujúceho používanie IS Objednávateľa, a to obnovou funkčnosti IS Objednávateľa, ktorá bola obmedzená a/alebo úpravou/ zosúladením fungovania IS Objednávateľa s dodanou dokumentáciou IS Objednávateľa podľa ÚSP uvedenej v ods. 2.4. tejto Prílohy č. 1,
- e) poskytovanie konzultácií o Problémoch,
- f) poskytovanie mailového/telefonického Helpdesku,
- g) projektové riadenie servisných činností,
- h) riešenie eskalácií,
- i) poskytovanie logových záznamov, reportov a hlásení
- j) podpora a konzultácie správcov systému pri neštandardnom správaní sa IS Objednávateľa, pri údržbe databáz a aplikačných serverov, pri výpadku aplikačných serverov spôsobených aplikáciou,
- k) profylaktika aplikačnej vrstvy – tieto činnosti sú realizované pravidelne na mesačnej báze a zahŕňajú nasledovné:
 - i. pravidelná kontrola funkčnosti aplikácie, softvérového vybavenia,
 - ii. pravidelná kontrola parametrov systému definovaných v akceptačných a výkonnostných testoch,
 - iii. kontrola a vyhodnocovanie záznamov zo systémových logov, aplikačných logov,
 - iv. kontrola prostredia, v ktorom beží IS Objednávateľa,
 - v. udržiavanie dokumentácie po každej zmene aplikácie alebo konfigurácie IS v rozsahu podpory v aktuálnosti – inštaláčnej, prevádzkovej, administrátorskej a užívateľskej,
- l) reportovanie zamerané na spracovávanie požadovaných reportov o Problémoch a operatívnych informácií o ich riešení.

2.2. Helpdesk

Na hlásenie problémov zo strany Objednávateľa bude Poskytovateľ prevádzkovať Helpdesk, ktorý bude poskytovať službu tímu druhoúrovňovej podpory (L2), ktorá pozostáva z nasledujúcich činností:

- a) Identifikácia Problému – poskytnutie pomoci Objednávateľovi s cieľom identifikovať príčinu daného Problému v rozsahu podporovaného IS Objednávateľa,
- b) Poskytovanie informácií o stave riešenia požiadaviek prostredníctvom on-line vzdialeného prístupu oprávnených osôb Objednávateľa do ESSP.

2.3. Postup pri riešení problémov/požiadaviek

1. Oprávnená osoba Objednávateľa hlási problém/požiadavku najmä v systéme ESSP na adrese: sd@ikanc.eu, v prípade nedostupnosti systému e-mailom na adresu: sd@ikanc.eu a/alebo telefonicky na +421 (2) 20 90 35 00. Oprávnená osoba Objednávateľa nahlasuje problém podľa predchádzajúcej vety Poskytovateľovi až potom, ako nebolo možné vyriešiť tento problém v prvom stupni Oprávnenou osobou Objednávateľa. Uskutočniť takéto hlásenie môže výlučne Oprávnená osoba Objednávateľa oznámená v súlade s postupom uvedeným v Servisnej zmlúve. Každé hlásenie prijaté akýmkoľvek spôsobom sa zaeviduje v ESSP. Tento informačný systém vygeneruje identifikačné číslo požiadavky/problému. Informačný systém eviduje minimálne: čas odoslania hlásenia a oprávnenú osobu, kritickosť, čas prijatia hlásenia oprávnenou osobou Poskytovateľa, čas pridelenia riešiteľovi, čas zahájenia riešenia, čas vyriešenia požiadavky/problému, stav požiadavky/problému, názov a popis požiadavky/problému. Akákoľvek budúca komunikácia medzi Poskytovateľom a Objednávateľom sa uskutočňuje použitím priradeného identifikačného čísla požiadavky/Problému. Všetky záznamy, prílohy a komunikácia Oprávnených osôb Poskytovateľa a Objednávateľa sú evidované najmä v ESSP dostupnom on-line. Systém vyhodnocuje i čas spracovania udalostí a hlásení, pre účely Servisnej zmluvy.
2. Službukonajúci špecialista Poskytovateľa preverí požiadavku/Problém a začne ich prešetrenie. Podľa potreby kontaktuje Oprávnenú osobu Objednávateľa. Komunikácia pracovníka Poskytovateľa prebieha priamo s Oprávnenou osobou Objednávateľa. Službukonajúci špecialista Poskytovateľa oznámi výsledok prešetrenia a odporúčané riešenie Oprávnenej osobe Objednávateľa. Na základe výsledkov prešetrenia bude pokračovať riešenie Problému.
3. Problém bude riešený na základe priority určenej dohodou a definíciou kritickosti Oprávnenými osobami Objednávateľa a Poskytovateľa. Oprávnená osoba Objednávateľa má právo zmeniť poradie priorít riešenia otvorených Problémov/požiadaviek po dohode s oprávneným zástupcom zo strany Poskytovateľa dokumentovateľným spôsobom – záznamom v ESSP.
4. Po vykonaní prác podpory (aj čiastkových) pracovníkom Poskytovateľa v priestoroch Objednávateľa potvrdí poskytnutie a funkčnosť riešenia v ESSP.
5. Všetky vyriešené požiadavky/Problémy Objednávateľa musia byť potvrdené a ich vyriešenie musí byť zaevidované v ESSP. Splnenie požiadavky/Problému bude potvrdené v rozsahu ich riešenia Oprávnenou osobou Objednávateľa. Objednávateľ je povinný potvrdiť vyriešenie každej požiadavky/Problému najneskôr do 5 pracovných dní odo dňa jej vyriešenia. Akceptovanie riešenia požiadavky/Problému bude zaevidované priamo v ESSP. V prípade, ak Objednávateľ riešenie požiadavky/Problému neakceptuje, v rovnakej lehote svoje pripomienky a výhrady uvedie v ESSP. Ak Objednávateľ bez závažného dôvodu neakceptuje vyriešenie požiadavky/Problému a ani nevznesie pripomienky k riešeniu požiadavky/Problému ani do 5 pracovných dní od ich vykonania, považuje sa riešenie požiadavky/Problému za akceptované a ESSP vykoná mailovú notifikáciu.
6. Ak je súčasne riešená kritická a nižšia úroveň Problému, doba neutralizácie Závažného problému a Nekritického problému sa predlžuje o dobu riešenia Kritického problému, maximálne však o dobu neutralizácie Kritického problému definovaného príslušnou USP podľa ods. 2.4. tejto Prílohy č. 1 Servisnej zmluvy. Doba neutralizácie Kritického problému nie je ovplyvňovaná počtom otvorených Kritických problémov.

