ZADÁVACÍ DOKUMENTACE

ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „*ZZVZ*“ či „*zákon*“)

VEŘEJNÁ ZAKÁZKA

„Identity Management - realizace“

nadlimitní veřejná zakázka na služby zadávaná v otevřeném zadávacím řízení podle ust. § 56 ZZVZ

Ing. Petr Valchář

Digitálně podepsal Ing. Petr Valchář
Datum: 2019.12.27 16:02:19 +01'00'

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví
Sídlo: Roškotova 1225/1, 140 21 Praha 4
IČO: 471 14 321

Obsah:

1. IDENTIFIKAČNÍ ÚDAJE ZADAVATELE A DALŠÍCH OSOB

1.1. Zadavatel

Název zadavatele	Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví
Sídlo zadavatele	Roškotova 1225/1, 140 21 Praha 4
IČO zadavatele	471 14 321
Profil zadavatele	http://www.e-zakazky.cz/Profil-Zadavatele/01d47fe3-916b-4869-bc75-c097dc0eefe1

V příloze č. 8 a jejích přílohách se pro zadavatele užívá označení „Objednatel", případně „Správce".

1.2. Zástupce zadavatele

Zástupcem zadavatele ve věcech souvisejících se zadáváním této veřejné zakázky je MT Legal s.r.o., advokátní kancelář, se sídlem Jakubská 121/1, 602 00 Brno, adresa k doručování Jugoslávská 620/29, 120 00 Praha 2, IČO 28305043 e-mail: **vz@mt-legal.com**. Zástupce zadavatele je v souladu s ust. § 43 ZZVZ pověřen výkonem zadavatelských činností v tomto zadávacím řízení a je taktéž pověřen k přijímání případných námitek dodavatelů dle ust. § 241 a násl. ZZVZ (tím není dotčeno oprávnění statutárního orgánu či jiné pověřené osoby zadavatele). Zástupce zadavatele zajišťuje na straně zadavatele též komunikaci dle čl. 2 této zadávací dokumentace.

1.3. Označení osoby, která zpracovala část zadávací dokumentace

Zadavatel uvádí, že na vypracování přílohy č. 1 (Specifikace předmětu plnění) Vzoru smlouvy o dílo a o poskytování služeb, která je připojena jako příloha č. 8 této zadávací dokumentace, se podílela osoba odlišná od zadavatele, a to **AMI Praha a.s.**, se sídlem Hanusova 826/29, Michle, 140 00 Praha 4, IČO: 25715909.

2. KOMUNIKACE MEZI ZADAVATELEM A DODAVATELI

Veřejná zakázka je zadávána v plném rozsahu elektronicky prostřednictvím elektronického nástroje E-ZAKAZKY společnosti OTIDEA CZ s.r.o. (dále jen „*elektronický nástroj E-ZAKAZKY*") dostupného na http://www.e-zakazky.cz/. Veškeré úkony v rámci tohoto zadávacího řízení a rovněž **veškerá komunikace** mezi zadavatelem (nebo jeho zástupcem) a dodavatelem probíhá elektronicky, a to zejména prostřednictvím elektronického nástroje E-ZAKAZKY.

Veškeré písemnosti zasílané prostřednictvím elektronického nástroje E-ZAKAZKY se považují za řádně doručené dnem jejich doručení do uživatelského účtu adresáta v elektronickém nástroji E-ZAKAZKY. Na doručení písemnosti nemá vliv, zda byla písemnost jejím adresátem přečtena, případně, zda elektronický nástroj E-ZAKAZKY adresátovi odeslal na kontaktní emailovou adresu upozornění o tom, že na jeho uživatelský účet v elektronickém nástroji E-ZAKAZKY byla doručena nová zpráva či nikoliv.

Zadavatel dodavatele upozorňuje, že pro plné využití všech možností elektronického nástroje E-ZAKAZKY je **nezbytné** provést a dokončit tzv. registraci dodavatele. **Manuál pro registraci dodavatele** v elektronickém nástroji E-ZAKAZKY je uveden v uživatelské příručce s názvem Manuál dodavatele v elektronickém nástroji E-ZAKAZKY. Zadavatel upozorňuje, že registrace neproběhne okamžitě a podléhá akceptaci administrátorem systému v délce až 3 pracovních dnů; v případě nedostatků v žádosti o registraci může dojít i k zamítnutí registrace.

Za řádné a včasné seznamování se s písemnostmi zasílanými zadavatelem prostřednictvím elektronického nástroje E-ZAKAZKY, jakož i za správnost kontaktních údajů uvedených u dodavatele, odpovídá vždy dodavatel. **Zadavatel v souladu se ZZVZ požaduje, aby nabídky byly zašifrovány prostřednictvím veřejného klíče (certifikátu pro šifrování) zpřístupněného zadavatelem, jinak se nabídka nebude považovat za podanou a nebude se k ní v souladu s § 28 odst. 2 ZZVZ přihlížet (pro zašifrování nabídky dodavatel nemusí nic činit, pouze stisknout tlačítko „Podat nabídku" ve formuláři nabídky, proces zašifrování proběhne automatizovaně).**

Podmínky a informace týkající se elektronického nástroje E-ZAKAZKY jsou dostupné na https://www.e-zakazky.cz/.

3. INFORMACE O PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

3.1. Předmět veřejné zakázky

Účelem této veřejné zakázky na služby je zabezpečení hospodárného, efektivního a účelného plnění zákonných a smluvních povinností zadavatele, jakož i zajištění kvalitních, moderních a dynamických služeb pro klienty zadavatele a jeho partnerů, prostřednictvím nástroje pro správu identit.

Účelem veřejné zakázky je výběr dodavatele, který zadavateli dodá nástroj pro správu identit dle požadavků uvedených v příloze č. 1 přílohy č. 8 této zadávací dokumentace – Vzor smlouvy o dílo a o poskytování služeb (dále jen „*Vzor smlouvy*" a „*Specifikace plnění*"). Vybraný dodavatel dodá zadavateli SW řešení pro správu identit v rozsahu požadavků dle kapitoly 1 Specifikace plnění (základní požadavky) (dále jen „*Dílo*"). V případě objednávky zadavatele rozšíří vybraný dodavatel Dílo o funkcionality ke splnění požadavků dle kapitoly 2 Specifikace plnění (další požadavky), přičemž další požadavky může zadavatel objednávat jednotlivě a není povinen je objednat v žádném rozsahu. V případě objednávky zadavatele rozšíří vybraný dodavatel Dílo o funkcionality ke splnění požadavků dle kapitoly 3 Specifikace plnění (zabezpečení privilegovaných účtů), přičemž tuto část plnění není zadavatel povinen objednat. Realizované další požadavky a zabezpečení privilegovaných účtů se stávají součástí Díla. Vybraný dodavatel zajistí pro zadavatele také poskytnutí potřebných licencí ke všem součástem Díla, jejich podporu výrobcem a dále bude poskytovat servisní (technickou) podporu ke všem částem Díla, to vše na dobu neurčitou. Vybraný dodavatel bude poskytovat též služby rozvoje (rozvoj, změnové požadavky, konzultace), školení, pravidelné auditní zprávy a spolupráci při úpravě směrnic. Součástí plnění bude případně též dodávka HW a licencí (SW) potřebných pro provoz Díla, pokud pro nabízené řešení vybraným dodavatelem nebude dostačující infrastruktura zadavatele popsaná v čl. 7 přílohy č. 1 Vzoru smlouvy.

Podrobné vymezení předmětu veřejné zakázky, včetně technických podmínek v podrobnostech nezbytných pro zpracování nabídky, je uvedeno v přílohách této zadávací dokumentace.

3.2. Klasifikace předmětu veřejné zakázky (CPV)

KÓD CPV	NÁZEV
72268000-1	Dodávka programového vybavení
72000000-5	Informační technologie: poradenství, vývoj programového vybavení, internet a podpora
72222300-0	Služby informačních technologií
72245000-4	Smluvní analýza systémů a programování
72240000-9	Analýza systémů a programovací služby
72267100-0	Údržba programového vybavení pro informační technologie
72261000-2	Podpora programového vybavení
72310000-1	Zpracování dat
72250000-2	Systémové a podpůrné služby
72251000-9	Obnova po havárii

72253200-5	Systémová podpora
72253000-3	Helpdesk a podpůrné služby
50312600-1	Opravy a údržba zařízení pro informační technologie

3.3. Další informace/požadavky zadavatele

Zadavatel v souladu s § 105 odst. 1 písm. b) ZZVZ požaduje, aby účastník zadávacího řízení ve své nabídce předložil seznam poddodavatelů, pokud jsou účastníkovi zadávacího řízení známi, a uvedl, jakou část veřejné zakázky bude každý z poddodavatelů plnit.

Dodavatel splní tento požadavek vyplněním přílohy č. 5 zadávací dokumentace. Zadavatel výslovně upozorňuje, že pokud dodavatel nemá ke dni podání nabídky v úmyslu zadat část veřejné zakázky poddodavateli, ponechá přílohu č. 5 zadávací dokumentace nevyplněnou, popř. proškrtnutou.

4. LHŮTA A MÍSTO PLNĚNÍ VEŘEJNÉ ZAKÁZKY

Předpokládaný termín zahájení plnění veřejné zakázky je závislý na průběhu zadávacího řízení a jeho výsledku. Počáteční analýza musí být dodána do 12 měsíců od účinnosti smlouvy, Dílo v rozsahu základních požadavků pak ve lhůtě 24 měsíců od účinnosti smlouvy, další dílčí termíny jsou obsaženy ve Vzoru smlouvy. Smlouva bude uzavřena na dobu neurčitou.

Místem plnění je sídlo zadavatele (OZP) na adrese Praha 4, Roškotova 1225/1, PSČ 140 21.

5. PROHLÍDKA MÍSTA PLNĚNÍ

S ohledem na charakter plnění není prohlídka místa plnění organizována.

6. POŽADAVKY ZADAVATELE NA KVALIFIKACI

Kvalifikovaným pro plnění veřejné zakázky je v souladu s ust. § 73 a násl. ZZVZ dodavatel, který prokáže splnění požadavků:

a) základní způsobilosti podle ust. § 74 a § 75 ZZVZ (odst. 6.1),
b) profesní způsobilosti podle ust. § 77 ZZVZ (odst. 6.2),
c) ekonomické kvalifikace podle ust. § 78 ZZVZ (odst. 6.3) a
d) technické kvalifikace podle ust. § 79 ZZVZ (odst. 6.4).

6.1. Základní způsobilost dle ust. § 74 ZZVZ

Způsobilým je dodavatel, který		Způsob prokázání splnění základní způsobilosti (doklady)
a)	nebyl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží; Jde-li o právnickou osobu, musí tuto podmínku splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku splňovat tato právnická osoba, každý člen statutárního orgánu této právnické osoby a osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele; Pro prokazování kvalifikace prostřednictvím pobočky závodu platí ust. § 74 odst. 3 ZZVZ. Pobočka závodu, která má sídlo na území České republiky, se podle ust. § 5 ZZVZ považuje za dodavatele se sídlem v České republice.	*Výpis z evidence Rejstříku trestů pro* *- každou právnickou osobu a* *- každou fyzickou osobu,* *pro niž je dle ZZVZ a zadávacích podmínek vyžadován.*
b)	nemá v České republice ani v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek;	*- Potvrzení příslušného finančního úřadu* *a* *- Čestné prohlášení dodavatele ve vztahu ke spotřební dani, z něhož jednoznačně vyplývá splnění tohoto kvalifikačního požadavku.*
c)	nemá v České republice ani v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění;	*Čestné prohlášení dodavatele, z něhož jednoznačně vyplývá splnění tohoto kvalifikačního požadavku.*
d)	nemá v České republice ani v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti;	*Potvrzení příslušné okresní správy sociálního zabezpečení.*
e)	není v likvidaci, nebylo proti němu vydáno rozhodnutí o úpadku, nebyla vůči němu nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.	*- Výpis z obchodního rejstříku,* *nebo* *- Čestné prohlášení dodavatele ve vztahu k naplnění tohoto požadavku v případě, že dodavatel není v obchodním rejstříku zapsán.*

Způsobilým je dodavatel, který	Způsob prokázání splnění základní způsobilosti (doklady)
Doklady prokazující základní způsobilost musí prokazovat splnění požadované požadavku způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení (tedy nesmí být k okamžiku zahájení zadávacího řízení starší 3 měsíců). Prokázání základní způsobilosti může dodavatel prokázat také předložením výpisu ze seznamu kvalifikovaných dodavatelů v souladu s ust. § 228 ZZVZ či certifikátu vydaného v rámci systému certifikovaných dodavatelů dle § 234 ZZVZ.	

6.2. Profesní způsobilost dle ust. § 77 ZZVZ

Profesní způsobilost splňuje dodavatel, který předloží		Způsob prokázání splnění profesní způsobilosti (doklady)
a)	výpis z obchodního rejstříku nebo jiné obdobné evidence;	*Výpis z obchodního rejstříku nebo výpis z jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.*
b)	doklad, že je oprávněn podnikat v rozsahu odpovídajícímu předmětu veřejné zakázky, pokud jiné právní předpisy takové oprávnění vyžadují;	*Platné oprávnění k podnikání v oboru **poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály** podle přílohy č. 4 nař. vl. č. 278/2008 Sb., o obsahových náplních jednotlivých živností, v platném znění.* *Zadavatel uzná za průkaz podnikatelského oprávnění v požadovaném oboru aktuální výpis z živnostenského rejstříku nebo dosud platný živnostenský list či listy dokládající oprávnění dodavatele k podnikání v oboru (či oborech), který bude zadavatelem požadovanému oboru obsahově odpovídat (jedná se zejména o živnostenské listy vydané za dříve platné právní úpravy).*
Výpis z obchodního rejstříku nebo výpis z jiné obdobné evidence musí prokazovat splnění požadavku na profesní způsobilost dle odst. 6.2 písm. a) nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení (tedy nesmí být k okamžiku zahájení zadávacího řízení starší 3 měsíců). Splnění požadavku profesní způsobilosti může dodavatel prokázat také předložením výpisu ze seznamu kvalifikovaných dodavatelů v souladu s ust. § 228 ZZVZ či certifikátu vydaného v rámci systému certifikovaných dodavatelů dle § 234 ZZVZ **v tom rozsahu, v jakém údaje ve výpisu** ze seznamu kvalifikovaných dodavatelů nebo certifikátu prokazují splnění požadavků na profesní způsobilost.		

6.3. Ekonomická kvalifikace dle ust. § 78 ZZVZ

Ekonomická kvalifikace:		**Způsob prokázání splnění**
a)	relevantní obrat dodavatele, tj. obrat dodavatele dosažený s ohledem na předmět veřejné zakázky, za poslední 3 bezprostředně předcházející účetní období dosahuje částky minimálně **30.000.000 Kč** v součtu za všechny 3 roky. Obratem dosaženým s ohledem na předmět veřejné zakázky se v tomto případě rozumí obrat dosažený za služby a činnosti v oblasti vývoje či dodávky a implementace informačních systémů či jejich částí a zajištění jejich následného provozu a rozvoje.	*(i) Výkaz zisku a ztrát dodavatele nebo obdobný doklad podle právního řádu země sídla dodavatele **a současně*** (ii) *Čestné prohlášení dodavatele o dosaženém ročním obratu dodavatele s ohledem na předmět veřejné zakázky, a to **za každé ze tří** (3) bezprostředně předcházejících účetních období.*
Jestliže dodavatel vznikl později, postačí, předloží-li údaje o svém obratu v požadované výši za všechna účetní období od svého vzniku. Pokud dodavatel bude prokazovat ekonomickou kvalifikaci dle § 78 ZZVZ prostřednictvím jiné osoby ve smyslu § 83 ZZVZ, pak zadavatel v souladu s § 83 odst. 3 ZZVZ požaduje, aby dodavatel a tato jiná osoba, jejímž prostřednictvím dodavatel prokazuje ekonomickou kvalifikaci podle § 78 ZZVZ, nesli společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.		

6.4. Technická kvalifikace dle ust. § 79 ZZVZ

	Technickou kvalifikaci splňuje dodavatel, který předloží	**Vymezení min. úrovně technické kvalifikace a způsob jejího prokázání**
a)	**Ve smyslu § 79 odst. 2 písm. b) ZZVZ** Seznam významných dodávek a služeb poskytnutých za poslední 3 roky před zahájením zadávacího řízení včetně uvedení ceny a doby jejich poskytnutí a identifikace objednatele.	*Ze seznamu významných dodávek a služeb musí jednoznačně vyplývat, že dodavatel v uvedeném období (tj. v posledních 3 letech před zahájením zadávacího řízení) realizoval:* ***1) Alespoň 3 dodávky a služby (referenční zakázky), jejichž předmětem bylo dodání nástroje pro správu identit včetně technické a servisní podpory[1], přičemž musí být splněny následující podmínky*** ***a) alespoň 1 z těchto 3 referenčních zakázek byla realizována v hodnotě plnění nejméně 7.000.000 Kč bez DPH;*** ***b) minimální počet identit ve správě IdM byl alespoň u 1 referenční zakázky 1000;*** ***c) dodaný nástroj pro správu identit měl napojení na koncové systémy MS Active Directory 2016, MS Exchange 2016 a MS SharePoint (nutno prokázat napojení na všechny tyto systémy, ale postačuje prokázat napojení vždy alespoň na 1 z uváděných koncových systémů v rámci 1 referenční zakázky)[2].***

[1] Identity Management je informační systém, který spravuje životní cyklus uživatelů, definuje přístupy uživatelů a jejich rolí v koncových systémech

[2] To znamená, že zadavatel uzná splnění této podmínky dle písm. c) v případě, kdy i jen 1 referenční zakázka zahrnovala napojení na všechny 3 uvedené koncové systémy, stejně jako v případě, kdy bude například prokázáno, že v rámci každé ze 3 referenčních zakázek bylo realizováno napojení jen na jeden z uváděných koncových systémů. Zadavatel požaduje prokázat napojení nástroje pro správu identit na všechny 3 uvedené koncové systémy (každý z nich), nezáleží však, zda toto napojení bylo realizováno v rámci jedné nebo více referenčních zakázek.

