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:	*Realizátor vyšpecifikuje:* • *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 *Formulár je určený pre vypracovanie plánu realizácie zmeny a vypĺňa ho Realizátor zmeny*		**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:	*Popis výsledkov testovania v produkčnom prostredí*
Výsledok nasadenia zmeny:	*Popis priebehu - bez problémov, vyskytli sa chyby – ich popis*
Realizácia školení	*Zoznam zrealizovaných školení.* *Prípadne odkaz na Školiaci plán*
Odovzdanie dokumentácie:	*Zoznam odovzdanej dokumentácie.* *Prípadne odkaz na externý dokument.*

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:	Župné nám. 13, 813 11 Bratislava
Kontakt:	Kontakt:
Servisná zmluva na IS RÚ	
Report činností za *mesiac/rok* v zmysle Servisnej zmluvy (interné číslo Objednávateľa ...):	

Report o profylaktických činnostiach

Report o profylaktických činnostiach sa predkladá v elektronickej forme vo formáte Microsoft Excel. Názov zasielaného súboru je SYSTÉM_PC_RRRR_MM.xlsx (kde RRRR je aktuálny rok a MM aktuálny mesiac).

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 sadzieb 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	Sadzba DPH v %	Výška DPH v EUR	Cena za požadované množstvo v EUR vrátane DPH
1.	Cena za poskytnutie služieb podpory prevádzky pre IS RÚ	mesiac	48	23 999,00	28 798,80	1 151 952,00	20	230 390,40	**1 382 342,40**

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	Sadzba DPH v %	Výška DPH v EUR	Cena za predpokladané množstvo v EUR vrátane DPH
1.	Expert- jednotný paušál	MD	2 100	450,00	540,00	945 000,00	20	189 000,00	**1 134 000,00**

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
	2 096 952,00	20	524 238,00	**2 516 342,40**

1. MD manday – človekodňová 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.	TEMPEST a.s.	Ing. Roman K ,	Predmetom subdodávky budú služby: - kľúčový expert č.3 - SW analytik, - kľúčový expert č.4 - Expert pre riadenie IT procesov, - kľúčový expert č.6 - Expert pre oblasť integrácie
2.	CNC, a.s.	Ing. Miroslav S ,	Predmetom subdodávky budú služby: - prevádzka aplikácie, správa užívateľov, prevádzka helpdesku, poskytovanie reportovania a štatistických hlásení a pod. - kľúčový expert č.1 – Projektový manažér
3.	SWAN, a.s.	Ing. Juraj O , Ing. Miroslav S ,	Predmetom subdodávky budú služby: - podpora centralizovaného informačného systému architektúrou klient-server na báze technológie webových služieb - technickej podpory softvérového a aplikačného riešenia pre informačný systém, ktorý poskytuje elektronické služby verejnej správy a tieto elektronické služby využívajú štandardizovanú formulárovú technológiu v rámci štruktúrovaných podaní podpisovaných kvalifikovaným podpisom alebo kvalifikovanou elektronickou pečaťou v zmysle platnej legislatívy. - prevádzka aplikácie, správa užívateľov, prevádzka helpdesku, poskytovanie reportovania a štatistických hlásení a pod. - súvisiace s implementáciou aplikácie založenej na komponentoch Microsoft Windows Server alebo ekvivalentných
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Príloha č. 10 – Zoznam kľúčových expertov

Kľúčový expert č. 1 Projektový manažér

e) minimálne 5-ročné praktické skúsenosti (odborná prax) v oblasti projektového riadenia IT projektov;
f) minimálne 2 (dve) praktické skúsenosti (odborná prax) s realizáciou projektov/zmlúv v pozícii projektového manažéra v oblasti IT, s aplikovaním metodiky riadenia IPMA, PRINCE2 alebo ekvivalentnej, pričom minimálne jeden z týchto projektov bol zameraný na poskytovanie elektronických služieb klientom;
g) platný certifikát projektového manažmentu IPMA minimálne úrovne „B" alebo PRINCE 2 úrovne „Practitioner" alebo ekvivalent daného certifikátu.