2.4. Parametre kvality poskytovanej služby

Reakčná doba Poskytovateľa na problém Objednávateľa sa určuje na základe príslušnej úrovne spracovania požiadaviek. Poskytovateľ poskytuje Služby podpory prevádzky na základnej úrovni

spracovania požiadaviek. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do ESSP alebo v prípade nedostupnosti ESSP od momentu nahlásenia Problému alternatívnym spôsobom v zmysle ods. 2.3. bod 1 tohto článku Prílohy č. 1 Servisnej zmluvy, t. j. od momentu doručenia hlásenia Problému emailom alebo nahlásením Problému telefonicky.

Dostupnosť služieb IS Objednávateľa:

Popis	Parameter	Poznámka
Prevádzkové hodiny podpory	8 hod.	08:00 – 16:00 hod
Servisné okno	11 hod.	20:00 – 07:00 počas pracovných dní
	24 hod	0:00 – 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov

Tabuľka č. 1

Úroveň spracovania požiadaviek - ÚSP:

Pracovné hodiny Služieb podpory prevádzky Poskytovateľa sú počas pracovných dní < 08:00; 16:00> (5x8). Čas mimo pracovné hodiny podľa predchádzajúcej vety sa do Reakčnej doby ani do Doby neutralizácie problému nezapočítava.

Typ požiadavky	Reakčná doba v pracovných hodinách	Doba neutralizácie problému v pracovných hodinách
Kritický problém	2	8
Závažný problém	4	16
Nekritický problém	8	40

Tabuľka č. 2

Zľava z ceny

Výška zľavy	Hodnota problémov (x)
5 %	$x > 10$
10 %	$x > 15$
15 %	$x > 21$
20 %	$x > 27$
25 %	$x > 33$
30 %	$x > 39$
35 %	$x > 45$
40 %	$x > 51$
45 %	$x > 57$
50 %	$x > 63$

Tabuľka č. 3

Hodnota problémov („x“) v Tabuľke č. 3 sa vypočíta podľa vzorca:

$x = [\text{počet kritických problémov v príslušnom kalendárnom mesiaci} \times 5] + [\text{počet závažných problémov v príslušnom kalendárnom mesiaci} \times 3]$

Výška zľavy závisí od počtu Problémov, ktoré sa v danom kalendárnom mesiaci vyskytli, pričom do počtu Problémov určujúcich výšku zľavy z ceny sa nezapočítavajú Problémy, ktoré vznikli:

- následkom okolností vylučujúcich zodpovednosť v zmysle § 374 ods. 1 Obchodného zákonníka,
- nesprávnou alebo neautorizovanou modifikáciou IS Objednávateľa (HW komponentov, Komponentov SW komponentu, SW produktov 3. strany) vykonanou Objednávateľom bez vedomia Poskytovateľa alebo
- nedodržaním odporúčaných postupov Objednávateľom, ktoré sú uvedené v prevádzkovej dokumentácii alebo nesprávnym používaním zo strany Objednávateľa,
- v dôsledku výpadku fungovania HW komponentu alebo SW produktu 3. strany, s výnimkou prípadov, ak k takémuto výpadku došlo z dôvodu porušenia povinností Poskytovateľa v zmysle tejto Servisnej zmluvy.

2.5. Akceptačné konanie

Poskytovateľ sa zaväzuje poskytovať Služby podpory prevádzky sústavne počas trvania Servisnej zmluvy, pričom akceptácia tohto plnenia je vykonaná automaticky na mesačnej báze na konci daného mesiaca na podklade reportu (výkazu) o vykonaných Službách podpory prevádzky a reportu o profylaktických činnostiach (ďalej len „Report“), ktorý Poskytovateľ doručí Objednávateľovi najskôr v posledný deň príslušného kalendárneho mesiaca. Objednávateľ je oprávnený zaslať pripomienky k poskytnutým Službám podpory prevádzky, resp. ku kvalite a úplnosti ich poskytnutia, v lehote 5 (piatich) pracovných dní od doručenia Reportu. Poskytovateľ je povinný sa k pripomienkam Objednávateľa vyjadriť, ak nie je možné niektorú z pripomienok Objednávateľa akceptovať, Poskytovateľ túto skutočnosť bezodkladne oznámi a vysvetlí Objednávateľovi.

Fakturácia je vykonávaná mesačne, pričom prílohou faktúry je report (výkaz) o vykonaných Službách podpory prevádzky obsahujúci štatistiku (prehľad) a parametre poskytnutých služieb (vrátane údajov o rozsahu čerpaných človekohodín na drobné požiadavky na zmenu), minimálne v rozsahu podľa ods. 2.3. bod 1 tejto Prílohy č. 1 Servisnej zmluvy.