	Technickou kvalifikaci splňuje dodavatel, který předloží	Vymezení min. úrovně technické kvalifikace a způsob jejího prokázání
		2) Alespoň 2 referenční zakázky, jejichž předmětem bylo dodání nástroje pro správu privilegovaných účtů (PAM)[3] včetně technické a servisní podpory, přičemž alespoň 1 z těchto 2 významných dodávek byla realizována v hodnotě plnění nejméně 3.000.000 Kč bez DPH. Současně minimální počet účtů ve správě PAM byl alespoň u jedné referenční zakázky 100. *Za poskytnutí významné služby zadavatel pro účely této veřejné zakázky považuje, pokud byly takové služby v požadovaném objemu v rozhodném období dokončeny. Tento kvalifikační požadavek splní také dodavatel, pokud se jedná o služby zahájené dříve než v posledních 3 letech, pokud byly tyto služby v posledních 3 letech dokončeny, a dále služby, které nejsou ještě dokončeny, avšak výše minimálního finančního objemu a věcného požadavku je prokazatelně splněna. Zadavatel pro odstranění jakýchkoli pochybností uvádí, že požadovaná minimální finanční hodnota referenční zakázky bude počítána k ceně plnění za dobu maximálně 3 let plnění.* <u>Všechny</u> *výše uvedené a požadované informace musí vyplývat z předloženého seznamu významných dodávek a služeb, jehož součástí bude rovněž následující informace:* *a) název objednatele či objednatelů referenční zakázky/zakázek,* *b) kontaktní osoba objednatele/ů, u které bude možné realizaci referenční zakázky ověřit, včetně uvedení kontaktů (telefonický a/nebo emailový kontakt),* *c) podrobný popis předmětu referenční zakázky (vč. popisu naplnění dílčích podmínek),* *d) cena referenční zakázky,* *e) místo a doba plnění referenční zakázky,* *f) u dokončených referenčních zakázek informaci o tom, zda byla referenční zakázka poskytnuta řádně, odborně a včas;* *g) u nedokončených referenčních zakázek výši doposud dosaženého finančního objemu.*
K prokázání splnění kritérií technické kvalifikace dle čl. 6.4 písm. a) je dodavatel oprávněn využít formulář, který je obsažen v příloze č. 3 této zadávací dokumentace (Formulář vzorového seznamu významných dodávek a služeb k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. a) zadávací dokumentace).		
b)	**<u>Ve smyslu § 79 odst. 2 písm. d) ZZVZ</u>** Jmenný seznamu techniků, kteří se budou podílet na plnění veřejné zakázky a osvědčení o vzdělání a odborné kvalifikaci dodavatele – osob odpovědných za poskytování příslušných služeb, tj. složení	*Dodavatel musí mít pro plnění této veřejné zakázky k dispozici nejméně 7 členný realizační tým složený z osob zastávajících níže uvedené pozice (označení pro účely této veřejné zakázky).* *Zadavatel požaduje, aby níže uvedení členové týmu na pozici* *a) Projektový manažer* *b) Architekt IDM / PAM* *c) Specialista na softwarovou bezpečnost*

[3] Jedná se o uživatelský účet, který má přiděleno vyšší oprávnění, než kterým disponuje běžný uživatel. Může se např. jednat o oprávnění na instalaci software, úpravy nastavení systému či aplikací, změnu konfigurace síťových zařízení atp.

	Technickou kvalifikaci splňuje dodavatel, který předloží	Vymezení min. úrovně technické kvalifikace a způsob jejího prokázání
	realizačního/řešitelského týmu pro plnění veřejné zakázky.	*d) Senior analytik,* *e) Systémový inženýr,* *f) Programátor,* *g) Tester,* *splňovali níže uvedené požadavky způsobem uvedeným v následující tabulce:*

Název pozice	Požadavky	Způsob splnění kvalifikačního požadavku (prokázání)
Projektový manažer	• VŠ vzdělání min. bc stupně	Dodavatel prokazuje VŠ diplomem.
	• Praxe v oblasti informačních a komunikačních technologií minimálně 3 roky	Dodavatel prokazuje: Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
	• Certifikace Projektového manažera.	Prokazuje certifikací PRINCE2, IPMA nebo obdobné.
Architekt IDM / PAM	• VŠ vzdělání min. bc stupně	Dodavatel prokazuje VŠ diplomem.
	• Praxe v oblasti architektury IdM systémů minimálně 3 roky	Dodavatel prokazuje: Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
Specialista na softwarovou bezpečnost	• VŠ vzdělání min. bc stupně	Dodavatel prokazuje VŠ diplomem.
	• Praxe v oblasti softwarové bezpečnosti informačních a komunikačních technologií nebo na obdobné pozici minimálně 3 roky.	Dodavatel prokazuje: Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
Senior analytik	• VŠ vzdělání min. bc stupně	Dodavatel prokazuje VŠ diplomem.

	• Praxe v oblasti architektury IdM systémů minimálně 3 roky	Dodavatel prokazuje: Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
Systémový inženýr	• minimálně SŠ vzdělání	• Dodavatel prokazuje maturitním vysvědčením nebo vysokoškolským diplomem.
	• Praxe v oblasti informačních a komunikačních technologií minimálně 3 roky	Dodavatel prokazuje: • Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
Programátor	• minimálně SŠ vzdělání	• Dodavatel prokazuje maturitním vysvědčením nebo vysokoškolským diplomem.
	• Praxe v oblasti informačních a komunikačních technologií minimálně 3 roky	Dodavatel prokazuje: • Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).
Tester	• minimálně SŠ vzdělání	• Dodavatel prokazuje maturitním vysvědčením nebo vysokoškolským diplomem.
	• Praxe v oblasti informačních a komunikačních technologií minimálně 2 roky	Dodavatel prokazuje: • Vyplněným jmenným seznamem členů týmu v souladu s přílohou č. 4 zadávací dokumentace s výslovným uvedením délky příslušné praxe (vymezená měsíci a roky).

Zadavatel neumožnuje plnit více rolí stejnou osobou.

Zadavatel připouští, aby dodavatel obsadil příslušnou pozici v týmu větším než uvedeným počtem osob, považuje-li to za účelné, zejména s ohledem na zastupitelnost členů realizačního týmu; to neplatí pro člena realizačního týmu na pozici projektový manažer, která musí být obsazena

právě jednou osobou. Každý z navržených členů týmu musí splňovat všechny stanovené minimální požadavky na vzdělání a odbornou kvalifikaci samostatně.[4]

K prokázání splnění kritérií technické kvalifikace dle odst. 6.4. písm. b) této zadávací dokumentace je dodavatel oprávněn využít formuláře, který je přílohou č. 4 této zadávací dokumentace (**Příloha č. 4 - Formulář realizačního týmu k prokázání kritérií technické kvalifikace dle čl. 6.4. písm. b) zadávací dokumentace dokumentace**).

7. SPOLEČNÁ USTANOVENÍ KE KVALIFIKACI

7.1. Pravost a jazyk dokladů prokazujících splnění kvalifikace ve lhůtě pro prokázání splnění kvalifikace

Dodavatel prokáže splnění kvalifikace ve všech případech doklady předloženými v prostých kopiích (např. v naskenované podobě). Zadavatel může pro účely zajištění řádného průběhu zadávacího řízení postupem podle § 46 odst. 1 ZZVZ požadovat předložení originálu dokladu v elektronické podobě. Zadavatel v souladu s § 86 odst. 2 ZZVZ nepřipouští, aby účastník nahradil předložení dokladů ke kvalifikaci čestným prohlášením.

Povinnost předložit doklad může dodavatel splnit i odkazem na odpovídající informace vedené v informačním systému veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, nebo v obdobném systému vedeném v jiném členském státu, který umožňuje neomezený dálkový přístup. Takový odkaz musí obsahovat internetovou adresu a údaje pro přihlášení a vyhledání požadované informace, jsou-li takové údaje nezbytné. V ČR jde zejména o

- výpis z obchodního rejstříku,
- výpis z veřejné části živnostenského rejstříku nebo
- výpis ze seznamu kvalifikovaných dodavatelů.

Dodavatel také může nahradit požadované doklady jednotným evropským osvědčením pro veřejné zakázky ve smyslu § 87 ZZVZ.

V případě **cizojazyčných** dokumentů připojí účastník k dokumentům (prostý) **překlad do českého jazyka**. Bude-li mít zadavatel pochybnosti o správnosti překladu, je oprávněn si vyžádat předložení úředně ověřeného překladu dokladu do českého jazyka. Povinnost připojit k dokladům překlad do českého jazyka se nevztahuje na doklady ve slovenském jazyce. Doklady o vzdělání (např. vysokoškolské diplomy) lze předkládat rovněž v latinském jazyce.

7.2. Doklady předkládané vybraným dodavatelem

Zadavatel si od dodavatele, kterého identifikoval jako **vybraného dodavatele**, vyžádá předložení originálů dokladů o kvalifikaci, pokud již nebyly v této podobě v zadávacím řízení předloženy, a to v **elektronické podobě** (viz článek 2).

V případě potvrzení vydávaných orgánem státní správy se může jednat například o potvrzení, které bude elektronicky podepsáno a zasláno tímto orgánem do datové schránky dodavatele (v takovém případě postačí předložení pouze tohoto elektronicky podepsaného souboru) či se může jednat o původní listinný originál dokladu, který byl prostřednictvím autorizované konverze převeden do elektronické podoby (například na některém z pracovišť Czech POINT).

[4] Nelze například 1 pozici obsadit 2 osobami s tím, že první má požadované vzdělání a druhá praxi.

Za originál v elektronické podobě se **nepovažuje sken** dokladu vydávaného orgánem státní správy (ani pokud by byl například následně elektronicky podepsán dodavatelem).

7.3. Prokázání kvalifikace získané v zahraničí

V případě, že byla kvalifikace získána v zahraničí, prokazuje se doklady vydanými podle právního řádu země, ve které byla získána, a to v rozsahu požadovaném zadavatelem a ZZVZ.

Potvrzení pro zahraniční dodavatele o neexistenci nedoplatků v ČR vydává ve vztahu k

- daňovým nedoplatkům Finanční úřad pro Prahu 1,
- nedoplatkům na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti Pražská správa sociálního zabezpečení.

7.4. Prokázání části kvalifikace prostřednictvím jiných osob

Pokud není účastník schopen prokázat splnění určité části profesní způsobilosti, ekonomické kvalifikace nebo technické kvalifikace požadované zadavatelem v plném rozsahu a zadávací dokumentace nestanoví jinak, je oprávněn splnění kvalifikace v chybějícím rozsahu prokázat prostřednictvím jiné osoby (to neplatí v případě profesní způsobilosti podle odst. 6.2 písm. a) zadávací dokumentace).

Za jinou osobu se považuje osoba s jiným IČO, a to i tehdy, je-li například součástí stejného koncernu jako účastník.

Účastník je v takovém případě povinen zadavateli předložit

a) doklady prokazující splnění **základní** způsobilosti podle odst. 6.1 zadávací dokumentace (ust. § 74 a § 75 ZZVZ) jinou osobou,
b) doklady prokazující splnění **profesní** způsobilosti podle odst. 6.2 písm. a) zadávací dokumentace (ust. § 77 odst. 1 ZZVZ) jinou osobou,
c) doklady prokazující splnění **chybějící části kvalifikace** prostřednictvím jiné osoby, a
d) písemný **závazek** jiné osoby (případně i ve formě smlouvy s dodavatelem) k poskytnutí **konkrétního** plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat v rámci plnění veřejné zakázky, a to alespoň v **rozsahu**, v jakém jiná osoba prokázala kvalifikaci za dodavatele. Dále viz ust. § 83 odst. 2 ZZVZ.

7.5. Společné prokazování kvalifikace

V případě společné účasti více dodavatelů prokazuje základní způsobilost (odst. 6.1 zadávací dokumentace) a profesní způsobilost (odst. 6.2 písm. a) zadávací dokumentace) každý z těchto dodavatelů samostatně v plném rozsahu.

Společné prokazování kvalifikace musí dále splňovat následující předpoklady:

a) Jeden z dodavatelů bude výslovně identifikován jako vedoucí účastník určený pro komunikaci se zadavatelem v rámci zadávacího řízení;

b) Součástí dokladů prokazujících splnění kvalifikace musí být i doklad (např. smlouva), z něhož bude zřejmý závazek všech dodavatelů nést společnou a nerozdílnou odpovědnost za plnění veřejné zakázky.

7.6. Důsledek nesplnění kvalifikace

Účastník, který neprokáže splnění kvalifikace v rozsahu požadovaném ZZVZ a zadávací dokumentací, může být zadavatelem z účasti v zadávacím řízení vyloučen. Pokud se jedná o vybraného dodavatele, tento musí být ve smyslu § 48 odst. 8 ZZVZ z těchto důvodů ze zadávacího řízení vyloučen.

8. OBCHODNÍ PODMÍNKY

8.1. Obchodní a jiné smluvní podmínky jsou obsaženy v příloze č. 8 - Vzor Smlouvy o dílo a o poskytování služeb.

8.2. Účastník zadávacího řízení není povinen předložit návrh smlouvy ve své nabídce. Účastník zadávacího řízení však podáním nabídky akceptuje závazný text vzoru smlouvy včetně všech příloh v plném rozsahu. Účastník zadávacího řízení není oprávněn požadovat změny či doplnění vzoru smlouvy, s výjimkou doplnění údajů, které jsou výslovně vyhrazeny pro doplnění ze strany účastníka zadávacího řízení, jež budou doplněny před podpisem smlouvy dle nabídky vybraného dodavatele. Smlouva bude uzavřena s vybraným dodavatelem postupem dle ZZVZ.

9. POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

9.1. **Nabídková cena** bude v nabídce účastníka uvedena vždy v korunách českých bez DPH.

9.2. Účastník je povinen zpracovat nabídkovou cenu ve formě vyplnění zadavatelem závazně stanoveného Formuláře Specifikace nabídkové ceny (dále rovněž jen „***Formulář***"), který tvoří přílohu č. 6 této zadávací dokumentace. Formulář je vytvořen ve formátu excel.

9.3. Účastník je povinen vyplnit **všechna** předem určená a barevně (žlutě) odlišená pole jednotkových cen jednotlivých položek Formuláře, které jsou předmětem plnění této veřejné zakázky.

9.4. **Účastník není oprávněn provádět ve Formuláři žádné další úpravy, změny či doplnění, kromě výše uvedeného doplnění jednotlivých, zadavatelem předem určených polí nebo listů Formuláře**.

9.5. **Jednotkové ceny doplněné do Formuláře jsou maximální a nejvýše přípustné nabídkové ceny jednotlivých položek** platné po celou dobu platnosti a účinnosti uzavřené Smlouvy. Do nabídkové ceny musí být započteny veškeré náklady, zisk, rizika, bonusy, slevy a další vlivy. Nabídková cena musí obsahovat cenu veškerých prací, dodávek, dopravy, zaškolení odpovědných pracovníků, činností, finančních vlivů (např. inflace, změna kurzu CZK apod.) a souvisejících nákladů ve vztahu k celé době realizace zakázky v souladu s touto zadávací dokumentací.

9.6. Nabídková cena musí zahrnovat cenu HW vč. podpory (nacenění podpory na dobu 4 let) a licencí (SW; naceněné na dobu 4 let) potřebných pro provoz Díla, pokud pro nabízené řešení účastníka nebude dostačující infrastruktura zadavatele popsaná v čl. 7 přílohy č. 1 Vzoru smlouvy. V případě, že pro řádné poskytnutí Díla účastník hodlá využít jiný HW a SW, než uvedený v čl. 7 přílohy č. 1 Vzoru smlouvy, je jejich cenu povinen vyplnit v souhrnné výši na prvním listu přílohy č. 6 této zadávací dokumentace a zároveň vyplnit druhý list přílohy č. 6 s podrobným rozpadem ceny za takto dodávaný HW a SW.

9.7. Zadavatel upozorňuje dodavatele, aby u jednotkových cen věnovali pozornost tomu, za jakou jednotku je cena stanovena (rok, měsíc, hodina, kus, zejména pak jednotka inkrementálního nárůstu). Zadavatel dodavatele dále upozorňuje, že příloha č. 6 zadávací dokumentace má nastaveny automatické vzorce. S ohledem na skutečnost, že na druhém listu přílohy č. 6 jsou dodavatelé oprávnění doplňovat další řádky, jsou dodavatelé povinní zkontrolovat, že doplněním těchto řádku nedošlo k poškození vzorce a chybnému součtu hodnot, které jsou přenášeny automaticky na první list. Některé složitější výpočty jsou označeny komentáři (týká se hlavně vzorců pro inkrementální nárůsty cen).

9.8. Celková nabídková cena, která bude automaticky dopočtena Formulářem, bude předmětem hodnocení nabídek v rámci dílčího hodnotícího

kritéria nabídková cena. Způsob hodnocení je podrobně popsán v čl. 10 této zadávací dokumentace.

10. HODNOCENÍ NABÍDEK

Hodnocení nabídek bude provedeno v souladu s ustanovením § 114 a násl. ZZVZ podle **ekonomické výhodnosti nabídek**, na základě nejnižší nabídkové ceny. Hodnocena bude celková nabídková cena v Kč bez DPH za 4 roky plnění.[5] Jako nejvýhodnější nabídka bude hodnocena nabídka s nejnižší celkovou nabídkovou cenou v Kč bez DPH.

11. POŽADAVKY NA ZPRACOVÁNÍ A PODÁNÍ NABÍDKY

11.1. Účastník zadávacího řízení podá pouze úplnou **elektronickou podobu nabídky**, a to s využitím elektronického nástroje dle článku 2 zadávací dokumentace. **Nabídka musí být šifrována v souladu s požadavky právních předpisů a elektronického nástroje**.

11.2. Nabídka musí být zpracována **v českém jazyce**. Výjimku tvoří odborné názvy, které mohou být kromě českého jazyka předloženy v anglickém jazyce; v anglickém jazyce pouze tehdy, pokud jsou v anglickém jazyce běžně používány i v českém prostředí nebo nemají vhodný český ekvivalent.

11.3. V případě, že jsou některé údaje v nabídce účastníka uvedeny v jiné měně než v Kč, aniž by to bylo v rozporu se zadávací dokumentací (např. článkem 9), použije se pro přepočet na Kč kurz ČNB (střed) vyhlášený ke dni zahájení zadávacího řízení.

11.4. Zadavatel doporučuje použít následující pořadí dokumentů (zejména budou-li součástí jednoho souboru)

- **krycí list nabídky** obsahující identifikační údaje účastníka v rozsahu uvedeném v ust. § 28 odst. 1 písm. g) ZZVZ,
- **doklady prokazující splnění kvalifikace** [předkládá-li nabídku více dodavatelů společně rovněž originál nebo úředně ověřenou kopii smlouvy o solidární odpovědnosti podle článku 7.5. písm. b)],
- v souladu s požadavky zadavatele vyplněný **Formulář Specifikace nabídkové ceny**,
- v souladu s požadavky zadavatele vyplněný **Seznam poddodavatelů** (příloha č. 5 a článek 3.4),
- vyplněný **formulář „Ověření splnění požadavků zadavatele na zabezpečení privilegovaných účtů"** dle přílohy č. 7 této zadávací dokumentace – účastník musí vyplnit u každého z požadavků, zda je splněn [sloupec „splňuje (ano/ne)"] a popsat způsob splnění požadavku. Je-li některý z požadavku naplněn, ale například v rámci jiného požadavku, účastník uvede „ano" a popíše, v rámci jakého jiného požadavku a jakým způsobem je splněn. Všechny požadavky uvedené v příloze č. 7 jsou povinné, neprokázání splnění všech požadavků je považováno za nesplnění zadávacích podmínek,
- ostatní dokumenty, které mají dle účastníka tvořit obsah nabídky.

12. ZÁVAZNOST POŽADAVKŮ ZADAVATELE

Informace a údaje uvedené v zadávací dokumentaci vymezují závazné požadavky zadavatele na plnění veřejné zakázky.

Tyto požadavky je účastník povinen plně a bezvýhradně respektovat při zpracování své nabídky. Neakceptování požadavků zadavatele uvedených v této zadávací dokumentaci bude považováno za nesplnění zadávacích podmínek.