identifikácia experta: *Ing. Rastislav D*

Kľúčový expert č. 2 - Expert pre oblasť architektúry informačných systémov

e) minimálne 5-ročné skúsenosti v oblasti procesnej analýzy a modelovania informačných systémov;
f) minimálne 2 (dve) profesionálne praktické skúsenosti v oblasti návrhu IT infraštruktúry, ktorého obsahom bol návrh alebo implementácia integrácie systému na viaceré externé informačné systémy;
g) platný certifikát s minimálnou úrovňou TOGAF Certified alebo ekvivalent;
h) platný certifikát s minimálnou úrovňou SOA Certified Consultant alebo ekvivalent daného certifikátu. identifikácia experta: *Ing. Igor G*

Kľúčový expert č. 3 - SW analytik

d) minimálne 5-ročné praktické skúsenosti (odborná prax) v oblasti procesnej analýzy informačných systémov;
e) minimálne 2 (dve) profesionálne praktické skúsenosti (odborná prax) s analýzou SW riešení klient-server, pričom súčasťou minimálne jedného projektu bol návrh a implementácia modulu autentifikácie pre interných alebo externých klientov systému;
f) platný certifikát s minimálnou úrovňou OMG Certified UML Professional na úrovni Advanced alebo ekvivalent daného certifikátu (napr. IBM Certified Solution Designer - Object Oriented Analysis and Design).

identifikácia experta: *Ing. Martin S*

Kľúčový expert č. 4 - Expert pre riadenie IT procesov

e) minimálne 5-ročné skúsenosti s vypracovaním návrhov riešení v oblasti architektúry informačných systémov;
f) minimálne 2 (dve) profesionálne praktické skúsenosti v pozícii experta pre riadenie IT procesov;
g) minimálne 1 platný certifikát /doklad o vykonaní skúšky v oblasti riadenia a správy služieb informačných a komunikačných technológií ITIL (Information Technology Infrastructure Library) podľa EXIN (Examination Institute For Information Science) minimálne v úrovni ITIL Expert in IT Service Management; alebo ekvivalent daného certifikátu od inej akreditovanej autority;
h) platný certifikát ISO 20000 alebo ekvivalent daného certifikátu od inej akreditovanej autority. identifikácia experta: *Ing. Oskar Z*

Kľúčový expert č. 5 - Konzultant pre podporu riadenia prevádzky

c) minimálne 5-ročné skúsenosti v oblasti riadenia prevádzky IT systémov; túto podmienku preukáže životopisom alebo ekvivalentným dokladom;
d) minimálne 2 (dve) profesionálne praktické skúsenosti s riadením podpory IT prevádzky na úrovni L1-L3, ktorej súčasťou bola platforma klient-server s virtualizáciou serverov na báze VMware alebo ekvivalent, zálohovaním a správou bázy dát pre DB platformu Oracle alebo ekvivalent a sieťovej infraštruktúry vrátane aplikácií a bázy dát.

identifikácia experta: *Ing. Juraj O*

Kľúčový expert č. 6 - Expert pre oblasť integrácie

e) minimálne 5-ročné skúsenosti (odborná prax) v oblasti návrhu a implementácie integračných rozhraní informačných systémov;
f) minimálne 2 (dve) profesionálne praktické skúsenosti (odborná prax) v oblasti návrhu a implementácie integračných rozhraní informačných systémov v pozícii SOA a ESB experta;
g) certifikát znalosti ESB alebo ekvivalent daného certifikátu preukazujúci znalosti ESB systémov; túto podmienku uchádzač preukáže prostredníctvom kópie platného certifikátu,
certifikát pre oblasť návrhu architektúry SOA riešení alebo ekvivalent daného

certifikátu. identifikácia experta: *Filip G*

Príloha č. 11 – Elektronický systém pre správu požiadaviek

Pre IS RÚ bude plniť úlohu systému pre správu požiadaviek servicedeskru.atlassian.net 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 RÚ, 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).

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) **Treťou stranou**, Poskytovateľa, resp. jeho subdodávatelia, podieľajúci sa na plnení Zmluvy,
2) **Aktívom** objekt, subjekt, štruktúra, vzťah alebo proces, ktorého narušením môže Objednávateľ utrpieť 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 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 nevniesť 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 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 dôvernosť 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: + , resp. email: _____).

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.