Report o profylaktických činnostiach

Pri reportovaní profylaktických činností bude záznam obsahovať minimálne nasledovné položky:

Identifikácia komponentu prípadne funkčnej časti IS Objednávateľa, na ktorom sa profylaktické činnosti vykonávali. Popis činností, ktoré sa vykonali:

- časový interval, kedy a akým spôsobom sa zásah vykonával,
- popis činnosti.

Report profylaktických činností predstavuje prehľad paušálnych činností vykonaných v príslušnom období a nie je predmetom schvaľovania ani hodnotenia úrovne poskytovania služieb.

3. Služby rozvoja

Služby rozvoja zahŕňajú zmeny funkčnosti IS Objednávateľa, ktoré vyplývajú z legislatívnych zmien alebo z novo vzniknutých potrieb Objednávateľa, zmeny funkčnosti, konfigurácie a nastavení IS Objednávateľa, ktoré sú vynútené novými zmenami prevádzkového prostredia Objednávateľa a aktualizácia príslušnej dokumentácie k IS Objednávateľa na základe týchto zmien.

3.1. Postup objednania Služby rozvoja

Proces objednania Služby rozvoja sa začína vytvorením Požiadavky na zmenu a jej predložením Poskytovateľovi. Požiadavku na zmenu je oprávnená predložiť len Oprávnená osoba Objednávateľa. Jednotný formulár Požiadavky na zmenu je uvedený v Prílohe č. 2 – Formulár požiadavky na zmenu.

Na základe Požiadavky na zmenu Poskytovateľ vypracuje záväzný rozpočet realizácie zmeny vo forme Cenovej kalkulácie, ktorej prílohou bude:

- vlastná cenová kalkulácia –
 - v prípade požiadavky na zmenu v menšom rozsahu bude predložená cenová kalkulácia na realizáciu zmeny,
 - v prípade komplexnej požiadavky na zmenu bude najprv predložená cenová kalkulácia na analýzu zmeny, následne po odsúhlasení oprávnenými osobami a vykonaní analýzy bude predložená cenová kalkulácia na realizáciu zmeny.
- podrobný návrh riešenia vo forme Štúdie realizovateľnosti a analýzu dopadu, v ktorej bude uvedené, ktoré iné časti funkčnosti IS Objednávateľa budú ovplyvnené realizáciou zmeny,
- predpokladaný harmonogram prác s uvedením navrhovanej doby odovzdania zmeny vo forme Plánu realizácie zmeny, ktorého súčasťou bude aj špecifikácia Akceptačných testov zmeny.

Do 5 (piatich) pracovných dní odo dňa doručenia Cenovej kalkulácie Objednávateľ písomne oznámi Poskytovateľovi svoje rozhodnutie, a to:

- v prípade schválenia Cenovej kalkulácie doručí Poskytovateľovi záväznú písomnú objednávku podpísanú oprávnenou osobou,
- v prípade neschválenia Cenovej kalkulácie doručí Poskytovateľovi písomné oznámenie o neschválení.

K realizácii Služby rozvoja Poskytovateľom dôjde až po prijatí záväznej písomnej objednávky. Neoddeliteľnou súčasťou objednávky bude aj Cenová kalkulácia, vrátane jej príloh.

V prípade, že Objednávateľ vo svojom písomnom vyjadrení nebude súhlasiť s Cenovou kalkuláciou Poskytovateľa a nedôjde ani k doručeniu písomnej záväznej objednávky Objednávateľa Poskytovateľovi v lehote uvedenej vyššie, Požiadavka na zmenu nebude realizovaná, pokiaľ sa Zmluvné strany vzájomne písomne nedohodnú inak.

Počas realizácie zmeny bude Poskytovateľ pravidelne aktualizovať a predkladať Objednávateľovi Plán realizácie zmeny spolu s odpočtom vykonaných prác, a to vždy k prvému dňu mesiaca nasledujúceho po prijatí písomnej objednávky Objednávateľa, až do dňa podpisu akceptačného protokolu alebo písomného odôvodnenia Objednávateľa o neakceptovaní požadovaných služieb.

3.2. Parametre kvality poskytovanej služby

V rámci Akceptačného testovania Objednávateľ overí súlad dodaného Komponentu s funkčnosťou uvedenou v objednávke a jej prílohách. Pre zamedzenie pochybností v prípade, že je pre realizáciu rozvoja nevyhnutná spoluúčasť tretej strany, súčasťou akceptačného testovania musí byť aj overenie

konektivity a potvrdenie funkčnosti dodaného komponentu treťou stranou. Minimálna vyžadovaná úroveň poskytnutia Služby rozvoja je stanovená počtom a závažnosťou Defektov zistených v rámci Akceptačného testovania tak, ako je to uvedené v nasledujúcej tabuľke.

Kategória	Popis	Povolený počet Defektov
Kritická	Defekt s dopadom na základné funkcionality IS Objednávateľa, ktorý by v prípade výskytu v produkčnom prostredí znemožnil prevádzku IS Objednávateľa, resp. v testovacom prostredí zastaví postup testov. Výrazná odchýlka od požadovanej funkčnosti uvedenej v schválenej Cenovej kalkulácii.	0
Normálna	Defekt s nepodstatným dopadom na obsluhu IS Objednávateľa, resp. bez dopadu na postup testov v testovacom prostredí.	3

Zistenie väčšieho počtu Defektov kategórie Normálna alebo akéhokoľvek Defektu kategórie Kritická znamená, že Poskytovateľ nedosiahol minimálnu vyžadovanú úroveň poskytovanej služby.