[5] Formulář je stanoven zčásti jako modelový koš, když položky A.2, A.3, B.2, C.2, B.3, C.3 (a jejich podpoložky) nemusí být odebrány v žádném rozsahu a položky G, H a U mají stanovený předpokládaný objem plnění za dobu 4 let. Stejně tak inkrementální nárůst cen licencí (položky D, E, F) nemusí být využit v případě, že nebude navýšen počet uživatelů, účtů, služeb, zařízení či systémů. Objem položky I může být snížen.

V případě, že zadávací podmínky obsahují odkazy na obchodní firmy, názvy nebo jména a příjmení, specifická označení zboží a služeb, které platí pro určitou osobu, popřípadě její organizační složku za příznačné, patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, umožňuje zadavatel výslovně použití i jiných, kvalitativně a technicky obdobných řešení, které naplní zadavatelem požadovanou či odborníkovi zřejmou funkcionalitu.

13. VYSVĚTLENÍ, ZMĚNA NEBO DOPLNĚNÍ ZADÁVACÍ DOKUMENTACE

Přestože tato zadávací dokumentace vymezuje předmět veřejné zakázky v podrobnostech nezbytných pro zpracování nabídky, mohou dodavatelé požadovat vysvětlení zadávacích podmínek.

Žádost musí být zadavateli doručena ve lhůtě dle § 98 odst. 3 ZZVZ (8 pracovních dnů před koncem lhůty pro podání nabídek).

Zadavatel upozorňuje, že **veškerá komunikace se zadavatelem v rámci zadávacího řízení této veřejné zakázky musí být vedena pouze elektronicky, a to zejména prostřednictvím elektronického nástroje** dle článku 2 zadávací dokumentace, **případně** i prostřednictvím datové schránky či na **emailovou adresu zástupce zadavatele** dle odst. 1.2. zadávací dokumentace.

Zadavatel v zákonné lhůtě 3 pracovních dní uveřejní vysvětlení zadávací dokumentace včetně přesného znění žádosti, na profilu zadavatele.

Zadavatel je oprávněn uveřejnit na profilu zadavatele za podmínek ust. § 98 odst. 1 ZZVZ vysvětlení zadávací dokumentace i z vlastního podnětu. Dle ust. § 99 ZZVZ může takto rovněž uveřejnit změnu nebo doplnění zadávací dokumentace.

14. PODMÍNKY PRO UZAVŘENÍ SMLOUVY S VYBRANÝM DODAVATELEM

14.1. Dodavatel, který byl zadavatelem (komisí) identifikován jako vybraný dodavatel, doloží na výzvu zadavatele za podmínek článku 2 (tj. v elektronické podobě)

a) originály nebo úředně ověřené kopie dokladů o kvalifikaci ve smyslu odst. 7.2 zadávací dokumentace.

14.2. Zadavatel požaduje od vybraného dodavatele jako další podmínky pro uzavření smlouvy ve smyslu § 104 písm. e) ZZVZ předložení následujících dokladů:

- předložení pojistné smlouvy, jejímž předmětem je sjednané pojištění odpovědnosti za škodu v rozsahu a za podmínek specifikovaných v čl. 9.3 Vzoru smlouvy. Vybraný dodavatel je povinen před uzavřením smlouvy předat zadavateli originál nebo úředně ověřenou kopii pojistné smlouvy (popř. originál pojistného certifikátu) uzavřené v rozsahu a za podmínek specifikovaných v čl. 9.3 Vzoru smlouvy.

14.3. Pokud je vybraný dodavatel právnickou osobou, zadavatel zjistí údaje o jeho skutečném majiteli v souladu s ustanovením § 122 odst. 4 ZZVZ. Nebude-li možné zjistit údaje o skutečném majiteli postupem podle § 122 odst. 4 ZZVZ, zadavatel vyzve vybraného dodavatele k předložení výpisu z evidence obdobné evidenci údajů o skutečných majitelích nebo

a) ke sdělení identifikačních údajů všech osob, které jsou jeho skutečným majitelem, a

b) k předložení dokladů v elektronické podobě, z nichž vyplývá vztah všech osob podle písmene a) k dodavateli; těmito doklady jsou například

1. výpis z obchodního rejstříku nebo jiné obdobné evidence,
2. seznam akcionářů,
3. rozhodnutí statutárního orgánu o vyplacení podílu na zisku,

4. společenská smlouva, zakladatelská listina nebo stanovy,

a to vše v souladu s článkem 2 v elektronické podobě.

15. LHŮTA A MÍSTO PRO PODÁNÍ NABÍDEK

Účastník zadávacího řízení je povinen podat nabídku výhradně v elektronické podobě prostřednictvím elektronického nástroje dle článku 2, a to do konce lhůty pro podání nabídek:

Lhůta pro podání nabídek: do 3. 2. 2020, 10:00 hod.

Místo (adresa) pro elektronické podání nabídek:

http://www.e-zakazky.cz/Profil-Zadavatele/01d47fe3-916b-4869-bc75-c097dc0eefe1

16. OTEVÍRÁNÍ NABÍDEK

Otevírání elektronicky podaných nabídek je v souladu s ust. § 109 ZZVZ **neveřejné**.

17. VÝHRADY ZADAVATELE

17.1. Náklady spojené se svou účastí v zadávacím řízení nese účastník.

17.2. Zadavatel si vyhrazuje právo upravit zadávací podmínky či zrušit zadávací řízení v souladu s příslušnými ustanoveními ZZVZ.

17.3. Zadavatel nepřipouští ani nepožaduje varianty nabídky.

17.4. Zadavatel může ověřovat věrohodnost poskytnutých údajů a dokladů a může si je opatřovat také sám, a to například u třetích osob či z veřejně dostupných zdrojů. Účastník je povinen mu v tomto ohledu poskytnout veškerou potřebnou součinnost.

17.5. Zadavatel upozorňuje, že vybraný dodavatel je dle ust. § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly.

17.6. Zadavatel si vyhrazuje právo vyloučit ze zadávacího řízení účastníka, který přímo nebo prostřednictvím poddodavatele, prostřednictvím kterého účastník prokazuje kvalifikaci, poruší ustanovení § 4b zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů.

18. INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

18.1. Zadavatel v postavení správce osobních údajů tímto informuje ve smyslu čl. 13 Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „*GDPR*") účastníky zadávacího řízení o zpracování osobních údajů za účelem realizace zadávacího řízení dle ZZVZ.

18.2. Zadavatel může v rámci realizace zadávacího řízení zpracovávat osobní údaje dodavatelů a jejich poddodavatelů (z řad fyzických osob podnikajících), členů statutárních orgánů a kontaktních osob dodavatelů a jejich poddodavatelů, osob, prostřednictvím kterých je dodavatelem prokazována kvalifikace, členů realizačního týmu dodavatele a skutečných majitelů dodavatele.

18.3. Zadavatel bude zpracovávat osobní údaje pouze v rozsahu nezbytném pro realizaci zadávacího řízení a pouze po dobu stanovenou právními předpisy, zejména ZZVZ. Subjekty údajů jsou oprávněny uplatňovat jejich práva dle čl. 13 až 22 GDPR v písemné formě na adrese sídla zadavatele.

18.4. Zadavatel předává osobní údaje ke zpracování zástupci zadavatele jako zpracovateli osobních údajů, za účelem administrace zadávacího řízení dle ust. § 43 ZZVZ.

19. SEZNAM PŘÍLOH

Součástí zadávací dokumentace jsou následující přílohy:

Příloha č. 1 – Krycí list

Příloha č. 2 – Formulář čestného prohlášení k prokázání některých kritérií základní způsobilosti dle čl. 6.1. zadávací dokumentace

Příloha č. 3 – Formulář vzorového seznamu významných dodávek a služeb k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. a) zadávací dokumentace

Příloha č. 4 – Formulář realizačního týmu k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. b) zadávací dokumentace

Příloha č. 5 - Formulář Seznam poddodavatelů

Příloha č. 6 - Formulář Specifikace nabídkové ceny

Příloha č. 7 - Formulář Ověření splnění požadavků zadavatele na zabezpečení privilegovaných účtů

Příloha č. 8 - Vzor smlouvy o dílo a o poskytování služeb

Příloha č. 1 - Specifikace předmětu plnění

Příloha č. 2 - Kalkulace ceny – *bude připojena v souladu s vyplněným Formulářem Specifikace nabídkové ceny dle nabídky vybraného dodavatele*

Příloha č. 3 - Seznam poddodavatelů – *bude připojena v souladu s vyplněným Formulářem Seznam poddodavatelů dle nabídky vybraného dodavatele*

Příloha č. 4 - Seznam členů realizačního týmu – *bude připojena v souladu s vyplněným Formulářem realizačního týmu k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. b) zadávací dokumentace dle nabídky vybraného dodavatele*

Příloha č. 5 - Smlouva o zpracování osobních údajů

Příloha č. 6 - Dohoda o ochraně důvěrných informací (NDA)

V Praze dne dle elektronického podpisu

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví
právně zastoupený
MT Legal s.r.o., advokátní kancelář

OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA
ZAMĚSTNANCŮ BANK, POJIŠŤOVEN
A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 1 – Krycí list

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

Krycí list nabídky

Dodavatel:

Identifikační údaje dodavatele	
Obchodní firma/název	[doplní dodavatel]
IČO	[doplní dodavatel]
Sídlo	[doplní dodavatel]
Jméno a příjmení osoby zastupující dodavatele, včetně uvedení titulu opravňujícího k zastupování dodavatele	[doplní dodavatel]
Spisová značka v obchodním rejstříku či jiné evidenci, je-li v ní dodavatel zadávacího řízení zapsán	[doplní dodavatel]
Kontaktní osoba	[doplní dodavatel]
Tel./fax	[doplní dodavatel]
E-mail	[doplní dodavatel]
Je účastník malým nebo středním podnikem dle doporučení Komise 2003/361/ES	[doplní dodavatel]

pro účely podání nabídky v rámci veřejné zakázky s názvem ***„Identity Management - realizace"*** zadávané v otevřeném řízení dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

prohlašuje, že

- údaje uvedené v nabídce a přílohách jsou ve vztahu k zadávací dokumentaci úplné, pravdivé a odpovídají skutečnosti;
- se v plném rozsahu seznámil se zadávací dokumentací a zadávacími podmínkami;
- si před podáním nabídky vyjasnil veškerá sporná ustanovení, nebo technické nejasnosti;
- s podmínkami zadání a zadávací dokumentací souhlasí a respektuje je;
- je si vědom všech následků plynoucích z uvedení nepravdivých údajů.

V [místo] dne [DD.MM.RRRR]

[název dodavatele]
[jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování]

OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA
ZAMĚSTNANCŮ BANK, POJIŠŤOVEN
A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 2 – Formulář čestného prohlášení k prokázání některých kritérií základní způsobilosti dle čl. 6.1. zadávací dokumentace

Dodavatel:

Identifikační údaje dodavatele	
Obchodní firma/název	
IČO	
Sídlo	
Jméno a příjmení osoby zastupující dodavatele, včetně uvedení titulu opravňujícího k zastupování dodavatele	

pro účely prokázání základní způsobilosti v rámci veřejné zakázky s názvem ***„Identity Management - realizace“*** zadávané v otevřeném řízení v souladu s ust. § 56 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

prohlašuje, že je dodavatelem

1) který nemá v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek ve vztahu ke spotřební dani;
2) který nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění;
3[1]) který není v likvidaci[2], proti němuž nebylo vydáno rozhodnutí o úpadku[3], vůči němuž nebyla nařízena nucená správa podle jiného právního předpisu[4] nebo v obdobné situaci podle právního řádu země sídla dodavatele.

V [místo] dne [DD.MM.RRRR]

[název dodavatele]
[jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování]

[1] *Čestné prohlášení ve vztahu k § 74 odst. 1 písm. e) zákona předkládá dodavatel v případě, že není zapsán v obchodním rejstříku.*
[2] *§ 187 občanského zákoníku.*
[3] *§ 136 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.*
[4] *Například zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech a některých opatřeních s tím souvisejících a o doplnění zákona České národní rady č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů, zákon č. 363/1999 Sb., o pojišťovnictví a o změně některých souvisejících zákonů.*

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 3 – Formulář vzorového seznamu významných dodávek a služeb k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. a) zadávací dokumentace

Dodavatel:

Identifikační údaje dodavatele	
Obchodní firma/název	
IČO	
Sídlo	
Jméno a příjmení osoby zastupující dodavatele, včetně uvedení titulu opravňujícího k zastupování dodavatele	

tímto za účelem prokázání splnění technického kvalifikačního předpokladu dle čl. 6.4, písm. a) zadávací dokumentace k veřejné zakázce s názvem ***„Identity Management - realizace“***

předkládá následující:

seznam významných dodávek a služeb (dále jen „referenčních zakázek“ nebo „zakázek“) poskytnutých dodavatelem za poslední 3 roky před zahájením zadávacího řízení:

Zakázka č. 1: [1]

Název zakázky	(DOPLNIT)
Identifikační údaje objednatele zakázky	Název/obchodní firma: (DOPLNIT) Sídlo: (DOPLNIT) IČO: (DOPLNIT) Kontaktní osoba pro ověření údajů uvedených dodavatelem: (DOPLNIT), tel.: (DOPLNIT), e- mail: (DOPLNIT)
Podrobný popis předmětu referenční zakázky, z něhož vyplývá splnění požadavků zadavatele dle čl. 6.4 písm. a) bod 1 zadávací dokumentace.	(DOPLNIT)

[1] *Za účelem prokázání splnění kvalifikačního předpokladu pro uvedení dalších zakázek zkopíruje dodavatel tabulku tolikrát, kolikrát bude třeba.*

Cena plnění celkem (v Kč bez DPH)		(DOPLNIT) Kč bez DPH
Cena doposud dosaženého finančního objemu		(DOPLNIT) Kč bez DPH
Počet identit ve správě IDM		(DOPLNIT)
Nástroj pro správu identit měl napojení na koncový systém	**MS Active Directory 2016**	ANO/NE
	MS Exchange 2016	ANO/NE
	MS SharePoint	ANO/NE
Doba plnění zakázky od – do (měsíc a rok)		od (DOPLNIT) do (DOPLNIT)
Místo provádění zakázky		(DOPLNIT)
Referenční zakázka byla poskytnuta řádně, odborně a včas		ANO/NE

Zakázka č. 2:

Název zakázky	(DOPLNIT)
Identifikační údaje objednatele zakázky	Název/obchodní firma: (DOPLNIT) Sídlo: (DOPLNIT) IČO: (DOPLNIT) Kontaktní osoba pro ověření údajů uvedených dodavatelem: (DOPLNIT), tel.: (DOPLNIT), e- mail: (DOPLNIT)
Podrobný popis předmětu referenční zakázky, z něhož vyplývá splnění požadavků zadavatele dle čl. 6.4 písm. a) bod 1 zadávací dokumentace.	(DOPLNIT)
Cena plnění celkem (v Kč bez DPH)	(DOPLNIT) Kč bez DPH
Cena doposud dosaženého finančního objemu	(DOPLNIT) Kč bez DPH
Počet identit ve správě IDM	(DOPLNIT)

Nástroj pro správu identit měl napojení na koncový systém	**MS Active Directory 2016**	ANO/NE
	MS Exchange 2016	ANO/NE
	MS SharePoint	ANO/NE
Doba plnění zakázky od – do (měsíc a rok)		od (DOPLNIT) do (DOPLNIT)
Místo provádění zakázky		(DOPLNIT)
Referenční zakázka byla poskytnuta řádně, odborně a včas		ANO/NE

Zakázka č. 3:

Název zakázky		(DOPLNIT)
Identifikační údaje objednatele zakázky		Název/obchodní firma: (DOPLNIT) Sídlo: (DOPLNIT) IČO: (DOPLNIT) Kontaktní osoba pro ověření údajů uvedených dodavatelem: (DOPLNIT), tel.: (DOPLNIT), e- mail: (DOPLNIT)
Podrobný popis předmětu referenční zakázky, z něhož vyplývá splnění požadavků zadavatele dle čl. 6.4 písm. a) bod 1 zadávací dokumentace.		(DOPLNIT)
Cena plnění celkem (v Kč bez DPH)		(DOPLNIT) Kč bez DPH
Cena doposud dosaženého finančního objemu		(DOPLNIT) Kč bez DPH
Počet identit ve správě IDM		(DOPLNIT)
Nástroj pro správu identit měl napojení na koncový systém	**MS Active Directory 2016**	ANO/NE
	MS Exchange 2016	ANO/NE
	MS SharePoint	ANO/NE
Doba plnění zakázky od – do (měsíc a rok)		od (DOPLNIT) do (DOPLNIT)
Místo provádění zakázky		(DOPLNIT)

Referenční zakázka byla poskytnuta řádně, odborně a včas	ANO/NE

Zakázka č. 4: [2]

Název zakázky	(DOPLNIT)
Identifikační údaje objednatele zakázky	Název/obchodní firma: (DOPLNIT) Sídlo: (DOPLNIT) IČO: (DOPLNIT) Kontaktní osoba pro ověření údajů uvedených dodavatelem: (DOPLNIT), tel.: (DOPLNIT), e- mail: (DOPLNIT)
Podrobný popis předmětu referenční zakázky, z něhož vyplývá splnění požadavků zadavatele dle čl. 6.4 písm. a) bod 2 zadávací dokumentace.	(DOPLNIT)
Cena plnění celkem (v Kč bez DPH)	(DOPLNIT) Kč bez DPH
Cena doposud dosaženého finančního objemu	(DOPLNIT) Kč bez DPH
Počet účtů ve správě PAM	(DOPLNIT)
Doba plnění zakázky od – do (měsíc a rok)	od (DOPLNIT) do (DOPLNIT)
Místo provádění zakázky	(DOPLNIT)
Referenční zakázka byla poskytnuta řádně, odborně a včas	ANO/NE

Zakázka č. 5:

Název zakázky	(DOPLNIT)

[2] *Za účelem prokázání splnění kvalifikačního předpokladu pro uvedení dalších zakázek zkopíruje dodavatel tabulku tolikrát, kolikrát bude třeba.*

Identifikační údaje objednatele zakázky	Název/obchodní firma: (DOPLNIT) Sídlo: (DOPLNIT) IČO: (DOPLNIT) Kontaktní osoba pro ověření údajů uvedených dodavatelem: (DOPLNIT), tel.: (DOPLNIT), e- mail: (DOPLNIT)
Podrobný popis předmětu referenční zakázkay, z něhož vyplývá splnění požadavků zadavatele dle čl. 6.4 písm. a) bod 2 zadávací dokumentace.	(DOPLNIT)
Cena plnění celkem (v Kč bez DPH)	(DOPLNIT) Kč bez DPH
Cena doposud dosaženého finančního objemu	(DOPLNIT) Kč bez DPH
Počet účtů ve správě PAM	(DOPLNIT)
Doba plnění zakázky od – do (měsíc a rok)	od (DOPLNIT) do (DOPLNIT)
Místo provádění zakázky	(DOPLNIT)
Referenční zakázka byla poskytnuta řádně, odborně a včas	ANO/NE

V [místo] dne [DD.MM.RRRR]

[název dodavatele]
[jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování]

OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA
ZAMĚSTNANCŮ BANK, POJIŠŤOVEN
A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 4 – Formulář realizačního týmu k prokázání kritérií technické kvalifikace dle čl. 6.4 písm. b) zadávací dokumentace

Dodavatel:

Identifikační údaje dodavatele	
Obchodní firma/název	
IČO	
Sídlo	
Jméno a příjmení osoby zastupující dodavatele, včetně uvedení titulu opravňujícího k zastupování dodavatele	

tímto za účelem prokázání splnění technického kvalifikačního předpokladu dle čl. 6.4, písm. b) zadávací dokumentace k veřejné zakázce s názvem ***„Identity Management - realizace"***

předkládá následující:

jmenný seznam členů realizačního týmu a současně čestně prohlašuje, že veškeré údaje uvedené v tomto jmenném seznamu realizačního týmu jsou pravdivé.