3.3. Akceptačné konanie

Poskytovateľ sa zaväzuje poskytovať Služby rozvoja na základe objednávky na realizáciu zmeny doručenej Objednávateľom Poskytovateľovi. Poskytovateľ potvrdí Objednávateľovi prijatie objednávky bez zbytočného odkladu po jej doručení. Pre zamedzenie pochybností, potvrdenie prijatia objednávky sa považuje za akceptáciu objednávky.

Na odovzdanie príslušného plnenia vyzve Poskytovateľ Objednávateľa písomne minimálne 2 (dva) kalendárne dni pred termínom odovzdania plnenia. Objednávateľ sa zaväzuje umožniť Poskytovateľovi odovzdanie plnenia do 5 (piatich) pracovných dní od doručenia písomného oznámenia Poskytovateľa, že príslušné plnenie bolo poskytnuté a že je pripravené na odovzdanie. Odovzdanie a prevzatie jednotlivých plnení sa uskutoční na základe akceptačného protokolu, ktorý podpíšu zástupcovia obidvoch Zmluvných strán.

Objednávateľ je oprávnený odmietnuť podpísanie akceptačného protokolu iba písomne s uvedením dôvodov odmietnutia prevzatia príslušného plnenia. Toto písomné odôvodnenie je Objednávateľ povinný doručiť Poskytovateľovi bezodkladne, najneskôr do 2 pracovných dní odo dňa odovzdávania plnenia Poskytovateľom Objednávateľovi. Pokiaľ nebude akceptačný protokol akceptovaný podpisom Objednávateľa a nebudú podľa predchádzajúcej vety doručené Objednávateľom Poskytovateľovi písomne dôvody, prečo nebol podpísaný, platí nevyvrátiteľná domnienka, že akceptačný protokol sa považuje za podpísaný a účinky podpísaného akceptačného protokolu nastali v deň odovzdávania plnenia. Ak nastane prípad podľa predchádzajúcej vety, prílohou faktúry na úhradu ceny nie je akceptačný protokol.

3.4. Hodnotenie kvality poskytnutej služby

Hodnotenie poskytnutej Služby rozvoja je vykonané Akceptačným testovaním, ktoré je zároveň minimálnym vyžadovaným predpokladom pre akceptáciu zmeny. Akceptačné testovanie prebieha podľa špecifikácie uvedenej v Pláne realizácie zmeny v testovacom prostredí Objednávateľa (požadovanú funkčnosť uvedie Objednávateľ v Požiadavke na zmenu).

Zmluvné strany potvrdia poskytnutie Služieb rozvoja akceptačným protokolom, pričom pre účely úhrady ceny za poskytnuté služby sa rozlišuje úroveň akceptácie nasledovne:

- Neakceptované – výstupom je písomné odôvodnenie rozhodnutia zo strany Objednávateľa o neakceptovaní požadovanej Služby. V danom prípade nemá Poskytovateľ právo na úhradu ceny za uvedené Služby. Po vzájomnej dohode môže Poskytovateľ vyzvať Objednávateľa k akceptácii v dodatočnom termíne.
- Akceptované – výstupom je podpísanie akceptačného protokolu zo strany oprávnených osôb Poskytovateľa a Objednávateľa.

Pokiaľ sa zmluvné strany nedohodnú inak, Objednávateľ sa zaväzuje akceptovať implementované zmeny, ak spĺňajú požiadavky v zmysle obojstranne odsúhlasených funkčných špecifikácií uvedených v objednávke a jej prílohách a zároveň počet nevyriešených Defektov k termínu ukončenia Akceptačných testov neprevýši stanovené limity. Nevyriešené defekty (v rámci limitov) sa Poskytovateľ zaväzuje odstrániť v lehote dohodnutej oprávnenými osobami Zmluvných strán. V prípade absencie dohody je Poskytovateľ povinný defekty (kategórie - normálna) odstrániť do 10 (desiatich) pracovných dní od podpísania akceptačného protokolu.

Akceptačný protokol s úrovňou akceptácie „Akceptované“ podpísaný oprávnenými osobami Objednávateľa a Poskytovateľa slúži ako podklad pre vystavenie príslušnej faktúry Poskytovateľom a úhradu ceny za Služby rozvoja v zmysle Cenovej kalkulácie Poskytovateľa.

Príloha č. 2 – Formulár Požiadavka na zmenu

Požiadavka na zmenu			Číslo Zmeny
Gestor (Objednávateľ):		Organizácia:	
Telefón:		E-mail:	
Projektový manažér (Objednávateľ):		Telefón:	
Dátum a čas zadania požiadavky:		Požadovaný termín ukončenia realizácie:	
Popis zmeny:			
Detailný popis požiadavky na zmenu:			
Prílohy:			

Príloha č. 3 – Formulár Štúdia realizovateľnosti a analýza dopadov

Štúdia realizovateľnosti a Analýza dopadov	
Analýza požiadavky, spracovanie funkčnej špecifikácie, návrh riešenia, analýza dopadov zmeny:	
Rozsah prácnosti implementácie zmeny:	
Návrh implementácie požiadavky:	
Návrh testovania a akceptácie požiadavky:	
Návrh harmonogramu plnenia:	<p>Realizátor vyšpecifikuje:</p> <ul style="list-style-type: none"> • Predpokladaný časový plán realizácie zmeny • Návrh termínov testovania • Návrh termínu nasadenia na testovacie prostredie a funkčné testovanie
Požadovaná súčinnosť interných pracovníkov Objednávateľa:	
Štúdiu pripravil:	
Dátum:	
Podpis:	

Príloha č. 4a – Formulár Cenová kalkulácia

Cenová ponuka	
Číslo Zmeny:	
Predmet cenovej ponuky:	
Prácnosť v MD:	
Cenová ponuka:	
Ponuku pripravil:	
Dátum:	
Podpis:	

Príloha č. 4b – Formulár Objednávka na realizáciu zmeny

Objednávka realizácie zmeny	
Číslo Zmeny:	
ID Objednávky:	
Predmet objednávky:	
Prácnosť v MD:	
Cenová ponuka:	
Harmonogram plnenia:	
Objednávku vystavil:	
Dátum vystavenia:	
Podpis:	

Príloha č. 5 – Formulár Plán realizácie zmeny

Plán realizácie zmeny <i>Formulár je určený pre vypracovanie plánu realizácie zmeny a vyplňa ho Realizátor zmeny</i>		Číslo Zmeny:
ID objednávky:		Dátum vystavenia objednávky:
Gestor:		Organizácia:
Projektový manažér:		Plánovaný termín ukončenia realizácie:
Popis požiadavky na zmenu		

Príloha č. 6 – Formulár Akceptačný protokol Zmeny

	Akceptačný protokol k zmene	Číslo Zmeny:
ID objednávky:		Dátum vystavenia objednávky:
Gestor:		Organizácia:
Projektový manažér:		Plánovaný termín ukončenia realizácie:
Krátky popis požiadavky na zmenu		

Popis predmetu akceptácie

Výsledok testovania:	<i>Popis výsledkov testovania v produkčnom prostredí</i>
Výsledok nasadenia zmeny:	<i>Popis priebehu - bez problémov, vyskytli sa chyby – ich popis</i>
Realizácia školení	<i>Zoznam zrealizovaných školení. Prípadne odkaz na Školiaci plán</i>
Odozdanie dokumentácie:	<i>Zoznam odovzdanej dokumentácie. Prípadne odkaz na externý dokument.</i>

Akceptácia realizácie Zmeny Akceptácia Zmeny schvaľovacou autoritou

Oprávnená osoba Objednávateľa - Gestor		Oprávnená osoba Objednávateľa - Projektový manažér	
Meno:		Meno:	
Funkcia:		Funkcia:	
Dátum:		Dátum:	
Podpis:		Podpis:	

Príloha č. 7 – Formulár report o vykonaných Službách podpory prevádzky

Report činností

Poskytovateľ	Objednávateľ
obchodné meno:	Ministerstvo spravodlivosti SR
Adresa:	Račianska ulica 71, 813 11 Bratislava
Kontakt:	Kontakt:
Servisná zmluva na IS Objednávateľa	
Report činností za <i>mesiac/rok</i> v zmysle Servisnej zmluvy (interné číslo Objednávateľa ...):	

Report o profylaktických činnostiach

Report o profylaktických činnostiach sa predkladá v elektronickej forme vo formáte Microsoft Excel..

Štatistické hlásenie o vykonaných podporných službách			Obdobie:	MM/YYYY
ID Aktivity	ID Komponentu / Funkčnej časti	Popis vykonanej profylaktickej činnosti	Čas vykonania činnosti	Poznámka

Príloha č. 8 – Cenník jednotkových sadziieb Poskytovateľa pre Služby rozvoja a Cenník Služby podpory prevádzky

Cenník Služieb podpory prevádzky

P.č.	Položka	Merná jednotka	Požadované množstvo	Jednotková cena v EUR bez DPH	Jednotková cena v EUR vrátane DPH	Cena za požadované množstvo v EUR bez DPH	Cena za požadované množstvo v EUR vrátane DPH	Sadzba DPH v %	Výška DPH v EUR	Cena za požadované množstvo v EUR vrátane DPH
1.	Cena za poskytnutie služieb podpory prevádzky	mesiac	48	20 000	24 000	960 000	1 152 000	20	192 000	1 152 000

Cenník Služieb rozvoja

P.č.	Položka	Merná jednotka	Predpokladané množstvo	Jednotková cena v EUR bez DPH	Jednotková cena v EUR vrátane DPH	Cena za predpokladané množstvo v EUR bez DPH	Cena za predpokladané množstvo v EUR vrátane DPH	Sadzba DPH v %	Výška DPH v EUR	Cena za predpokladané množstvo v EUR vrátane DPH
1.	Expert- jednotný paušál	MD	1565	460	552	719 000	863 880	20	143 980	863 880

Celková cena za predmet zmluvy

Celková cena za predmet zmluvy v EUR	Cena v EUR bez DPH	Sadzba DPH v %	Výška DPH v EUR	Cena v EUR vrátane DPH
	1 679 900	20	335 980	2 015 880

1. MD manday – človekohodňová sadzba; 8 hodín

Príloha č. 9 – Zoznam subdodávateľov

Por. č.	Subdodávateľ	Osoba oprávnená konať za subdodávateľa	Stručný opis časti zmluvy, ktorá bude predmetom subdodávky
1.	BSP Consulting spol. s r.o.	Michal Jarábek, Jelšová 749/16 Marianka	Modul ESS a Modul DS-LTA
2.	Ensentia s.r.o.	Jaroslav Rojka, Hrušovská 14508/11C, Bratislava – mestská časť Ružinov 821 07	Modul ESS a Modul Ephesoft
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Príloha č. 10 – Zoznam kľúčových expertov

Por. č. kľúčového experta	Názov pozície kľúčového experta	Titul, Meno, Priezvisko
1.	Projektový manažér	Ing. Martin Paulíny
2.	Expert pre oblasť architektúry informačných systémov	Ing. Mgr. Ján Malý
3.	SW analytik	Peter Bubeníček
4.	Databázový špecialista	Karol Papaj
5.	Expert pre riadenie IT procesov	Ing. Radovan Jurovčák
6.	Konzultant pre podporu riadenia prevádzky	Bc. Adam Lojkó
7.	Expert pre IT bezpečnosť	Ing. Štefan Rajec

Príloha č. 11 – Elektronický systém pre správu požiadaviek

Pre IS Objednávateľa bude plniť úlohu systému pre správu požiadaviek ESSP poskytnutý Poskytovateľom.