Jmenný seznam členů realizačního týmu

Název pozice[1]	**Požadavky**	**Způsob splnění kvalifikačního požadavku (prokázání)**
Projektový manažer Jméno a příjmení: _____ Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): a) Pracovní poměr b) Dohoda o pracích konaných mimo prac. poměr c) Jiná dohoda: _____ (specifikujte)	• Má VŠ vzdělání min. bc stupně.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (VŠ diplom).
	• Má praxi v oblasti informačních a komunikačních technologií minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: od MM.RRRR do MM.RRRR na pozici _____[2]
	• Má certifikaci Projektového manažera.	Dodavatel prokazuje kopií dokladu o certifikaci PRINCE2 nebo IPMA nebo obdobnou.

[1] Je-li pozice v souladu se zadávací dokumenatcí obsazena více osobami (nelze pro projektového manažera), opakujte řádky tabulky.

[2] V případě potřeby opakujte.

Název pozice[1]	Požadavky	Způsob splnění kvalifikačního požadavku (prokázání)
Architekt IDM / PAM Jméno a příjmení: _____ Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): d) Pracovní poměr e) Dohoda o pracích konaných mimo prac. poměr f) Jiná dohoda: _____ (specifikujte)	• Má VŠ vzdělání min. bc stupně.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (VŠ diplom).
	• Má praxi v oblasti architektury IdM systémů minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: • od MM.RRRR do MM.RRRR na pozici _____[2]
Specialista na softwarovou bezpečnost Jméno a příjmení: _____ Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): g) Pracovní poměr h) Dohoda o pracích konaných mimo prac. poměr i) Jiná dohoda: _____ (specifikujte)	• Má VŠ vzdělání min. bc stupně.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (VŠ diplom).
	• Má praxi v oblasti softwarové bezpečnosti informačních a komunikačních technologií nebo na obdobné pozici minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: • od MM.RRRR do MM.RRRR na pozici _____[2]
Senior analytik Jméno a příjmení: _____	• Má VŠ vzdělání min. bc stupně.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (VŠ diplom).

Název pozice[1]	Požadavky	Způsob splnění kvalifikačního požadavku (prokázání)
Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): j) Pracovní poměr k) Dohoda o pracích konaných mimo prac. poměr l) Jiná dohoda: _____ (specifikujte)	• Má praxi v oblasti architektury IdM systémů minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: od MM.RRRR do MM.RRRR na pozici _____[2]
Systémový inženýr Jméno a příjmení: _____ Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): a) Pracovní poměr b) Dohoda o pracích konaných mimo prac. poměr c) Jiná dohoda: _____ (specifikujte)	• Má minimálně SŠ vzdělání.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (např. maturitní vysvědčení; VŠ diplom).
	• Má praxi v oblasti informačních a komunikačních technologií minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: od MM.RRRR do MM.RRRR na pozici _____[2]
Programátor Jméno a příjmení: _____	• Má minimálně SŠ vzdělání.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (např. maturitní vysvědčení; VŠ diplom).

Název pozice[1]	Požadavky	Způsob splnění kvalifikačního požadavku (prokázání)
Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): a) Pracovní poměr b) Dohoda o pracích konaných mimo prac. poměr c) Jiná dohoda: _____ (specifikujte)	• Má praxi v oblasti informačních a komunikačních technologií minimálně 3 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: od MM.RRRR do MM.RRRR na pozici _____[2]
Tester Jméno a příjmení: _____ Datum narození: _____ Vztah k dodavateli (*účastník vybere jen jednu možnost*): a) Pracovní poměr b) Dohoda o pracích konaných mimo prac. poměr c) Jiná dohoda: _____ (specifikujte)	• Má minimálně SŠ vzdělání.	• Dodavatel prokazuje kopií dokladu o nejvýše dosaženém vzdělání (např. maturitní vysvědčení; VŠ diplom).
	• Má praxi v oblasti informačních a komunikačních technologií minimálně 2 roky.	• Dodavatel uvádí délku praxe v oblasti informačních a komunikačních technologií: od MM.RRRR do MM.RRRR na pozici _____[2]

V [místo] dne [DD.MM.RRRR]

[název dodavatele]
[jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování]

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 5 – Formulář Seznam poddodavatelů

Dodavatel vyplní v souladu s čl. 3.4. zadávací dokumentace seznam poddodavatelů, které předpokládá využít v rámci realizace předmětu veřejné zakázky, a to ve formě vyplnění níže uvedené tabulky, kterou vyplní ve všech předepsaných kolonkách.

Seznam poddodavatelů

Pol.	Obchodní firma, sídlo a IČO poddodavatele	Specifikace plnění poskytovaného poddodavatelem	Jde o poddodavatele, prostřednictvím kterého je prokazována kvalifikace? (ANO/NE)
1.			
2.			
3.			
4.			
5.			

V [místo] dne [DD.MM.RRRR]

[název dodavatele]
[jméno a příjmení osob/y oprávněné jednat za dodavatele, včetně titulu opravňujícího k zastupování]

Identity Management - realizace
Příloha č. 6 - Specifikace nabídkové ceny (Kalkuce ceny)
List 1 - Celková nabídková cena

Dodavatel vyplní žlutě označená pole, oranžová pole se vyplní automaticky dle nastaveného vzorce. Dodavatel není oprávněn zasahovat do nastavených vzorců. Tato příloha má 2 listy k vyplnění. (List 2 má nastaveny automatické vzorce, z důvodu možnosti doplnění položek je však dodavatel povinen zkontrolovat, zda se vzorce chybně nepřepsaly a není přenášena na list 1 nesprávná hodnota.)

A. Cena za Dílo			B. Cena za licence na 4 roky				C. Cena za podporu produktu výrobcem a servisní podporu (Podpora) na 4 roky			
Označení položky	Název položky	Cena v Kč bez DPH celkem	Označení položky	Název položky	Cena v Kč bez DPH za 1 rok	Cena v Kč bez DPH za 4 roky	Označení položky	Název položky	Cena v Kč bez DPH za 1 rok	Cena v Kč bez DPH za 4 roky
A.1	IdM - Základní požadavky		B.1	Licenční náklady - IdM - Základní požadavky		0,00	C.1	Podpora - IdM - Základní požadavky		0,00
A.2	IdM - Další požadavky	0,00	B.2	Licenční náklady - IdM - Další požadavky	0,00	0,00	C.2	Podpora - IdM - Další požadavky	0,00	0,00
A.2.1	Rozšířené atributy		B.2.1	Licenční náklady - Rozšířené atributy		0,00	C.2.1	Podpora - Rozšířené atributy		0,00
A.2.2	Systemizovaná místa		B.2.2	Licenční náklady - Systemizovaná místa		0,00	C.2.2	Podpora - Systemizovaná místa		0,00
A.2.3	Změna loginu a emailové adresy automaticky		B.2.3	Licenční náklady - Změna loginu a emailové adresy automaticky		0,00	C.2.3	Podpora - Změna loginu a emailové adresy automaticky		0,00
A.2.4	Změna oprávnění při změně systemizovaného místa		B.2.4	Licenční náklady - Změna oprávnění při změně systemizovaného místa		0,00	C.2.4	Podpora - Změna oprávnění při změně systemizovaného místa		0,00
A.2.5	Editovatelné šablony notifikací		B.2.5	Licenční náklady - Editovatelné šablony notifikací		0,00	C.2.5	Podpora - Editovatelné šablony notifikací		0,00
A.2.6	Verzování rolí		B.2.6	Licenční náklady - Verzování rolí		0,00	C.2.6	Podpora - Verzování rolí		0,00
A.2.7	Kontrolní pravidla		B.2.7	Licenční náklady - Kontrolní pravidla		0,00	C.2.7	Podpora - Kontrolní pravidla		0,00
A.2.8	Delegace oprávnění		B.2.8	Licenční náklady - Delegace oprávnění		0,00	C.2.8	Podpora - Delegace oprávnění		0,00
A.2.9	Plná projekce identit na koncové systémy		B.2.9	Licenční náklady - Plná projekce identit na koncové systémy		0,00	C.2.9	Podpora produktu výrobcem - Plná projekce identit na koncové systémy		0,00
A.2.10	Responzivní design, corporate branding		B.2.10	Licenční náklady - Responzivní design, corporate branding		0,00	C.2.10	Podpora - Responzivní design, corporate branding		0,00
A.2.11	Napojení na monitorovací nástroj Flowmon a Monet		B.2.11	Licenční náklady - Napojení na monitorovací nástroj Flowmon a Monet		0,00	C.2.11	Podpora - Napojení na monitorovací nástroj Flowmon a Monet		0,00
A.2.12.1	Koncový systém VPN		B.2.12.1	Licenční náklady - Koncový systém VPN		0,00	C.2.12.1	Podpora produktu výrobcem - Koncový systém VPN		0,00
A.2.12.2	Koncový systém HelpDesk		B.2.12.2	Licenční náklady - Koncový systém HelpDesk		0,00	C.2.12.2	Podpora - Koncový systém HelpDesk		0,00
A.2.12.3	Koncový systém TIC		B.2.12.3	Licenční náklady - Koncový systém TIC		0,00	C.2.12.3	Podpora - Koncový systém TIC		0,00
A.2.12.4	Koncový systém MS SQL server		B.2.12.4	Licenční náklady - Koncový systém MS SQL server		0,00	C.2.12.4	Podpora - Koncový systém MS SQL server		0,00
A.2.12.5	Koncový systém Základní registry		B.2.12.5	Licenční náklady - Koncový systém Základní registry		0,00	C.2.12.5	Podpora - Koncový systém Základní registry		0,00
A.2.12.6	Koncový systém Juno		B.2.12.6	Licenční náklady - Koncový systém Juno		0,00	C.2.12.6	Podpora- Koncový systém Juno		0,00
A.2.12.7	Koncový systém KS		B.2.12.7	Licenční náklady - Koncový systém KS		0,00	C.2.12.7	Podpora - Koncový systém KS		0,00
A.2.12.8	Koncový systém Evidence 2000		B.2.12.8	Licenční náklady - Koncový systém Evidence 2000		0,00	C.2.12.8	Podpora - Koncový systém Evidence 2000		0,00
A.2.12.9	Koncový systém ČiSoft		B.2.12.9	Licenční náklady - Koncový systém ČiSoft		0,00	C.2.12.9	Podpora - Koncový systém ČiSoft		0,00
A.2.12.10	Koncový systém OZP Express		B.2.12.10	Licenční náklady - Koncový systém OZP Express		0,00	C.2.12.10	Podpora - Koncový systém OZP Express		0,00
A.2.13	Vysoká dostupnost		B.2.13	Licenční náklady - Vysoká dostupnost		0,00	C.2.13	Podpora - Vysoká dostupnost		0,00
A.3	Zabezpečení privilegovaných účtů		B.3	Licenční náklady - Zabezpečení privilegovaných účtů		0,00	C.3	Podpora - Zabezpečení privilegovaných účtů		0,00
A	Celková nabídková cena za Dílo	0,00	B	Celková nabídková cena za licenční náklady	0,00	0,00	C	Celková nabídková cena za Podporu	0,00	0,00

D. Inkrementální nárůst ceny za Podporu										
Označení položky	**Název položky**	**Nárůst ceny za zvýšený počet uživatelů o 20 - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet uživatelů na celkových 1000 - 1 rok (v Kč bez DPH**	**Nárůst ceny za zvýšený počet uživatelů na celkových 1000 - 4 roky (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet privilegovaných identit o 5 - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet privilegovaných identit na celkových 185 - 1 rok (v Kč bez DPH**	**Nárůst ceny za zvýšený počet privilegovaných identit na celkových 185 - 4 roky (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet koncových systémů připojených k IdM o 2 - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet koncových systémů připojených k IdM na celkových 20 - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet koncových systémů připojených k IdM na celkových 20 - 4 roky (v Kč bez DPH)**
D.1	Podpora - IdM - Základní požadavky - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2	Podpora - IdM - Další požadavky - inkrementální nárůst	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
D.2.1	Podpora - Rozšířené atributy - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.2	Podpora -Systemizovaná místa - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.3	Podpora - Změna loginu a emailové adresy automaticky - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.4	Podpora - Změna oprávnění při změně systemizovaného místa - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.5	Podpora - Editovatelné šablony notifikací - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.6	Podpora - Verzování rolí - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.7	Podpora - Kontrolní pravidla - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.8	Podpora - Delegace oprávnění - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.9	Podpora - Plná projekce identit na koncové systémy - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.10	Podpora - Responzivní design, corporate branding - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.11	Podpora - Napojení na monitorovací nástroj Flowmon a Monet - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.1	Podpora - Koncový systém VPN- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.2	Podpora - Koncový systém HelpDesk- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.3	Podpora - Koncový systém TIC - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.4	Podpora - Koncový systém MS SQL server - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.5	Podpora - Koncový systém Základní registry - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.6	Podpora - Koncový systém Juno - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.7	Podpora - Koncový systém KS - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.8	Podpora - Koncový systém Evidence 2000- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.12.9	Podpora - Koncový systém ČiSoft- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00

D.2.12.10	OZP Express - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.2.13	Podpora - Vysoká dostupnost - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D.3	Podpora - Zabezpečení privilegovaných účtů - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0,00
D. Inkrementální nárůst ceny za podporu	Celková nabídková cena za Podporu - inkrementální nárůst	0,00								

E. Inkrementální nárůst ceny za licence

Označení položky	Název položky	Nárůst ceny za zvýšený počet uživatelů o 20 - 1 rok (v Kč bez DPH)	Nárůst ceny za zvýšený počet uživatelů na celkových 1000 - 1 rok (v Kč bez DPH	Nárůst ceny za zvýšený počet uživatelů na celkových 1000 - 4 roky (v Kč bez DPH)	Nárůst ceny za zvýšený počet privilegovaných identit o 5 - 1 rok (v Kč bez DPH)	Nárůst ceny za zvýšený počet privilegovaných identit na celkových 185 - 1 rok (v Kč bez DPH	Nárůst ceny za zvýšený počet privilegovaných identit na celkových 185 - 4 roky (v Kč bez DPH)	Nárůst ceny za zvýšený počet koncových systémů připojených k IdM o 2 - 1 rok (v Kč bez DPH)	Nárůst ceny za zvýšený počet koncových systémů připojených k IdM na celkových 20 - 1 rok (v Kč bez DPH)	Nárůst ceny za zvýšený počet koncových systémů připojených k IdM na celkových 20 - 4 roky (v Kč bez DPH)
E.1	Licenční náklady - IdM - Základní požadavky - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2	Licenční náklady - IdM - Další požadavky - inkrementální nárůst	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0
E.2.1	Licenční náklady - Rozšířené atributy - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.2	Licenční náklady - Systemizovaná místa - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.3	Licenční náklady - Změna loginu a emailové adresy automaticky - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.4	Licenční náklady - Změna oprávnění při změně systemizovaného místa - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.5	Licenční náklady - Editovatelné šablony notifikací - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.6	Licenční náklady - Verzování rolí - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.7	Licenční náklady - Kontrolní pravidla - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.8	Licenční náklady - Delegace oprávnění - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.9	Licenční náklady - Plná projekce identit na koncové systémy - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.10	Licenční náklady - Responzivní design, corporate branding - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.11	Licenční náklady - Napojení na monitorovací nástroj Flowmon a Monet - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.1	Licenční náklady - Koncový systém VPN- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.2	Licenční náklady - Koncový systém HelpDesk- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.3	Licenční náklady - Koncový systém TIC - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0

E.2.12.4	Licenční náklady - Koncový systém MS SQL server - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.5	Licenční náklady - Koncový systém Základní registry - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.6	Licenční náklady - Koncový systém Juno - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.7	Licenční náklady - Koncový systém KS - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.8	Licenční náklady - Koncový systém Evidence 2000- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.9	Licenční náklady - Koncový systém ČiSoft- inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E.2.12.10	Licenční náklady - Koncový systém OZP Express		0,00	0,00		0,00	0,00		0,00	0
E.2.13	Licenční náklady - Vysoká dostupnost - inkrementální nárůst		0,00	0,00		0,00	0,00		0,00	0
E	Celková nabídková cena za Licenční náklady - inkrementální nárůst	0,00								

F. Inkrementální nárůst ceny za licence pro Zabezpečení privilegovaných účtů					
	Aktuální počet	**Celkový plánovaný počet**	**Nárůst ceny za zvýšený počet uživatelů, účtů, služeb, zařízení či systémů o 1 - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet uživatelů, účtů, služeb, zařízení či systémů na celkový plánovaný počet - 1 rok (v Kč bez DPH)**	**Nárůst ceny za zvýšený počet uživatelů, účtů, služeb, zařízení či systémů na celkový plánovaný počet - 4 roky (v Kč bez DPH)**
Privilegovaní uživatelé / privilegované identity v infrastruktuře					
Počet administrátorů (správců + externistů)	25	65		0,00	0,00
Počet privilegovaných účtů na koncových systémech	100	120		0,00	0,00
Koncový systém / služba / zařízení					
Linux RHEL 6/7	29	60		0,00	0,00
Windows Server 2008/12/16	102	150		0,00	0,00
Microsoft SQL Server 2016	16	25		0,00	0,00
VMware ESXi / vSphere	9	15		0,00	0,00
ERP icis	0	1		0,00	0,00
Firewall	4	8		0,00	0,00
Aktivní prvky	35	50		0,00	0,00
Aplikace/skripty ** využívající privilegované účty k přístupu k lokálním i vzdáleným službám nebo systémům	10	500		0,00	0,00
** tyto skripty jsou spouštěny ručně nebo automaticky na následujícím počtu operačních systémů	50	50	x	x	x
F	Celková nabídková cena za Licenční náklady pro Zabezpečení privilegovaných účtů - inkrementální nárůst	0,00			

G. Cena za rozvoj, změnové požadavky a konzultace na 4 roky

Označení položky	Název položky	Cena v Kč bez DPH za 1 hodinu	Cena v Kč bez DPH za 4 roky (150 hodin měsíčně * 48 měsíců, tj. 7200 hodin za 4 roky)[1)]
G	Rozvoj, změnové požadavky a konzultace		0,00

H. Cena za školení v rozsahu dle čl. 1.4 přílohy č.1 smlouvy		
Označení položky	**Název položky**	**Cena v Kč bez DPH za školení (celé školení)**
H	Školení	

I. Cena za pravidelné auditní zprávy za 4 roky			
Označení položky	**Název položky**	**Cena v Kč bez DPH za 1 pravidelnou auditní zprávu**	**Cena v Kč bez DPH za 4 roky** (8 pravidelných auditních zpráv)
I	Pravidlená auditní zpráva		0,00

J. Cena za úpravu směrnic na 4 roky			
Označení položky	**Název položky**	**Cena v Kč bez DPH za 1 hodinu úpravy směrnic**	**Cena v Kč bez DPH za 4 roky** (240 hodin)[2)]
J	Úprava směrnic		0,00

K. Cena za dodávku HW		
Označení položky	**Název položky**	**Cena v Kč bez DPH**
K	Dodávka HW[3)]	0,00

L. Cena za podporu HW na 4 roky		
Označení položky	**Název položky**	**Cena v Kč bez DPH**
L	Podpora HW na 4 roky[3)]	0,00

M. Cena za dodávku SW za 4 roky		
Označení položky	**Název položky**	**Cena v Kč bez DPH za 4 roky**
M	Dodávka SW[4)]	0,00

Celková nabídková cena		
Označení položky	**Název položky**	**Cena v Kč bez DPH**
A	**Celková nabídková cena za Dílo**	**0,00**
B	**Celková nabídková cena za Licenční náklady**	**0,00**
C	**Celková nabídková cena za Podporu**	**0,00**
D	**Celková nabídková cena za Podporu - inkrementální nárůst**	**0,00**
E	**Celková nabídková cena za Licenční náklady - inkrementální nárůst**	**0,00**

F	Celková nabídková cena za Licenční náklady pro Zabezpečení privilegovaných účtů - inkrementální nárůst	0,00
G	Celková nabídková cena za Rozvoj, změnové požadavky a konzultace	0,00
H	Celková nabídková cena za Školení	0,00
I	Celková nabídková cena za Pravidlenou auditní zprávu	0,00
J	Celková nabídková cena za Úpravu Směrnic	0,00
K	Celková nabídková cena za dodávku HW	0,00
L	Cena za podporu HW na 4 roky	0,00
M	Celková nabídková cena za dodávku SW na 4 roky	0,00
Celková nabídková cena	x	0,00

1) Jedná se o modelový příklad pro účely hodnocení nabídek, Objednatel není povinen odebrat žádný minimální objem této služby a zároveň lze odebrat i větší než stanovené množství.