Popis systému:

- a. spracovanie požiadaviek a Problémov
- b. servicedesk

Možnosti zadávania požiadaviek, Problémov a otázok prostredníctvom:

- web rozhranie koncového používateľa,
- web rozhranie riešiteľa,
- e-mail.

Jednotlivé hlásenia budú prístupné on-line v systéme pre správu požiadaviek pre IS Objednávateľa, ktorý poskytne Oprávneným osobám Objednávateľa nasledovné prehľadné zoznamy:

- nahlásených požiadaviek
- nahlásených Problémov s priradením úrovne podľa ÚSP,
- otázok a odpovedí,
- ďalšie informácie a štatistiky po dohode medzi Poskytovateľom a Objednávateľom. Jednotlivé zoznamy budú podporovať možnosti exportu do formátu xls.

Nad zoznamami si každý používateľ bude môcť konfigurovať filtrovanie, zároveň bude systém pre správu požiadaviek podporovať nastavovanie emailových notifikácií na základe používateľských nastavení.

K uvedeným evidenciám budú mať prístup všetky oprávnené osoby, pričom je možné definovať rôzne úrovne oprávnení (čítanie, zapisovanie, administrácia).

Dostupnosť systému pre správu požiadaviek bude z verejnej siete, na prihlásenie bude požadovaná autentifikácia osoby (prihlasovacie údaje vygeneruje Poskytovateľ).

Pre zamedzenie pochybností vlastníkom obsahu ESSP k IS Objednávateľa (resp. zaznamenaných údajov v ESSP) v rozsahu podľa bodu 2.3 Prílohy č. 1 tejto Servisnej zmluvy je výhradne Objednávateľ.

Príloha č. 12 – Bezpečnostné požiadavky

Ustanovenia tejto prílohy sa použijú pre účely Servisnej zmluvy primerane s prihliadnutím na predmet Servisnej zmluvy a práva a povinnosti zmluvných strán v Servisnej zmluve upravené.

Pre účely tejto prílohy sa rozumie :

- 1) **Tretiou stranou**, Poskytovateľa, resp. jeho subdodávateľa, podieľajúci sa na plnení Zmluvy,
- 2) **Aktívom** objekt, subjekt, štruktúra, vzťah alebo proces, ktorého narušením môže Objednávateľ utrieť stratu; aktíva môžu byť hmotné a nehmotné: budovy, hardvér, softvér, nosiče informácií, na nich uložené informácie, komunikačná technika, databázy údajov, kancelárska technika, dokumenty v papierovej a elektronickej podobe, poskytované služby, dodávateľská podpora, dôležité osoby potrebné na prevádzku organizácie, identifikačné prostriedky, bezpečnostné prostriedky, peniaze, dobré meno, kredit a ďalšie informácie, ktoré považuje ministerstvo za dôležité, dôverné alebo citlivé ,
- 3) **Bezpečnostným incidentom** alebo **BI** každá situácia alebo stav, ktorý priamo ohrozuje bezpečnosť, alebo funkčnosť aktíva. Bezpečnostný incident môže byť vyvolaný náhodným faktorom, neúmyselným činom, úmyselným útokom alebo podvodom,
- 4) **Oprávneným zamestnancom** zamestnanec Objednávateľa a tretej strany poverený výkonom určených úloh vyplývajúcich z činností spojených s naplnením účelu Zmluvy, objednávky alebo projektu (napr. projektový manažér).
- 5) **Kritickým informačným systémom** je každý informačný systém, poskytujúci dostupnosť 24/7 (t.j. poskytujúci služby 24 hodín denne, 7 dní v týždni, s definovaným časom plánovaného výpadku), alebo informačný systém poskytujúci služby verejnosti, alebo informačný systém obsahujúci osobné údaje, alebo podporný informačný systém a technológia, nevyhnutné pre zabezpečenie dostupnosti 24/7 pre iné kritické IS.
- 6) **Dostupnosťou** je pomer celkového času z celého časového intervalu, počas ktorého možno funkčnú jednotku (systém, údaj, služba a pod.) používať, k celému zvolenému časovému intervalu. Dostupnosť zaručuje, že aktívum bude na požiadavku autorizovanej entity prístupné a schopné použitia.
- 7) **Dôvernosťou** je ochrana správ, informácií alebo uchovávaných údajov proti zneužitiu, odpočúvaniu alebo čítaniu neoprávnenými osobami. Zachovanie dôvernosti znamená, že prístup k aktívu je povolený len určenej skupine užívateľov IS alebo IKT.
- 8) **Integritou** je konzistencia komponentov a dát obsiahnutých v IS a ich zhoda s realitou. Zachovanie integrity znamená, že informačné aktíva neboli zmenené neautorizovaným alebo náhodným spôsobom.
- 9) **Informačnou bezpečnosťou** je ochrana IS a informácií, ktoré sú v nich uchovávané, spracovávané a prenášané. Informačná bezpečnosť je schopnosť IKT alebo IS ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam alebo nezákonnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom IS a IKT.

Článok 1

Základné povinnosti tretej strany voči Objednávateľovi pri poskytovaní prác a služieb spojených s naplnením účelu Zmluvy

- 1) Tretia strana sa zaväzuje, že:
 - a. pred začatím činností spojených s naplnením účelu Zmluvy, a pred pridelením prístupových práv potrebných na výkon týchto činností oznámi Oprávnenej osobe objednávateľa personálne obsadenie svojho tímu, ktorý bude vykonávať činnosti spojené s naplnením účelu Zmluvy,

- b. bude bezodkladne informovať Oprávnenú osobu objednávateľa o všetkých personálnych zmenách vo svojom tíme, ktorý vykonáva činnosti spojené s naplnením účelu Zmluvy,
- c. oboznámi svojich zamestnancov, resp. tretie osoby realizujúce činnosti spojené s naplnením účelu Zmluvy s bezpečnostnými požiadavkami v rozsahu tejto prílohy,
- d. oboznámi svojich zamestnancov resp. tretie osoby realizujúce činnosti spojené s naplnením účelu Zmluvy a následne zabezpečí od týchto zamestnancov dodržiavanie povinnosti:
 - ochrany údajov a záväzku mlčanlivosti o údajoch, s ktorými prišli počas výkonu prác na projekte pre Objednávateľa do styku, a to aj po ukončení pracovného, resp. služobného pomeru,
 - zachovávať mlčanlivosť o osobných údajoch, s ktorými počas práce na projekte prídu do styku, ako aj zákaz ich využitia pre osobnú potrebu, bez písomného súhlasu Oprávnenej osoby Objednávateľa ich nesmie zverejniť, nikomu poskytnúť ani sprístupniť, pričom povinnosť mlčanlivosti trvá aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu k tretej strane; povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, zdokumentovať všetky zásahy do IKT Objednávateľa podľa pokynov oprávneného zamestnanca za Objednávateľa,
 - rešpektovať operatívne pokyny zamestnancov s pridelenými bezpečnostnými rolami u Objednávateľa a oprávnených zamestnancov počas výkonu práce na projekte,
 - rešpektovať autorské práva k materiálom poskytnutým Objednávateľom,
 - vrátiť Objednávateľovi všetky poskytnuté materiály a údaje vrátane elektronických a bezpečne zlikvidovať všetky ich kópie, ak to nebude zmluvne dohodnuté inak.
- e. poskytne potrebnú súčinnosť audítorovi vykonávajúcemu audit IS, ak tento súvisí s výkonom práce na projekte,
- f. poskytne potrebnú súčinnosť Objednávateľovi pre prípadný audit svojich IS a IKT, ak tieto súvisia s predmetom plnenia projektu,
- g. ak predmet projektu súvisí s vývojom a aktualizáciou IS, resp. IKT Objednávateľa, bude dodržiavať bezpečnostné požiadavky bezpečnostnej politiky Objednávateľa, platnej bezpečnostnej legislatívy, najmä požiadaviek zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a súvisiaceho výnosu MF SR a nevniešť nepožadované alebo neschválené funkcie do IS. Nenaplnenie tejto požiadavky sa bude považovať za podstatné porušenie zmluvného vzťahu.

Článok 2

Povinnosti zamestnancov tretích strán pri riadení prístupu do IS a aplikácií Objednávateľa

- 1) Zamestnanec tretej strany, resp. tretia osoba realizujúca činnosti spojené s naplnením účelu Zmluvy pre Objednávateľa, je povinný prihlasovať sa do IS Objednávateľa a aplikácií pod prideleným prihlasovacím účtom (ID používateľa) a heslom na prístup do tejto aplikácie alebo IS. Zdieľanie účtov je povolené len po písomnej autorizácii bezpečnostným manažérom a Oprávnenou osobou Objednávateľa a to iba v prípadoch, kedy nie je technologicky možné vynútiť iný spôsob prístupu. Zamestnanec tretej strany má vopred pridelenú rolu a prístupové oprávnenia potrebné na výkon jeho činnosti. Zamestnanec tretej strany nesmie vykonávať iné činnosti, ako sú definované v jeho roli. Prístupové práva používateľov v pozícii tretích strán k informáciám a prostriedkom na ich spracovanie budú po ukončení pracovnoprávneho pomeru, zmluvy alebo dohody odňaté alebo upravené
- 2) Privilegované používateľské účty nesmú byť používané na bežné činnosti nevyžadujúce privilegované oprávnenia. Všetky činnosti privilegovaných používateľov v IS objednávateľa musia byť logované a archivované neobmedzenú dobu. Logy musia byť dostupné odborom auditu a IB objednávateľa.
- 3) Zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu Zmluvy, nesmie na vykonávanie konfigurácií využívať generické a servisné používateľské účty. Výnimku tvorí

len ich individuálne použitie, ktoré musí byť vopred písomne schválené manažérom bezpečnosti a Oprávnenou osobou Objednávateľa. Používanie IS a IKT ministerstva tretími stranami pred i po uvedení do prevádzky musia byť monitorované a evidované.