2) Jedná se o modelový příklad pro účely hodnocení nabídek, Objednatel není povinen odebrat žádný minimální objem této služby a zároveň lze odebrat i větší než stanovené množství.

3) Pokud Dodavatel bude dodávat jiný HW, než který je uvedený v čl. 7 přílohy č. 8.1 Vzoru smlouvy, vyplní tuto položku a na listu 2 uvede podrobný rozpad ceny dodávaného HW a jeho podpory.

4) Pokud dodavatel bude dodávat jiný SW, než který je uvedený v čl. 7 přílohy č. 8.1 Vzoru slouvy, vyplní tuto položku a na listu 2 uvede podrobný rozpad ceny dodávaného SW.

Identity Management - realizace
Příloha č. 6 - Specifikace nabídkové ceny
List 2 - Rozpad ceny dodávaného HW a SW

K. Cena za dodávku HW			L. Cena za podporu HW na 4 roky			
Číslo položky	**Název položky (vč. popisu)**	**Cena v Kč bez DPH**	**Označení položky**	**Název položky**	**Cena v Kč bez DPH za 1 rok**	**Cena v Kč bez DPH za 4 roky**
K[1)]	Dodávka HW[2)]	0,00	L	Cena za podporu HW na 4 roky	0,00	0,00
K.1	[2)]		L.1	[2)]		0,00
K.2	[2)]		L.2	[2)]		0,00
K.3	[2)]		L.3	[2)]		0,00

M. Cena za dodávku SW za 4 roky			
Číslo položky	**Název položky (vč. popisu)**	**Cena v Kč bez DPH za 1 rok**	**Cena v Kč bez DPH za 4 roky**
M[1)]	Dodávka SW	0,00	0,00
M.1	[2)]		0,00
M.2	[2)]		0,00
M.3	[2)]		0,00

1) Dodavatel vyplní (přidá) tolik řádků, kolik je třeba
2) Dodavatel popíše položky (název HW a jeho popis)

Identity Management - realizace
Příloha č. 7 - Ověření splnění požadavků zadavatele na zabezpečení privilegovaných účtů

SPRÁVA PRIVILEGOVANÝCH ÚČTŮ			
Oblast	**Požadavky na řešení**	**Splňuje (Ano/Ne)**	**Způsob splnění požadavku**
Funkční požadavky			
Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.		
Striktní oddělení přístupových oprávnění	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.		
Víceúrovňové schvalování přístupů	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému, atp.		
Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat. Systém jako celek musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivaletní certifikaci.		
Jednotná centrální správa	Správá řešení je umožněna pomocí jednotné centrální správy. Řešení musí umožňovat konfiguraci systému pomocí RestAPI nebo SOAP - správa uživatelů, zakládání a editace účtů, změny přihlašovacích údajů		
Integrace s ticketing nástroji	Řešení umožňuje integraci s ticketing nástroji třetích stran - žádost o schválení přístupu, přístup na základě existujícího ticketu, atp.		
Podpora MS Active Directory	Řešení nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech.		
Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server,...).		
Správa řešení pomocí Rest API	Řešení je možné spravovat pomocí Rest API a to minimálně na úrovni - vytváření uživatelů a účtů, nastavení oprávnění, změny politik, system health monitoring, schvalování požadavků, autentizace atp.		
Šifrování a zabezpečení dat	Řešení musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. Řešení umožňuje společnostem splnit compliance požadavky pro ZKB, GDPR, PCI-DSS, SOX, HIPAA, atd.		

Identity Management - realizace
Příloha č. 7 - Ověření splnění požadavků zadavatele na zabezpečení privilegovaných účtů

Password Management			
Vyhledávání a přidávání privilegovaných účtů	Řešení umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení. Systém umožňuje vyhledávání v on-premise i cloud prostředí (např. AWS).		
Řízení hesel a SSH klíčů	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bezagentsky. Řešení musí podporovat změnu přihlašovacích údajů minimálně pro typy systémů viz. bod "Podpora řízení hesel a bezpečné přístupy pro systémy", zároveň řešení musí umožňovat tzv. customizaci password management modulu pro další systémy zadavatele.		
Ověřování hesel	Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.		
Řízení servisních účtů	Systém umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object,...). Při přidávání účtů na návaznosti upozorňuje, nebo automaticky integruje do systému. Při vynucení změny hesla je heslo propsáno i do navázaných služeb.		
Vyhledání tzv. backdoor účtů a automatický onboarding	Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla.		
Aplikace a skripty	Systém umožňuje bezpečné nakládání s přihlašovacími údaji pro aplikace a skripty, kterým pomocí rozhraní poskytuje přístup k těmto údajům a eliminuje nutnost mít přístupové údaje napevno zadané ať už v těle aplikace, nebo v jiných konfiguračních souborech. Zároveň ošetřuje situaci, kdy by mohlo být rozhraní zneužito pro neoprávněnou aplikaci, např. kontrolou zdrojové cesty nebo pomocí hashe volajícího skriptu.		
Customizace Password Management	Řešení musí umožňovat možnost úpravy systému password management, tak aby bylo možné integrovat další systémy zadavatele. Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů.		
Řízení vzdálených relací			
Izolace relací	Správcovský přístup na cílový systém bude zprostředkován pomocí tzv. terminal/jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace...např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace. Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).		

Připojení do webových relací	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě pomocí tzv. Webové proxy. Řešení umožní uživateli přihlášení do vybrané webové aplikace pomocí standardního (neprivilegovaného) účtu, webová proxy následně zprostředkuje přihlášení do koncové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.		
Vzdálené připojení pomocí prohlížeče	Řešení poskytuje možnost připojení na vzdálené relace využitím pouze webového prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).		
Nahrávání relací	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat - minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u Webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je dostupné z GUI dodávaného řešení.		
Automatické označení podezřelých aktivit v nahrávkách	Systém poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. Systém zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp.		
Pozastavení/terminace relací	Řešení nabízí možnost automatického pozastavení, nebo terminace potenciálně nebezpečných relací. Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat - typ události, uživatelé (možnost nastavení výjimek na úrovni skupin v AD) a typ reakce.		
Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).		
Kontrola relací	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu.		
Analýza a detekce potenciálně škodlivého chování	Součástí řešení je nástroj umožňující provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování - uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístup v nestandardní časy, atp... Zároveň řešení umožňuje detekci útoků na úrovni zranitelností Kerberos typu OverPass the Hash a Golden ticket.		
Audit a reporting			
Zobrazení aktivit uživatele	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.		
Audit administrátorských akcí	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.		
Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.		
Export auditních dat	Systém musí umožňovat export auditních záznamů pro nástroje typu Crystal reports atp.		
Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.		

Zabezpečení auditních záznamů	Řešení musí umožňovat nesmazatelnost logů po dobu minimáně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel.		
Monitoring pomocí API	Systém umožňuje monitoring jednotlivých komponent pomocí RestAPI / SOAP - integrace s monitoring systémy zadavatele.		
Integrace a Podporované platformy			
Podpora systémů zadavatele	Systém musí umožňovat správu privilegovaných účtů pro různé druhy koncových systémů - minimálně v rozsahu viz. bod: "Podpora řízení hesel a bezpečné přístupy pro systémy". Případně možnost konfigurace a vývoje vlastních konektorů pro změnu hesel a vzdálených přístupů.		
Seznam podporovaných systémů	Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM, atp.		
MFA - multi factor autentizace	Řešení musí podporovat integraci s nástroji třetích stran pro vynucení multi factor autentizace. Minimálně na úrovní LDAP/S, RADIUS, PKI, RSA, atp.		
SIEM integrace	Systém musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů, nejlépe v reálném čase pomocí Syslog.		
HSM integrace	Systém musí umožňovat integraci s HSM moduly pro uložení šifrovacích klíčů k databázi nabízeného řešení.		
Podpora řízení hesel a bezpečné přístupy pro systémy			
Podpora pro vyjmenované systémy	Windows 7, 10, Windows Server 2016, 2019 Active Directory HP iLO, Dell iDRAC, IBM IMM Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+ VMWare, HyperV, Citrix Red Hat, Suse, Unix, AIX MS SQL, Oracle, PostgreSQL Checkpoint, Fortinet, Palo Alto, Symantec Cisco, Juniper, F5, HP, Blue Coat		
Architektura			
Architektura řešení	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.		
Vysoká dostupnost řešení	Řešení musí podporovat nasazení ve vysoké dostupnosti a vlastní technologické možnosti (nejsou používány nástroje/SW třetích stran) pro zabezpečení High Availability, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat.		
Disaster recovery	Disaster recovery a HA proces je plně automatický.		
Zálohování systému	Řešení musí umožňovat bezpečné zálohování dat systému - zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů.		

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

PŘÍLOHA Č. 8

SMLOUVA O DÍLO A O POSKYTOVÁNÍ SLUŽEB

„Identity Management – realizace“

Tato **SMLOUVA O DÍLO A O POSKYTOVÁNÍ SLUŽEB „IDENTITY MANAGEMENT – REALIZACE“** (dále jen „**Smlouva**“) je uzavřena níže uvedeného dne, měsíce a roku v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“)

MEZI

Oborovou zdravotní pojišťovnou zaměstnanců bank, pojišťoven a stavebnictví
se sídlem Roškotova 1225/1, 140 21 Praha 4
IČO: 47114321,
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 7232,
bankovní spojení: [BUDE DOPLNĚNO]
číslo účtu: [BUDE DOPLNĚNO]
datová schránka: [BUDE DOPLNĚNO]

DÁLE JEN „**Objednatel**“,
NA STRANĚ JEDNÉ

A

[DOPLNÍ DODAVATEL]
se sídlem: [DOPLNÍ DODAVATEL]
IČO: [DOPLNÍ DODAVATEL]
zápis v OR: [DOPLNÍ DODAVATEL]
bankovní spojení: [DOPLNÍ DODAVATEL]
číslo účtu: [DOPLNÍ DODAVATEL]
datová schránka: [DOPLNÍ DODAVATEL]

DÁLE JEN „**Dodavatel**“
NA STRANĚ DRUHÉ

OBJEDNATEL A DODAVATEL DÁLE SPOLEČNĚ JEN „**Smluvní strany**“
NEBO SAMOSTATNĚ „**Smluvní strana**“

1. Úvodní ustanovení

1.1 Smluvní strany se dohodly, že se jejich závazkový vztah řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

1.2 Smluvní strany prohlašují, že jejich identifikační údaje uvedené v záhlaví Smlouvy jsou v souladu se skutečností v době uzavření této Smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí písemně bez prodlení druhé Smluvní straně. V případě změny účtu Dodavatele je Dodavatel povinen rovněž doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu. Při změně identifikačních údajů (s výjimkou IČO) Smluvních stran včetně změny účtu není nutné uzavírat ke Smlouvě dodatek.

1.3 Smluvní strany prohlašují, že osoby podepisující Smlouvu jsou k tomuto právnímu jednání oprávněny.

1.4 Pojmy s velkými počátečními písmeny případně uvozené slovy „dále jen“ či „dále též jen“ definované v této Smlouvě budou mít význam, jenž je jim ve Smlouvě včetně jejích příloh a dodatků připisován. Odkazy na právní předpisy zahrnují i předpisy, které je případně v budoucnu nahradí.

1.5 Smlouva byla uzavřena na základě výsledku zadávacího řízení na veřejnou zakázku s názvem „Identity Management – realizace“ (dále jen „**zadávací řízení**“ a „**veřejná zakázka**“) zadávanou Objednatelem jako zadavatelem dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“).

1.6 Dodavatel dále prohlašuje, že se náležitě seznámil se všemi podklady, které byly součástí zadávacích podmínek veřejné zakázky a které stanoví požadavky na předmět, účel a cíl plnění této Smlouvy, a že je odborně způsobilý ke splnění všech jeho závazků podle této Smlouvy.

1.7 Dodavatel se dále zavazuje, že bude plnění předmětu této Smlouvy poskytovat v souladu s veškerými požadavky a za účelem a s cílem obsaženým v zadávacích podmínkách veřejné zakázky (dále jen „**zadávací podmínky**“) a v souladu se svou nabídkou.

1.8 Pro vyloučení jakýchkoliv pochybností o vztahu Smlouvy a zadávacích podmínek jsou stanovena tato výkladová pravidla:

1.8.1 v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel veřejné zakázky vyjádřený v zadávacích podmínkách;

1.8.2 v případě chybějících ustanovení Smlouvy budou použita dostatečně konkrétní ustanovení zadávacích podmínek;

1.8.3 v případě rozporu mezi ustanoveními Smlouvy a zadávacích podmínek budou mít přednost ustanovení této Smlouvy.

1.9 Dodavatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění dle této Smlouvy, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění dle této Smlouvy a že disponuje takovým technickým vybavením, kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění dle této Smlouvy za dohodnutou smluvní cenu uvedenou v této Smlouvě, a to rovněž ve vazbě na kvalifikaci pro plnění veřejné zakázky jím prokázanou v zadávacím řízení.

1.10 Dodavatel se zavazuje plnit předmět Smlouvy v souladu s platnými právními předpisy, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že postupy a služby, případně materiály či výrobky, vyhovují předmětu Smlouvy a veškerým zadávacím podmínkám.

2. Účel smlouvy

2.1 Účelem Smlouvy je zabezpečení hospodárného, efektivního a účelného plnění zákonných a smluvních povinností Objednatele, jakož i zajištění kvalitních, moderních a dynamických služeb pro klienty Objednatele a jeho partnerů, prostřednictvím provedení díla poskytování služeb v rozsahu specifikovaném v čl. 3 a ostatních ustanoveních této Smlouvy a jejích příloh.

3. Předmět smlouvy

3.1 Předmětem této Smlouvy je závazek Dodavatele poskytovat Objednateli za podmínek uvedených plnění v následujícím rozsahu:

3.1.1 SW řešení pro správu identit v rozsahu požadavků dle čl. 1 přílohy č. 1 (dále též jen „**Základní požadavky**“ a „**Dílo**“).

3.1.2 Rozšíření Díla o funkcionality dle čl. 2 přílohy č. 1 na základě objednávky Objednatele (dále též jen „**Další požadavky**“).

3.1.3 Rozšíření Díla o funkcionalitu dle čl. 3 přílohy č. 1 na základě objednávky Objednatele (dále též jen „**Zabezpečení privilegovaných účtů**“ nebo „**PAM**“).

Realizované Další požadavky a PAM se stávají součástí Díla. (Dílo je dále ve Smlouvě označováno též jako „**IdM**“).

3.1.4 Pravidelná auditní zpráva dle čl. 4 přílohy č. 1 (dále též jen „**Pravidelná auditní zpráva**“).

3.1.5 Úprava směrnic dle čl. 5 přílohy č. 1 na základě objednávky Objednatele (dále též jen „**Úprava směrnic**“).

3.1.6 Služby technické podpory dle čl. 6.1 přílohy č. 1 (dále též jen „**Technická podpora**“) a služby podpory výrobce (dále společně jen „**Podpora**“).

Služby rozvoje, změnové požadavky a konzultace dle čl. 6.2 přílohy č. 1 (dále též jen „**Rozvoj“**).

3.1.7 Dodávka HW řešení v případě, že pro plnění předmětu Smlouvy nepostačuje architektura Objednatele dle čl. 7 přílohy č. 1 a Dodavatel toto HW řešení učinil součástí nabídky v zadávacím řízení (dále též jen „**Dodávka HW**“), a to včetně jeho podpory.

Dodávka SW řešení v případě, že pro plnění předmětu Smlouvy nepostačuje architektura Objednatele dle čl. 7 přílohy č. 1 a Dodavatel toto SW řešení učinil součástí nabídky v zadávacím řízení (dále též jen „**Dodávka SW**“).

(Vše dále společně též jen „**předmět plnění**“ nebo „**předmět Smlouvy**“.)

Detailní specifikaci, obsah, náležitosti a detailní vymezení provozních a dalších parametrů předmětu plnění uvádí příloha č. 1.

3.2 Předmětem této Smlouvy je dále závazek Objednatele uhradit cenu plnění ve výši a způsobem sjednaným v této Smlouvě.

4. Doba a místo plnění

4.1 Doba plnění je stanovena následovně

4.1.1 Základní požadavky

4.1.1.1 Dodavatel dodá do 1 měsíce od účinnosti Smlouvy detailní harmonogram plnění, který musí respektovat dále uvedené doby plnění.

4.1.1.2 Dodavatel dodá do 12 měsíců od účinnosti Smlouvy počáteční analýzu ve smyslu čl. 1.2.1 přílohy č. 1.

4.1.1.3 Dodavatel dodá Dílo v rozsahu Základních požadavků do 24 měsíců od účinnosti Smlouvy.

4.1.1.4 Nedohodnou-li se Smluvní strany jinak, bude Dílo nejméně 4 měsíce před nasazením do ostrého provozu (dále jen „**provoz**“) nasazeno do testovacího prostředí. V případě, že testování Díla v testovacím prostředí bude z důvodů na straně Objednatele přerušeno, prodlužují se o dobu takového přerušení navazující doby plnění (zejména doba dokončení testování a doba dodání Díla). Ustanovení tohoto odst. 4.1.1.4 se přiměřeně aplikuje i na případné

přerušení testování při dodání Dalších požadavků, PAM nebo výstupů Rozvoje.