- 4) Pri práci s heslami je zamestnanec tretej strany povinný dodržiavať nasledovné zásady:
 - a. pravidlá zmeny hesla do aplikácií v rámci LAN Objednávateľa upravuje príslušný Garant systému a ich dodržiavanie kontroluje administrátor aplikácie,
 - b. používateľ je povinný dodržiavať tieto všeobecné zásady tvorby hesla pre prístup do LAN Objednávateľa, podľa ktorých heslo:
 - musí mať dĺžku minimálne 8 znakov,
 - musí sa skladať minimálne z veľkých a malých písmen, číselných znakov (NumLock) a špeciálnych znakov (napr. veľké písmeno + malé písmeno + číslo alebo znak),
 - nesmie byť slovníkovým slovom, menom ani názvom,
 - nesmie byť odvodené od osobných údajov používateľa,
 - nesmie byť tvorené priamou postupnosťou klávesov na klávesnici,
 - pri zmene na nové heslo sa musí od pôvodného líšiť najmenej v štyroch znakoch.
- 5) Ak to aplikácia alebo IS dovoľuje, musí byť prvotné heslo, ktoré bolo zamestnancovi tretej strany na prístup do tejto aplikácie alebo IS pridelené, pri prvom prihlásení zmenené.
- 6) Zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu Zmluvy, ručí za dôvernú a ochranu svojich prístupových hesiel a zodpovedá za všetky udalosti a transakcie, ktoré sa uskutočnili v IS s použitím jeho používateľského mena a hesla.
- 7) V prípade podozrenia na prezradenie prístupového hesla resp. v prípade jeho samotného prezradenia musí poškodený zamestnanec Poskytovateľa alebo tretej strany okamžite informovať oprávneného zamestnanca za Objednávateľa resp. príslušného správcu IS a nahlásiť udalosť ako bezpečnostný incident.
- 8) Po ukončení práce je zamestnanec tretej strany resp. tretia osoba realizujúca činnosti spojené s naplnením účelu Zmluvy, povinný znemožniť prístup k aplikáciám a programom a to tak, aby zabránil neoprávnenému prístupu alebo zneužitiu. Táto povinnosť sa nevzťahuje na zamestnanca tretej strany v prípade, ak mu to odôvodnene neumožňuje charakter vykonávaných prác a táto výnimka je písomne schválená manažérom bezpečnosti Objednávateľa.
- 9) Vzdialený prístup zamestnancov Poskytovateľa je počas vývoja možný len do testovacieho prostredia k IS dodávanému Poskytovateľom. Vzdialený prístup do produkčného prostredia je možný len po podpise SLA, a vyžaduje schválenie manažérom bezpečnosti a gestorom IS.
- 10) Vzdialený prístup dodávateľa a tretích strán v právnom vzťahu k dodávanému dielu do ďalších informačných systémov a ostatného softvéru Objednávateľa nie je možný. Prístup k nim je možné povoliť iba manažérom bezpečnosti na základe písomnej žiadosti a to len v priestoroch, ktoré sú v správe Objednávateľa, a to iba za prítomnosti na to určeného správcu, ktorý vykonáva nevyhnutne potrebný technický zásah.

Článok 3

Pripájanie prenosných počítačov a zariadení zamestnancov tretích strán do IS u Objednávateľa

- 1) Prenosné počítače zamestnancov tretích strán resp. tretích osôb v súvislosti s naplnením účelu Zmluvy smú byť pripájané do IS Objednávateľa len na základe nevyhnutného účelu, splnenia bezpečnostných požiadaviek a písomného súhlasu manažéra bezpečnosti Objednávateľa.
- 2) Zamestnanec tretej strany resp. tretie osoby realizujúce činnosti spojené s naplnením účelu Zmluvy, ktorý uchováva na prenosnom počítači/zariadení informácie, ktorých vlastníkom je Objednávateľ, je povinný:
 - a. chrániť ho pred krádežou alebo zneužitím; zamestnanec tretej strany nesmie ponechať prenosný počítač/zariadenie bez dozoru napr. na verejne dostupných miestach, v dopravných prostriedkoch, neuzamknutých kanceláriách a pod.,
 - b. okamžite hlásiť stratu, prípadne krádež prenosného počítača ako bezpečnostný incident,

- c. ak sú na pevnom disku prenosného počítača/zariadenia ukladané informácie musia byť tieto informácie chránené dodatočným zabezpečovacím prostriedkom, t. j. šifrovaním.
- 3) Dostatočnosť použitých šifrovacích prostriedkov posúdi na základe písomnej žiadosti a opisu manažér bezpečnosti Objednávateľa pred povolením uloženia dát na pevný disk prenosného počítača/zariadenia tretej strany.

Článok 4

Riadenie bezpečnostných incidentov

Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu Zmluvy je povinný zistenie bezpečnostného incidentu alebo podozrenie na bezpečnostný incident bezodkladne nahlásiť na určené kontaktné miesto, ktorým je Service Desk (tel. číslo: +421 2 888 91 200, resp. email: servicedesk.mssr@justice.sk).

V rámci dokumentácie pre dodávaný IS:

- a. musia byť identifikované a dokumentované udalosti a riziká, ktoré môžu ohroziť dostupnosť, dôvernosť a integritu IS, alebo ktoré môžu spôsobiť prerušenie vnútorných procesov, musia byť zavedené procesy na zníženie pravdepodobnosti výskytu a vypracovaný možný dopad takýchto prerušení na prevádzku IS;
- b. musia byť vytvorené a zavedené plány udržiavania (BCP) a plány zálohovania a obnovy prevádzky (DRP), zaisťujúce požadovanú dostupnosť informácií v rámci požadovaných časových intervalov, a ich obnovu po prerušení alebo zlyhaní kritických procesov IS;
- c. musí byť vypracovaná dokumentácia BCM a DRP pre rámec dodávaného IS.

Článok 5

Vyšetrovanie bezpečnostných incidentov

- 1) Každý zamestnanec tretej strany resp. tretie osoby realizujúce prácu v súvislosti s naplnením účelu Zmluvy je povinný, pri vyšetrovaní bezpečnostných incidentov zamestnancom alebo zamestnancami Objednávateľa, poskytnúť potrebnú súčinnosť.
- 2) Po vzniku bezpečnostného incidentu nesmie zamestnanec tretej strany resp. tretia osoba realizujúce prácu v súvislosti s naplnením účelu Zmluvy vykonávať akékoľvek aktivity, ktoré by mohli viesť k znehodnoteniu dôkazov alebo k zhoršeniu dôsledkov.