4.1.2 Další požadavky

4.1.2.1 V případě, že Objednatel objedná Další požadavky společně s akceptací počáteční analýzy nebo bezodkladně po ní, dodá je Dodavatel do provozu společně se Základními požadavky do 24 měsíců od účinnosti Smlouvy.

4.1.2.2 V případě, že Objednatel objedná další požadavky později než dle čl. 4.1.2.1, dodá je Dodavatel do provozu ve lhůtě 12 měsíců od doručení Objednávky, nedohodnou-li se Smluvní strany jinak.

4.1.3 Zabezpečení privilegovaných účtů

4.1.3.1 V případě, že Objednatel objedná PAM s akceptací počáteční analýzy nebo bezodkladně po ní, dodá jej do provozu Dodavatel společně se Základními požadavky do 24 měsíců od účinnosti Smlouvy.

4.1.3.2 V případě, že Objednatel objedná PAM později než dle předchozí věty, dodá jej do provozu Dodavatel ve lhůtě 18 měsíců od doručení Objednávky, nedohodnou-li se Smluvní strany jinak.

4.1.4 Pravidelná auditní zpráva bude poprvé dodána po uplynutí 6 měsíců provozu Díla a dále vždy pravidelně každých 6 měsíců. Objednatel je oprávněn jednostranně určit, že požaduje pravidelnou auditní zprávu pouze 1x ročně nebo ji vůbec nepožaduje.

4.1.5 Úprava směrnic bude poskytována na základě objednávky Objednatele. Dodavatel předá Objednateli znění upravené směrnice v přiměřené době před nasazením Díla, jeho části nebo výsledku služeb Rozvoje, jichž se úprava směrnice týká, do provozu (dále jen „**nasazení funkcionality do provozu**“). Přiměřenou dobou dle předchozí věty se rozumí doba, během níž bude Objednatel schopen provést kontrolu provedené úpravy směrnice, akceptaci a vnitřní schvalovací proces; nedohodnou-li se Smluvní strany jinak, činí tato doba alespoň 1 měsíc před nasazením funkcionality do provozu.

4.1.6 Podpora bude poskytována od okamžiku zahájení provozu IdM na dobu neurčitou.

Rozvoj bude poskytován po dobu neurčitou. Doba splnění požadavku na Rozvoj bude stanovena dohodou Smluvních stran.

4.1.7 Dodávka HW a/nebo SW bude poskytnuta tak, aby bylo možno zahájit řádné a včasné plnění té části předmětu plnění, pro který je potřebná.

4.1.8 V případě potřeby školení nad rámec rozsahu dle čl. 1.4 přílohy č. 1 bude školení realizováno v termínu stanoveném dohodou Smluvních stran.

4.2 Nestanoví-li tato Smlouva jinak, je místem plnění sídlo Objednatele.

4.3 V případech, kdy z charakteru poskytovaného předmětu plnění nebo jeho části nevyplývá nezbytně nutná přítomnost pracovníků Dodavatele pověřených tímto plněním na místě plnění, poskytuje Dodavatel daný předmět plnění prostřednictvím vzdáleného přístupu ze svého pracoviště, a to za podmínky splnění bezpečnostních požadavků Objednatele Dodavatelem. K tomu Objednatel zabezpečí vytvoření chráněného vzdáleného přístupu z pracoviště Dodavatele do počítačové sítě Objednatele, včetně zřízení přístupových práv potřebných pro administraci.

4.4 Pro poskytování předmětu plnění ze svého pracoviště je Dodavatel na svém pracovišti povinen:

4.4.1 zajistit dodržování pravidel pro řízení přístupu a komunikací u ICT prostředků využívaných pro plnění této Smlouvy v minimálně stejné úrovni, jaká je stanovena pro

ICT prostředky Objednatele bezpečnostní politikou a příslušnými směrnicemi Objednatele, které nepřesahují rozsah ZoKB;

4.4.2 umožnit Objednateli v jím zvoleném čase i bez předchozího vyzvání kontrolu prostor dle čl. 4.3 Smlouvy v rozsahu umožňujícím Objednateli ověřit splnění povinností Dodavatele.

5. Cena a platební podmínky

5.1 Cena za předmět plnění je stanovena dohodou na základě nabídky Dodavatele podané v zadávacím řízení. Dílčí části ceny jsou stanoveny v příloze č. 2 Smlouvy, přičemž platí následující

5.1.1 Základní požadavky (položka A.1)

- 20 % ceny položky A.1 bude uhrazeno po akceptaci počáteční analýzy ve smyslu čl. 1.2.1 přílohy č. 1;
- 10 % ceny položky A.1 bude uhrazeno po nasazení Díla do testovacího prostředí;
- 60 % ceny položky A.1 bude uhrazeno po akceptaci Díla v rozsahu Základních požadavků a jeho nasazení do provozu;
- 10 % ceny položky A.1 bude uhrazeno po 1 měsíci provozu Díla za předpokladu odstranění všech provozních chyb (pokud v době 1 měsíci provozu Díla nebudou odstraněny všechny provozní chyby, bude tato část ceny položky A.1 uhrazena až po jejich odstranění).

5.1.2 Další požadavky (položka A.2, resp. její podpoložky)

- 30 % ceny položky A.2 (resp. její podpoložky) bude uhrazeno po nasazení Dalšího požadavku do testovacího prostředí;
- 60 % ceny položky A.2 (resp. její podpoložky) bude uhrazeno po akceptaci Dalšího požadavku a jeho nasazení do provozu;
- 10 % ceny položky A.2 (resp. její podpoložky) bude uhrazeno po 1 měsíci provozu Dalšího požadavku za předpokladu odstranění všech provozních chyb (pokud v době 1 měsíci provozu Díla nebudou odstraněny všechny provozní chyby, bude tato část ceny položky A.2 (resp. její podpoložky) uhrazena až po jejich odstranění).

5.1.3 Cena za zabezpečení privilegovaných účtů (položka A.3)

- 30 % ceny položky A.3 bude uhrazeno po nasazení PAM do testovacího prostředí;
- 60 % ceny položky A.3 bude uhrazeno po akceptaci PAM a jeho nasazení do provozu;
- 10 % ceny položky A.3 bude uhrazeno po 1 měsíci provozu PAM za předpokladu odstranění všech provozních chyb (pokud v době 1 měsíci provozu Díla nebudou odstraněny všechny provozní chyby, bude tato část ceny položky A.3 uhrazena až po jejich odstranění).

5.1.4 Cena pravidelné auditní zprávy (položka I) bude uhrazena vždy po její akceptaci. Cena jedné pravidelné auditní zprávy se nemění v případě, kdy Objednatel změní její periodicitu na 1x ročně, jedná se o cenu za kus. Pokud Objednatel sdělí požadavek na zrušení zpracovávání pravidelných auditních zpráv, nemá Dodavatel nárok ani na úhradu jejich ceny.

5.1.5 Cena za Úpravu směrnic (položka J) bude hrazena v rozsahu skutečně poskytnutých hodin služeb na objednávku, a to po jejich akceptaci. Objem uvedený v příloze č. 2

Smlouvy byl stanoven pro účely stanovení nabídkové ceny v zadávacím řízení a může se změnit. Objednatel může odebrat tyto služby v menším, větším nebo žádném rozsahu.

5.1.6 Cena za Rozvoj (položka G) bude hrazena v rozsahu skutečně poskytnutých hodin služeb na objednávku, a to čtvrtletně zpětně. Objem uvedený v příloze č. 2 byl stanoven pro účely stanovení nabídkové ceny v zadávacím řízení a může se změnit. Objednatel může odebrat tyto služby v menším, větším nebo žádném rozsahu.

5.1.7 Cena za Dodávku HW (položka K) bude uhrazena za cenu ve výši uvedené na listu 2 přílohy č. 2, a to po její akceptaci.

5.1.8 Cena za licence (položky B) a Dodávku SW (položka M) bude hrazena 1 x ročně vždy po akceptaci části předmětu plnění, k němuž se tyto položky váží.

5.1.9 Cena za Podporu (položky C) a podporu HW (položka L) bude hrazena čtvrtletně zpětně vždy po skončení příslušného čtvrtletí (období 3 měsíců); čtvrtletní cena bude spočítána jako ¼ roční ceny uvedené v položce C nebo L.

5.1.10 V případě zvýšení počtu uživatelů, účtů, služeb, zařízení či systémů proti počtům uvedeným v příloze č. 1 Smlouvy má dodavatel nárok na tzv. inkrementální nárůst ceny za licence případně podporu příslušné části předmětu plnění o částky uvedené v příloze č. 2 (položky D, E, F). Inkrementální nárůst ceny je možno provést vždy 1x ročně.

5.1.11 V případě, že na základě počáteční analýzy bude učen vyšší počet uživatelů, účtů, služeb, zařízení či systémů proti počtům uvedeným v příloze č. 1 Smlouvy, bude inkrementální nárůst ceny hrazen od počátku poskytování licence či podpory pro takový vyšší počet.

5.1.12 V případě, že na základě počáteční analýzy bude určen nižší počet uživatelů, účtů, služeb, zařízení či systémů proti počtům uvedeným v příloze č. 1 Smlouvy anebo jejich počet bude v průběhu doby plnění snížen, bude provedeno inkrementální snížení ceny, přičemž tato snížená cena bude hrazena od počátku poskytování licence či podpory pro takový nižší počet. Dojde-li ke snížení počtu uživatelů, účtů, služeb, zařízení či systémů proti počtům uvedeným v příloze č. 1 Smlouvy později v průběhu doby plnění Smlouvy, bude provedeno inkrementální snížení ceny, které lze provést vždy po uplynutí 12 měsíců poskytování příslušné části předmětu plnění. Inkrementální snížení ceny bude provedeno vždy o stejnou částku, které by odpovídala inkrementálnímu nárůstu (tj. například u položky E.1 je nárůst ceny za zvýšený počet uživatelů stanoven za každých 20 uživatelů, o stejnou částku bude snížena cena za snížení počtu uživatelů o jednoho až dvacet).

5.1.13 Cena za školení dle čl. 1.4 přílohy č. 1 (položka H) je stanovena jako paušální částka. V případě potřeby školení nad rámec rozsahu dle čl. 1.4 přílohy č. 1 bude školení realizováno a hrazeno v rámci služeb Rozvoje dle skutečně poskytnutých služeb na objednávku.

5.2 Veškeré ceny uvedené v příloze č. 2 jsou cenami maximálními, nepřekročitelnými a nejvýše přípustnými. Součástí cen uvedených v příloze č. 2 jsou veškeré práce, poplatky a veškeré jiné náklady nezbytné pro řádné a úplné poskytování předmětu plnění. Součástí ceny jsou i práce, které v zadávací dokumentaci nebo této Smlouvě výslovně uvedeny nejsou, ale Dodavatel jakožto odborník o nich měl vědět nebo mohl vědět, že jsou k řádnému plnění předmětu této Smlouvy nezbytné.

5.3 Veškeré ceny uvedené v příloze č. 2 jsou ceny v korunách českých. Stane-li se v průběhu trvání Smlouvy Česká republika členem Evropské měnové unie a bude-li závazně stanoven koeficient pro přepočet CZK na EUR, budou ceny sjednané v CZK přepočteny na EUR na základě tohoto koeficientu sjednaného v příslušných mezinárodních úmluvách, kterými bude

Česká republika vázána, jakož i v souladu s případnou tomu odpovídající vnitrostátní právní úpravou České republiky.

5.4 Dodavatel odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy.

5.5 Veškeré ceny je možné v průběhu plnění Smlouvy změnit z důvodu, že dojde v době trvání Smlouvy ke změnám právních předpisů upravujících výši daně z přidané hodnoty. Změna smluvní ceny bude odpovídat výši změny (změně sazby) daně z přidané hodnoty.

5.6 Cena za řádně poskytnutý předmět plnění nebo jeho část bude Dodavateli hrazena na základě daňového dokladu – faktury (dále jen „**faktura**“).

5.7 Lhůta splatnosti fakturovaných částek je stanovena na 30 (slovy: třicet) kalendářních dní od doručení faktury Objednateli. Dodavatel se zavazuje odeslat fakturu Objednateli nejpozději následující pracovní den po jejím vystavení. V případě, že má lhůta splatnosti faktury uplynout v období od 16. do 31. prosince, bude se za poslední den lhůty splatnosti takovéto faktury považovat první pracovní den po skončení uvedeného období. Faktura bude doručena doporučenou listovní zásilkou nebo datovou schránkou. Totožná lhůta splatnosti je stanovena i pro placení jiných plateb dle této Smlouvy (smluvních pokut, úroků z prodlení, náhrady škody apod.).

5.8 Faktury musí obsahovat evidenční číslo Smlouvy, případně identifikaci dílčí objednávky, údaj o pojmenování akce „Identity Management – realizace“ a veškeré údaje vyžadované právními předpisy, zejména ustanovením § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**ZDPH**“), a § 435 OZ. Dodavatel je povinen k Fakturám připojit kopie příslušných akceptačních protokolů, pokud je Smlouva vyžaduje. Dodavatel je k fakturám povinen připojit report uplatněných slev ve smyslu čl. 14 Smlouvy.

5.9 Dodavatel, poskytovatel zdanitelného plnění, je povinen bezprostředně, nejpozději do 2 (slovy: dvou) pracovních dnů od zjištění insolvence, popř. od vydání rozhodnutí správce daně, že je Dodavatel nespolehlivým plátcem dle § 106a ZDPH oznámit takovou skutečnost prokazatelně Objednateli, příjemci zdanitelného plnění. Porušení této povinnosti je Stranami považováno za podstatné porušení Smlouvy.

5.10 Dodavatel se zavazuje, že bankovní účet jím určený pro zaplacení jakéhokoliv závazku Objednatele na základě Smlouvy bude od data podpisu Smlouvy do ukončení její platnosti zveřejněn způsobem umožňující dálkový přístup ve smyslu § 96 odst. 2 ZDPH, v opačném případě je Dodavatel povinen sdělit Objednateli jiný bankovní účet řádně zveřejněný ve smyslu § 96 ZDPH. Pokud bude Dodavatel označen správcem daně za nespolehlivého plátce ve smyslu § 106a ZDPH, zavazuje se zároveň o této skutečnosti neprodleně informovat Objednatele spolu s uvedením data, kdy tato skutečnost nastala.

5.11 Objednatel může ve lhůtě splatnosti fakturu vrátit k opravě či doplnění, pokud

- obsahuje nesprávné nebo neúplné cenové údaje;
- obsahuje nesprávné nebo neúplné náležitosti;
- Dodavatel nemá bankovní účet uvedený na faktuře řádně registrovaný v databázi „Registrů plátců DPH“.

5.12 Vrácením faktury Dodavateli se ruší lhůta splatnosti a nová lhůta splatnosti počne běžet doručením faktury nové nebo opravené. Tento postup lze uplatnit i opakovaně.

5.13 Smluvní strany se dohodly na tom, že Dodavatel není oprávněn činit jednostranná započtení svých pohledávek vzniklých na základě Smlouvy či v souvislosti s ní vůči jakýmkoliv pohledávkám Objednatele. Pohledávky a nároky Dodavatele vzniklé na základě Smlouvy či v souvislosti s ní nesmějí být Dodavatelem postoupeny třetím osobám, zastaveny, nebo s nimi jinak disponováno bez předchozího písemného souhlasu Objednatele (včetně zákazu

Dodavatele postoupit Smlouvu). Jakýkoliv právní úkon učiněný Dodavatelem v rozporu s tímto ustanovením bude považován za příčící se dobrým mravům.

5.14 Platby peněžitých částek se provádějí bankovním převodem na účet druhé Smluvní strany uvedený ve faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odepsání z účtu odesílatele ve prospěch účtu příjemce. Dodavatel není oprávněn nárokovat bankovní poplatky nebo jiné náklady vztahující se k převodu poukazovaných částek mezi Smluvními stranami na základě této Smlouvy.

6. Práva a povinnosti Smluvních stran

6.1 Dodavatel se zavazuje:

6.1.1 při poskytování předmětu plnění dle této Smlouvy postupovat v profesionální kvalitě a s odbornou péčí, podle svých nejlepších znalostí a schopností, aplikovat procesy „best practice“; dostane-li se Dodavatel do prodlení s povinností poskytovat předmět plnění řádně z důvodů na jeho straně po dobu delší než 30 (slovy: třicet) kalendářních dnů, je Objednatel oprávněn zajistit plnění dle této Smlouvy po dobu prodlení Dodavatele jinou osobou; v takovém případě nese náklady spojené s náhradním plněním Dodavatel;

6.1.2 poskytovat předmět plnění řádně a včas, a to bez faktických a právních vad a v kvalitě definované v jednotlivých Service Level Agreements (dále jen „SLA“); SLA uvedené v příloze č. 1 je Dodavatel povinen zachovat i pro HW a SW dodaný v souladu s čl. 7 přílohy č. 1;

6.1.3 upozorňovat Objednatele včas na všechny hrozící vady či potenciální výpadky plnění na straně Dodavatele, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění Smlouvy nezbytné;

6.1.4 informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách plnění, byť by za ně Dodavatel neodpovídal, o vznesených požadavcích orgánů státního dozoru a o uplatněných nárocích třetích osob, které by mohly plnění této Smlouvy jakýmkoli způsobem ovlivnit;

6.1.5 neprodleně písemně nebo na kontrolním dnu oznámit Objednateli překážky, které mu brání v řádném plnění předmětu Smlouvy a výkonu dalších činností souvisejících s plněním předmětu Smlouvy;

6.1.6 neprodleně písemně oznámit Objednateli změny svého majetkoprávního postavení, jako je např. přeměna společnosti, snížení základního kapitálu, vstup do likvidace, úpadek či prohlášení konkurzu apod.; tím není dotčeno ustanovení čl. 16.4;

6.1.7 upozornit Objednatele na Dodavateli známá specifická, tj. nejedná se o obecně známá, potenciální rizika vzniku škod a je-li to v rozsahu jím poskytovaného plnění možné, včas a řádně s nejvyšší odbornou péčí provést taková opatření, která riziko vzniku škod zcela vyloučí nebo dostatečně sníží, jde-li o rizika vzniku škod nezapříčiněných Dodavatelem, má Dodavatel právo na úhradu nezbytných a účelně vynaložených nákladů;

6.1.8 i bez pokynů Objednatele provést neodkladně nutné úkony, které, ač nejsou předmětem této Smlouvy, pokud budou s ohledem na nepředvídané okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody; jde-li o zamezení vzniku škod nezapříčiněných Dodavatelem, má Dodavatel právo na úhradu nezbytných a účelně vynaložených nákladů; Dodavatel však zároveň bez zbytečného odkladu informuje Objednatele o nutnosti provést neodkladně nutné úkony;

6.1.9 dodržovat bezpečnostní, hygienické, požární, organizační a ekologické předpisy na pracovištích Objednatele, se kterými byl seznámen nebo které jsou všeobecně známé a dále zajistit, aby i všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy Objednatele, s nimiž Objednatel Dodavatele předem obeznámil nebo které jsou všeobecně známé;

6.1.10 průběžně informovat Objednatele o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností Smluvních stran;

6.1.11 účastnit se kontrolních dní a projektových schůzek s Objednatelem. Nedohodnou-li se smluvní strany jinak,

- do doby nasazení Díla v rozsahu Základních požadavků do provozu budou probíhat projektové schůzky 1x týdně v sídle Objednatele,
- od nasazení Díla v rozsahu Základních požadavků do provozu po celou dobu účinnosti Smlouvy budou probíhat kontrolní dny, a to 1x měsíčně v sídle Objednatele;

6.1.12 respektovat práva duševního vlastnictví Objednatele;

6.1.13 písemně upozorňovat Objednatele na možné či vhodné rozšíření či změny Díla za účelem jeho lepšího využívání v rozsahu této Smlouvy;

6.1.14 písemně upozorňovat Objednatele na případnou nevhodnost pokynů Objednatele. Pokud Dodavatel Objednatele neupozornil na nevhodnost pokynů Objednatele a prokazatelně mohl dovodit možnost, že jejich provedení povede ke vzniku vad a způsobí bezprostřední škodu Objednateli a/nebo Dodavateli a/nebo třetím osobám, nese Dodavatel odpovědnost za vady a za škodu, které v důsledku pokynů Objednatele vznikly Objednateli a/nebo Dodavateli a/nebo třetím osobám. V případě, že Objednatel trvá na provedení pokynu i přesto, že byl Dodavatelem řádně upozorněn na nevhodnost takového pokynu, Dodavatel nenese odpovědnost za vady a za škodu, které v důsledku pokynů Objednatele Objednateli a/nebo Dodavateli a/nebo třetím osobám vznikly. Upozornění Objednatele na nevhodnost pokynů Objednatele bude Dodavatel provádět v písemné formě dostatečně srozumitelným způsobem, zejména zápisem do Provozního deníku s řádným označením „UPOZORNĚNÍ NA NEVHODNÝ POKYN OBJEDNATELE“, přičemž jednotlivá upozornění na nevhodné pokyny Objednatele budou vzestupně číslována.

6.2 Objednatel se zavazuje poskytnout ke splnění smluvních závazků Dodavateli včas nezbytnou součinnost a informace definované v této Smlouvě nebo potřebné pro účelné plnění předmětu této Smlouvy a dále bude neprodleně odpovědné zástupce Dodavatele informovat o všech organizačních změnách, poznatcích z kontrolní činnosti, podnětech vlastních zaměstnanců a třetích stran a dalších skutečnostech potřebných pro efektivní plnění předmětu Smlouvy, jakož i dílčích plnění sjednaných dle této Smlouvy.

6.3 Dodavatel je povinen zajistit plnění této Smlouvy prostřednictvím osob, které mají potřebnou kvalifikaci i zkušenosti k plnění svých úkolů. Dodavatel je povinen zajistit plnění příslušné části předmětu plnění pomocí osob, jejichž prostřednictvím prokázal splnění kvalifikace v zadávacím řízení, jakož i dalšími, které uvedl jako členy týmů (viz příloha č. 4). Dodavatel je oprávněn změnit osobu uvedenou v příloze č. 4 pouze s písemným předchozím souhlasem Objednatele. Objednatel tento souhlas neposkytne, pokud Dodavatel neprokáže, že nový člen týmu splňuje kvalifikaci pro něj stanovenou v zadávacích podmínkách.

6.4 Dodavatel je povinen písemně informovat Objednatele o všech svých poddodavatelích (včetně jejich identifikačních a kontaktních údajů a o tom, které části předmětu plnění dle této Smlouvy pro něj v rámci předmětu plnění každý z poddodavatelů poskytuje) a o jejich změně,

a to nejpozději do 7 (slovy: sedmi) kalendářních dnů ode dne, kdy Dodavatel vstoupil s poddodavatelem do smluvního vztahu, či ode dne, kdy nastala změna. Dodavatel je oprávněn změnit poddodavatele, pomocí něhož prokázal část splnění kvalifikace v rámci zadávacího řízení, jen z vážných objektivních důvodů a s předchozím písemným souhlasem Objednatele, přičemž nový poddodavatel musí disponovat kvalifikací ve stejném či větším rozsahu, jako původní poddodavatel, jehož prostřednictvím Dodavatel prokázal část kvalifikace. Objednatel nesmí souhlas se změnou poddodavatele bez vážných důvodů odmítnout, pokud mu budou příslušné doklady ve sjednané lhůtě předloženy. Tím není dotčena odpovědnost Dodavatele za poskytování řádného plnění dle této Smlouvy.

6.5 Dodavatel je povinen udržovat po celou dobu účinnosti této Smlouvy v platnosti veškeré certifikáty a osvědčení stanovené v zadávacích podmínkách veřejné zakázky pro prokázání splnění kvalifikace Dodavatele.

6.6 Dodavatel je povinen poskytnout veškerou potřebnou součinnost všem institucím a osobám, které vykonávají kontrolu a dohled nad činností pojišťoven v České republice, zejména pak České národní bance. Dodavatel je v této souvislosti zejména povinen poskytnout všem oprávněným institucím a osobám veškeré doklady vztahující se k realizaci plnění Smlouvy, umožnit průběžné ověřování souladu údajů o realizaci plnění a v případě provádění kontroly se této kontrole podrobit. Při poskytování součinnosti podle tohoto článku není Dodavatel oprávněn zpřístupnit příslušným institucím a osobám informace ve větším rozsahu, než ke kterému by byl povinen v daném případě sám Objednatel na základě příslušných právních předpisů. Dodavatel je dále povinen poskytnout přímo Objednateli veškerou potřebnou součinnost při provádění kontroly a dohledu nad Objednatelem ze strany příslušných institucí a osob.

6.7 Dodavatel se zavazuje umožnit osobám oprávněným k výkonu kontroly provést kontrolu dokladů souvisejících s plněním předmětu Smlouvy, a to po dobu nejméně 10 (slovy: deseti) let od ukončení financování předmětu Smlouvy, způsobem, který je v souladu s platnými právními předpisy České republiky a Evropské unie. Při poskytování součinnosti podle tohoto článku není Dodavatel oprávněn zpřístupnit osobám oprávněným k výkonu kontroly doklady ve větším rozsahu, než ke kterému by byl povinen v daném případě sám Objednatel na základě příslušných právních předpisů. Dodavatel je dále povinen poskytnout přímo Objednateli veškerou potřebnou součinnost při provádění kontroly dokladů Objednatele souvisejících s plněním předmětu Smlouvy ze strany osob oprávněných k výkonu kontroly.

6.8 Dodavatel je povinen na žádost Objednatele spolupracovat či poskytnout součinnost případným dalším dodavatelům Objednatele. Náklady Dodavatel na tuto spolupráci či součinnost bude Objednatel Dodavateli hradit jako náklady na poskytování služby Rozvoj.

6.9 Objednatel je rovněž oprávněn spolupracovat při provádění dohledu nad průběhem plnění dle této Smlouvy s vybranou, nezávislou, odborně erudovanou třetí osobou pro zajištění odborné garance řádného plnění na straně Objednatele. Dodavatel je povinen plně respektovat postavení takové třetí osoby, spolupracovat s ní a poskytnout jí přiměřenou součinnost dle pokynů Objednatele. Tato třetí osoba nesmí být ani v nepřímém konkurenčním postavení k Dodavateli nebo jeho poddodavatelům; Dodavatel má v tomto případě právo součinnost odmítnout.

6.10 Objednatel vede v service desk Provozní deník a Dodavatel i Objednatel do něj zaznamenávají veškeré provedené provozní změny. Za řádnou funkčnost a zajištění nepřetržitého vzdáleného přístupů k Provoznímu deníku pro Dodavatele zodpovídá Objednatel.

6.11 Dodavatel odpovídá za závady na provozním prostředí způsobené SW třetích stran, které jsou součástí IdM a je povinen navrhnout taková opatření, aby byla závada odstraněna či nalezeno dočasné náhradní řešení pro zprovoznění požadovaného plnění. Objednatel poskytne maximální možnou součinnost při plnění tohoto požadavku.

6.12 Dodavatel je povinen se vyvarovat poškození nebo zničení jakýchkoliv dat, která se nacházejí v provozní části IdM. Za data uložená v prostředí Objednatele a jejich případnou ztrátu či poškození nezpůsobené činností Dodavatele Dodavatel nezodpovídá. V případě modifikace dat provozní databáze při zásahu, který si vyžádal Objednatel nebo se provádí po předchozím projednání s Objednatelem, Objednatel vždy data před tímto zásahem zálohuje.

6.13 Dodavatel je povinen při výkonu svých činností respektovat potřeby provozu Objednatele tak, aby nebyly narušeny činnosti Objednatele. Pro účely plnění této Smlouvy Objednatel po dohodě s Dodavatelem zajistí odstávku (nedostupnost) IdM tak, aby mohl Dodavatel provést potřebné úkony.

7. Objednávky, změnové řízení

7.1 Objednávky

7.1.1 Návrh objednávky části předmětu plnění musí být Objednatelem učiněn písemně a doručen Dodavateli.

7.1.2 Jde-li o části předmětu plnění, za které tato smlouva stanoví v příloze č. 2 pevnou nikoliv hodinovou cenu (Další požadavky, PAM a jejich licence a Podpora, Dodávka HW vč. podpory a SW), Dodavatel v odpovědi na návrh objednávky navrhne termín splnění, případně dílčí harmonogram plnění a další relevantní podmínky plnění. Objednatel není povinen akceptovat delší termín plnění, než stanoví Smlouva. Obě smluvní strany podepíší konečné znění objednávky. V případě, že se Strany nedohodnou do 15 (slovy: patnácti) pracovních dnů na konečném znění objednávky, je Objednatel oprávněn jej stanovit jednostranně v souladu s touto Smlouvou.

7.1.3 Jde-li o části předmětu plnění, za které tato Smlouva stanoví cenu za hodinu (Úprava směrnic, Rozvoj, školení nad rámec rozsahu dle čl. 1.4 přílohy č. 1) použije se čl. 7.1.2 přiměřeně s tím, že Dodavatel navrhne předpokládaný rozsah plnění (počet hodin) a termín splnění. Podmínkou podpisu (příp. schválení dle následující věty) konečného znění objednávky je dohoda Smluvních stran o rozsahu a termínu (s)plnění. Nestanoví-li Objednatel jinak (např. pro určitý finanční limit), budou návrhy objednávek, odpovědi Dodavatele na ně a jejich schválení Objednatelem dle tohoto odstavce realizovány v service desk Objednatele, v němž bude probíhat také veškerý management takových objednávek a požadavků z nich plynoucích.

7.1.4 Nedohodnou-li se Smluvní strany jinak, je Dodavatel povinen učinit návrhy dle předchozích odstavců do 5 (slovy: pěti) pracovních dnů od doručení objednávky Objednatele. Opakovaná nesoučinnost Dodavatele v jednání o objednávce je považována za porušení Smlouvy podstatným způsobem.

7.2 Změnové řízení

7.2.1 Kterákoliv ze Smluvních stran je oprávněna písemně navrhnout změnu způsobu poskytování předmětu plnění. Žádná ze Smluvních stran však není povinna navrhovanou změnu akceptovat.

7.2.2 Dodavatel se zavazuje provést hodnocení dopadů kteroukoliv Smluvní stranou navrhovaných změn předmětu plnění podle čl. 7.2.1 na termíny plnění, cenu a součinnost Objednatele. Dodavatel je povinen toto hodnocení provést bez zbytečného odkladu, nejpozději do 10 (slovy: deseti) pracovních dnů ode dne doručení písemného návrhu změny od Objednatele, nedohodnou-li se smluvní strany na jiném termínu. V případě, že změny navrhuje Dodavatel, je povinen toto hodnocení dopadů předložit Objednateli současně s návrhem změny. Pokud Dodavatel změny nenavrhuje, náklady

Dodavatele na tuto činnost bude Objednatel Dodavateli hradit jako náklady na poskytování Rozvoje.

7.2.3 Jakékoliv změny předmětu plnění musí být sjednány v souladu se ZZVZ, a písemně ve formě dodatku k této Smlouvě podepsaného osobami oprávněnými zavazovat Smluvní strany, nestanoví-li tato Smlouva jinak. V závislosti na těchto písemných ujednáních může být upraven požadovaný rozsah plnění, termíny plnění, cena předmětu plnění, platební podmínky, součinnost Objednatele atd.

8. Akceptace výsledků poskytovaného plnění

8.1 Výsledky poskytnutého plnění dle této Smlouvy budou akceptovány Objednatelem na základě akceptační procedury.

8.2 Akceptační procedura zahrnuje ověření, zda poskytnuté plnění dle této Smlouvy vedlo k výsledku, ke kterému se Smluvní strany zavázaly touto Smlouvou, a to porovnáním skutečných vlastností jednotlivých dílčích výsledků plnění (výstupů) poskytnutých dle této Smlouvy s jejich specifikací uvedenou v této Smlouvě. Průběh akceptačního řízení bude zachycen v akceptačních protokolech. Je-li příslušná část předmětu plnění dle Smlouvy nebo dohody stran rozdělena na více fází (zejména počáteční analýza, nasazení do testovacího prostředí a nasazení do provozu), bude akceptační řízení včetně akceptačního protokolu realizováno pro každou z takových fází. Vzory akceptačních protokolů předá Objednatel Dodavateli po uzavření Smlouvy a může je v průběhu doby plnění změnit. Dodavatel je povinen zpracovávat protokoly dle vzoru stanovených Objednatelem. Má-li protokol přílohu, pro kterou není Objednatelem stanoven závazný vzor, je Dodavatel tuto přílohu zpracovávat ve strojově čitelných formátech MS Office.

8.3 Dodavatel se zavazuje v případě potřeby konzultovat práce na přípravě/zhotovení výstupu s Objednatelem a Objednatel se zavazuje obratem na konzultace reagovat.

8.4 Dodavatel se zavazuje předat výstup Objednateli k akceptaci ve lhůtě sjednané mezi Smluvními stranami na základě této Smlouvy, nebo jinak stanovené v souladu s touto Smlouvou. V pochybnostech má přednost lhůta, která byla za součinnosti a dohodou obou Smluvních stran v souladu s touto Smlouvou stanovena později.

8.5 Objednatel se zavazuje akceptovat předmětný výstup bez zbytečného odkladu, nebo vznést veškeré své výhrady nebo připomínky k výstupu předložené dle čl. 8.4 do 25 (slovy: dvaceti pěti) pracovních dnů od jejího doručení, nedohodnou-li se Smluvní strany v konkrétním případě jinak. Dodrží-li Objednatel lhůtu dle předchozí věty, neprodlužují se navazující doby plnění nebo celková doba plnění (zejména doba pro nasazení Základních požadavků, Dalších požadavků a PAM do provozu). Nedodrží-li Objednatel lhůtu dle první věty tohoto ustanovení, prodlužují se navazující doby plnění nebo celková doba plnění (zejména doba pro nasazení Základních požadavků, Dalších požadavků a PAM do provozu) o dobu prodlení Objednatele s akceptací, nedohodnou-li se smluvní strany jinak.

8.6 Dodavatel je povinen provést veškeré potřebné úpravy výstupu dle výhrad a připomínek Objednatele a takto upravený výstup předat Objednateli bez zbytečného odkladu, avšak nejpozději do 10 (slovy: deseti) pracovních dní od doručení výhrad nebo připomínek k výstupu, nedohodnou-li se Smluvní strany jinak.

8.7 V případě, že postupem podle čl. 8.5 a 8.6 nedojde k odstranění veškerých vzájemných rozporů mezi Smluvními stranami a akceptaci výstupu, Dodavatel může předkládat další verze výstupu a Objednatel k nim vznášet své výhrady až do konečné akceptace výstupu ze strany Objednatele, nedohodnou-li se Smluvní strany v konkrétním případě jinak.

8.8 Smluvní strany se zavazují po řádném předání a převzetí výstupu potvrdit toto předání a převzetí sepsáním písemného akceptačního protokolu příslušného dané části předmětu

plnění, který za Smluvní strany podepíší oprávněné osoby nejpozději do 5 (slovy: pěti) pracovních dnů od řádného předání a převzetí výstupu, nedohodnou-li se Smluvní strany v konkrétním případě jinak. Akceptační protokol jednotlivých výstupů musí být podepsán osobami oprávněnými jednat za Smluvní strany nebo osobami, které k tomu Smluvní strany výslovně písemně zmocnily.

8.9 Bude-li trvání akceptační procedury ovlivněné vznesením případných výhrad nebo připomínek k výstupu a potřebou jejich vyřešení, nebude to mít vliv na další termíny dohodnuté pro předání dalších výstupů.

8.10 Plnění Dodavatele dle této Smlouvy musí být dodáno ve lhůtách stanovených touto Smlouvou nebo na jejím základě. Plnění Dodavatele dle této Smlouvy budou osvědčená za řádně poskytnutá dnem podpisu akceptačního protokolu Objednatelem. Pro účely uplatnění slev z ceny a smluvních pokut (dále pro účely tohoto článku jen „**sankce**“) dle čl. 14 se sankce za prodlení s poskytnutím předmětu plnění aplikují pouze do doby předání předmětu plnění či jeho části k akceptaci. Pokud má Objednatel k výstupu plnění výhrady nebo připomínky, použijí se sankce za prodlení s předáním upraveného výstupu (tedy od předání se neaplikuje sankce za prodlení s předáním).

8.11 Objednatel je oprávněn akceptovat plnění Dodavatele i s drobnými vadami nebránícími řádnému užívání předmětu plnění nebo jeho části. Nárok na fakturaci však vzniká nejdříve k okamžiku odstranění všech vytčených vad předmětu plnění.

9. Odpovědnost za škodu, odpovědnost za vady, záruka

9.1 Dodavatel se zavazuje k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a této Smlouvy. Dodavatel odpovídá za škodu rovněž v případě, že část předmětu plnění poskytuje prostřednictvím poddodavatele.

9.2 Žádná ze Smluvních stran není odpovědná za škodu nebo prodlení způsobené mimořádnými nepředvídatelnými a nepřekonatelnými překážkami nezávislými na jejich vůli ve smyslu OZ. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na tyto vzniklé překážky bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání těchto překážek.

9.3 Dodavatel se zavazuje, že bude mít po celou dobu trvání této Smlouvy sjednánu pojistnou smlouvu, která se vztahuje na plnění předmětu této Smlouvy a jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění na jednu škodnou událost minimálně 20.000.000 Kč (slovy: dvacet milionů korun českých). Na žádost Objednatele je Dodavatel povinen Objednateli do 3 (slovy: tří) pracovních dnů od doručení žádosti předložit kopii pojistné smlouvy, případně pojistku či pojistný certifikát (dále jen „**pojistná smlouva**“).

9.4 Dodavatel je odpovědný za to, že poskytnutý předmět plnění je v souladu se zadávacími podmínkami veřejné zakázky a touto Smlouvou a že po dobu záruční doby bude mít dohodnuté vlastnosti, úroveň a charakteristiky.

9.5 Záruční doba činí

9.5.1 60 (slovy: šedesát) měsíců ode dne nasazení do provozu v případě Díla; u částí Díla předaných později (Další požadavky, PAM, výsledky Rozvoje) počíná běžet záruční doba samostatně ode dne jejich nasazení do provozu.

9.5.2 60 (slovy: šedesát) měsíců ode dne akceptace v případě dodávky HW; záruční doba počíná běžet samostatně ode dne akceptace každé samostatné dodávky.

9.5.3 60 (slovy: šedesát) měsíců ode dne akceptace v případě ostatních částí předmětu plnění.

9.6 Dodavatel je povinen plnit předmět plnění v nejvyšší dostupné kvalitě a odpovídá za to, že případné vady plnění poskytnutého dle této Smlouvy zjištěné v záruční době řádně odstraní, případně nahradí plněním bezvadným v souladu s touto Smlouvou. Tím není dotčen nárok Objednatele na náhradu prokázané škody vzniklé v souvislosti s touto vadou plnění způsobenou na straně Dodavatele, přičemž Dodavatel odpovídá za prokázanou škodu maximálně do výše limitu pojistného plnění dle čl. 9.3. Pokud Objednatel zjistí vady poskytovaného plnění dle této Smlouvy, je povinen oznámit takové vady Dodavateli neprodleně způsobem stanoveným v této Smlouvě a Dodavatel takové vady odstraní v souladu s touto Smlouvou.

9.7 Pokud byly vady předmětu plnění sděleny Objednatelem v době poskytování Podpory a/nebo podpory HW, pak pro jejich odstranění platí lhůty uvedené v čl. 6.1 přílohy č. 1.

9.8 Pokud byly vady předmětu plnění sděleny Objednatelem v době, kdy Dodavatel již není poskytována Podpora a/nebo podpory HW (ukončení Smlouvy, kdy však stále trvá záruční doba), je Dodavatel povinen odstranit vady ve lhůtě do 5 (slovy: pěti) pracovních dnů ode dne jejich sdělení Objednatelem, nedohodnou-li se smluvní strany jinak.

10. Vlastnické právo, právo užití, licenční ujednání

10.1 Vlastnické právo, právo užití

10.1.1 Dodavatel prohlašuje, že jím poskytované plnění dle této Smlouvy není zatíženo právy třetích osob za předpokladu, že Objednatel používá IdM v souladu s dokumentací a smluvním a licenčním ujednáním.

10.1.2 V případě, že součástí plnění Dodavatele podle této Smlouvy budou movité věci předávané Objednateli (zejména Dodávka HW), nabývá Objednatel vlastnické právo k těmto věcem dnem převzetí takového plnění Objednatelem. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem, kdy Objednatel věci převezme; o takovémto převzetí bude sepsán písemný protokol (případně dodací list) podepsaný Smluvními stranami nebo jejich oprávněnými osobami. Vlastnické právo Objednatel nabývá dnem podpisu akceptačního protokolu. Do okamžiku nabytí vlastnického práva uděluje Dodavatel Objednateli právo tyto věci užívat bezplatně v rozsahu a způsobem, který vyplývá z účelu této Smlouvy.

10.2 Licenční ujednání

10.2.1 Definice

V této Smlouvě, pokud z jejího kontextu nevyplývá jinak, mají níže uvedené pojmy následující význam:

10.2.1.1 „**Autorské dílo**“ znamená autorské dílo ve smyslu § 2 Autorského zákona; pro účely této Smlouvy se Autorským dílem rozumí Software a jakékoliv výstupy Poskytovatele vytvořené v rámci nebo v souvislosti s poskytováním Služeb, které splňují podmínky stanovené v § 2 Autorského zákona.

10.2.1.2 „**Autorský zákon**“ znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů;

10.2.1.3 „**Databáze**“ znamená databázi ve smyslu § 88 Autorského zákona;

10.2.1.4 „**Licence Software**“ má význam uvedený v čl.10.2.2.1;

10.2.1.5 „**Poddodavatel**“ znamená jakoukoliv osobu anebo subjekt, který je v postavení anebo který bude v postavení poddodavatele Dodavatele v rámci nebo v souvislosti s poskytováním předmětu plnění.

10.2.2 Udělení licence Dodavatelem

10.2.2.1 Dodavatel poskytuje Objednateli nevýhradní oprávnění (licenci, resp. podlicenci) k výkonu práva užít Autorská díla a k výkonu práva vytěžovat a zužitkovat Databáze vytvořené v rámci nebo v souvislosti s realizací předmětu plnění, a to v územně a technologicky neomezeném rozsahu a všemi známými způsoby užití, a to na celou dobu trvání majetkových práv autora (dále jen „**Licence Software**“). Množstevní určení vyplývá z přílohy č. 1, případně v souladu s touto Smlouvou navýšeného počtu uživatelů, účtů, služeb, zařízení či systémů.

10.2.2.2 Součástí Licence Software je rovněž neomezené právo Objednatele poskytnout třetím osobám podlicenci k užití Autorského díla v rozsahu shodném s rozsahem Licence Software za předpokladu, že tím nezpůsobí Dodavateli dodatečné náklady, souhlas Dodavatele k postoupení Licence Software na třetí osoby a souhlas Dodavatele udělený Objednateli k provedení jakýchkoliv změn nebo modifikací Autorského díla. Licence Software se automaticky vztahuje i na všechny nové verze, aktualizované verze i na úpravy Autorského díla dodané Dodavatelem. Dodavatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k Autorskému dílu a že má souhlas autorů k uzavření těchto licenčních ujednání a že toto prohlášení zahrnuje i taková práva autorů, která by vytvořením Autorského díla teprve vznikla.

10.2.2.3 Poskytovatel poskytuje Licenci Software v rozsahu dle čl. 10.2.2.1 a 10.2.2.2 této Smlouvy k počítačovým programům, které patří do skupiny Autorských děl ve smyslu Smlouvy, vyvíjených Dodavatelem. S ohledem na charakter technologické formy předmětu plnění je část software poskytována Dodavateli při implementaci přímo ve zdrojových textech. Licence Software se ve stejném rozsahu vztahuje k počítačovým programům ve zdrojovém a strojovém kódu. Dodavatel se ohledně Licence Software k počítačovým programům, které nejsou při implementaci přímo ve zdrojových textech a patří do skupiny Autorských děl ve smyslu Smlouvy, zavazuje poskytnout Dodavateli zdrojové kódy s komentáři takových počítačových programů a tyto v případě změny průběžně aktualizovat a poskytovat i dokumentaci provedených změn. Dodavatel se dále zavazuje předat Objednateli finální dokumentované zdrojové kódy těch počítačových programů, které patří do skupiny Autorských děl ve smyslu Smlouvy, v aktuální podobě nejpozději do 30 (slovy: třiceti) kalendářních dnů od skončení Smlouvy. Formu a způsob poskytnutí kódů uvedených v tomto článku stanoví Objednatel na základě posouzení konkrétních návrhů Dodavatele.

10.2.2.4 Smluvní strany výslovně prohlašují, že pokud při poskytování plnění dle Smlouvy vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Dodavatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena za licence je stanovena se zohledněním tohoto ustanovení a Dodavateli nevzniknou v případě vytvoření díla spoluautorů

žádné nové nároky na odměnu. Výše uvedené dílo spoluautorů nevznikne zadáním požadavku na Dodavatele ze strany Objednatele.

10.2.2.5 Dodavatel je povinen postupovat tak, aby udělení Licence Software k Autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci zabezpečil, a to bez újmy na právech třetích osob. Nebude-li možné po Dodavateli spravedlivě požadovat udělení Licence Software v rozsahu dle čl. 10.2.2.1 až 10.2.2.3, zejména proto, že se jedná o tzv. standardní počítačové programy, je Dodavatel povinen na to písemně Objednatele upozornit spolu s náležitým odůvodněním a poskytnout Objednateli nebo zajistit pro Objednatele bez nároku na další úplatu poskytnutí licence či podlicence v nejširším možném rozsahu, který Objednateli nezpůsobí dodatečné náklady. Postup dle předchozí věty je možný jen s výslovným písemným souhlasem Objednatele, přičemž se Objednatel zavazuje, že tento souhlas neodmítne poskytnout bez vážného důvodu.

10.2.2.6 Práva získaná v rámci plnění této Smlouvy přecházejí i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.

10.2.2.7 Ve vztahu k Licenci Software k Autorským dílům Dodavatel prohlašuje, že oprávněné zájmy autora nemohou být značně nepříznivě dotčeny tím, že Objednatel nebude Licenci vůbec či zčásti užívat. Bez ohledu na tuto skutečnost tímto Smluvní strany sjednávají, že právo Dodavatele na odstoupení dle § 2378 OZ není Dodavatel oprávněn uplatnit před uplynutím 10 (slovy: deseti) let od poskytnutí licence.

10.2.3 Udělení licence třetí osobou

10.2.3.1 Pro všechny případy, ve kterých nemůže Dodavatel z objektivních důvodů sám udělit Objednateli oprávnění dle čl. 10.2.2 k Autorskému dílu vytvořeným v rámci předmětu plnění, Dodavatel zajistí, že třetí osoba, jež vykonává majetková práva k příslušnému Autorskému dílu, udělí Objednateli bezúplatně výhradní oprávnění (licenci) Autorské dílo užít, resp. právo vytěžovat a zužitkovat Databázi, v rozsahu a za podmínek dle čl. 10.2.2, a dále výhradní oprávnění (licenci) užít zdrojové kódy k tomuto Autorskému dílu v rozsahu a za podmínek dle čl. 10.2.2, a to tak, že příslušné oprávnění bude Objednateli uděleno v písemně formě nejpozději v den předání příslušného Autorského díla.

10.2.3.2 Nebude-li Objednateli v den předání příslušného Autorského díla předloženo v písemné formě udělení oprávnění třetí osobou dle předchozí věty, znamená to, že příslušná oprávnění udělil Objednateli Dodavatel dle čl. 10.2.2.

10.2.4 Udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Dodavatele vypovědět.

10.2.5 Dodavatel prohlašuje, že veškeré jím dodané plnění podle Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého plnění dle Smlouvy. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním Dodavatele dle Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání Předmětu plnění či jeho části, zavazuje se Dodavatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu předmětu plnění sjednanou dle Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.

10.2.6 S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací předmětu plnění dle Smlouvy je Dodavatel povinen vždy smluvně zajistit možnost nakládání s těmito právy Objednatelem v rozsahu definovaném tímto článkem Smlouvy.

10.2.7 Dodavatel podpisem Smlouvy výslovně prohlašuje, že odměna za veškerá oprávnění poskytnutá Objednateli dle tohoto článku Smlouvy je již zahrnuta v ceně licencí dle Smlouvy či v ceně ostatních částí předmětu plnění, pokud předmět tohoto oprávnění vznikl v rámci jejich plnění.

10.2.8 Dodavatel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že Objednatel nemohl předmět plnění Smlouvy užívat řádně a nerušeně. Jestliže se jakékoliv prohlášení Dodavatele v tomto článku Smlouvy ukáže nepravdivým nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy, jde o podstatné porušení Smlouvy a Objednateli vzniká nárok na smluvní pokutu.

10.2.9 Bude-li Autorské dílo nebo jeho část dílem zaměstnaneckým (§ 58 Autorského zákona) nebo dílem kolektivním (§ 59 Autorského zákona), je Dodavatel povinen vypořádat práva s autory takových děl (zejména opatřit potřebné souhlasy autorů a uhradit veškeré odměny autorům) tak, aby práva k takovému Autorskému dílu Objednateli mohl poskytnout v plném rozsahu dle tohoto článku Smlouvy a jejích příloh. Předáním části předmětu plnění, které je Autorským dílem, Dodavatel poskytuje Objednateli potřebné licence k Autorskému dílu a zároveň tím stvrzuje, že veškerá práva s autory zaměstnaneckých či kolektivních děl řádně vypořádal a je oprávněn je poskytnout Objednateli.

11. Ochrana důvěrných informací a osobních údajů

11.1 Za účelem ochrany důvěrných informací uzavřely Smluvní strany smlouvu „Dohoda o ochraně důvěrných informací“, která tvoří přílohu č. 6 Smlouvy.

11.2 Zpracování osobních údajů ve smyslu GDPR je upraveno samostatnou smlouvou „Smlouva o zpracování osobních údajů“, která je nedílnou součástí této Smlouvy jako její příloha č. 5.

12. Oznámení a komunikace

12.1 Veškerá oznámení, tj. jakákoliv komunikace na základě této Smlouvy, bude probíhat v souladu s tímto článkem Smlouvy. Jakékoli oznámení, žádost či jiné sdělení, jež má být učiněno či dáno Smluvní straně dle této Smlouvy, bude učiněno písemně. Kromě jiných způsobů komunikace dohodnutých mezi Smluvními stranami se za účinné považují osobní doručování, doručování doporučenou poštou, kurýrní službou či datovou schránkou, elektronickou poštou se zaručeným elektronickým podpisem (IT vedení – **it.vedeni@ozp.cz**), a to na adresy Smluvních stran uvedené v záhlaví Smlouvy, nebo na takové adresy, které si Smluvní strany vzájemně písemně oznámí. Pro účel oznámení a komunikace se v tomto odstavci Smlouvy se Smluvní stranou rozumí i poddodavatelé Dodavatele.

12.2 Oznámení správně adresovaná se považují za doručená:

12.2.1 okamžikem, o němž tak stanoví zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů (dále jen „**ZDS**“), je-li oznámení dodáváno prostřednictvím datové zprávy do datové schránky ve smyslu ZDS; nebo

12.2.2 dnem fyzického předání oznámení, je-li oznámení zasíláno prostřednictvím kurýra nebo doručováno osobně; nebo

12.2.3 dnem doručení potvrzeným na doručence (dodejce), je-li oznámení zasíláno doporučenou poštou; nebo

12.2.4 dnem, kdy bude, v případě, že doručení některým z výše uvedených způsobů nebude z jakéhokoli důvodu možné, oznámení zasláno doporučenou poštou na adresu Smluvní strany, avšak k jeho převzetí z jakéhokoli důvodu nedojde, a to ani ve lhůtě 3 (slovy: tří) pracovních dnů od jeho uložení na příslušné pobočce pošty; nebo

12.2.5 okamžikem, kdy bude odesílateli doručeno potvrzení o úspěšném doručení odesílaného oznámení nebo následující pracovní den po odeslání oznámení, je-li oznámení odesláno prostřednictvím elektronické pošty se zaručeným elektronickým podpisem; nebo

12.2.6 zápisem informace do Provozního deníku nebo

12.2.7 dnem uvedeným v zápisu z kontrolního dne nebo projektové schůzky.

12.3 Informace a materiály, které obsahují osobní údaje či důvěrné informace, budou doručovány buď osobně, nebo zasílány elektronicky a budou zabezpečeny proti zneužití šifrováním.

13. Oprávněné osoby

13.1 Každá ze Smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat příslušnou Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy.

13.2 Oprávněné osoby budou oprávněny činit rozhodnutí závazná pro Smluvní strany ve vztahu ke Smlouvě. Oprávněné osoby, nejsou-li statutárními orgány, však nejsou oprávněny provádět změny ani zrušení Smlouvy, nebude-li jim udělena speciální plná moc.

13.3 Každá ze Smluvních stran má právo změnit jí jmenované oprávněné osoby, musí však o každé změně vyrozumět písemně druhou Smluvní stranu ve lhůtě 7 (slovy: sedmi) dnů. Změna oprávněných osob je vůči druhé Smluvní straně účinná okamžikem, kdy o ní byla písemně vyrozuměna. Písemné zmocnění oprávněné osoby musí být s uvedením rozsahu zmocnění.

13.4 Pokud je Dodavatel společností více osob ve smyslu § 2716 a násl. OZ nebo jiným sdružením či konsorciem, v souladu s § 5 ZZVZ, zavazuje jednání oprávněné osoby všechny členy společnosti společně a nerozdílně.

13.5 Oprávněnými osobami dle této Smlouvy jsou:

13.5.1 **Na straně Objednatele:**

<u>ředitel úseku informatiky OZP</u>

Jméno, příjmení:	Ing. Petr Valchář
Adresa:	Praha 4, Roškotova 1225/1, PSČ 140 00
Telefon:	+ 420 261 105 350
Email:	petr.valchar@ozp.cz

<u>vedoucí odboru vývoje aplikačního softwaru a datových analýz</u>

Jméno, příjmení:	Mgr. Lucie Fialová, Ph.D.
Adresa:	Praha 4, Roškotova 1225/1, PSČ 140 00
Telefon:	+ 420 261 105 184

Email:	lucie.fialova@ozp.cz

vedoucí odboru provozu IT

Jméno, příjmení:	Ing. Jan Devetter
Adresa:	Praha 4, Roškotova 1225/1, PSČ 140 00
Telefon:	+ 420 261 105 450
Email:	jan.devetter@ozp.cz

13.5.2 **Na straně Dodavatele:**

Jméno, příjmení:	[DOPLNÍ DODAVATEL]
Funkce:	[DOPLNÍ DODAVATEL]
Adresa:	[DOPLNÍ DODAVATEL]
Telefon:	+ 420 [DOPLNÍ DODAVATEL]
Fax:	+ 420 [DOPLNÍ DODAVATEL]
Email:	[DOPLNÍ DODAVATEL].

14. Sankční ustanovení

14.1 Povinnosti a lhůty stanovené k splnění předmětu plnění jsou stejně závazné bez ohledu na to, zda jsou výslovně uvedeny ve Smlouvě a/nebo jejích přílohách, anebo vznikly na základě Smlouvy a/nebo jejích příloh, a bez ohledu na to, zda byly stanoveny oboustranně (dohodou, návrhem a jeho akceptací atp.) či jednostranně v souladu s touto Smlouvou nebo na jejím základě (prohlášením Dodavatele, že určitou část předmětu plnění splní v konkrétní lhůtě; určením delší lhůty Objednatelem). Dokumenty vzniklými na základě Smlouvy se rozumí zejména harmonogram dle čl. 4.1 Smlouvy, akceptovaná počáteční analýza, Dodavatelem schválená objednávka a vzájemně sjednané podmínky poskytování Rozvoje.

14.2 Smluvní strany se dohodly, že

14.2.1 v případě prodlení Dodavatele s dodáním detailního harmonogramu v termínu uvedeném v čl. 4.1.1.1, vzniká Objednateli nárok na smluvní pokutu ve výši 2.000 Kč (slovy: dva tisíce korun českých) za každý i započatý kalendářní den prodlení;

14.2.2 v případě prodlení Dodavatele s dodáním počáteční analýzy v termínu uvedeném v čl. 4.1.1.2, vzniká Objednateli nárok na slevu z ceny předmětu plnění nebo její části (dále jen „**sleva**“ nebo „**sleva z ceny**“) ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.3 v případě prodlení Dodavatele s nasazením Díla v rozsahu Základních požadavků do provozu v testovacím prostředí v termínu uvedeném v čl. 4.1.1.4, vzniká Objednateli nárok na slevu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.4 v případě prodlení Dodavatele s dodáním Díla v rozsahu Základních požadavků v termínu uvedeném v čl. 4.1.1.3, vzniká Objednateli nárok na slevu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.5 slevy dle čl. 14.2.2 až 14.2.4 se kumulují, tzn. nově vzniklý nárok na slevu pozdější neruší nárok na slevu dřívější, trvá-li prodlení Dodavatele, k němuž se dřívější sleva váže;

14.2.6 v případě prodlení Dodavatele s dodáním Díla v rozsahu Dalších požadavků v termínech uvedených v čl. 4.1.2 a/nebo prodlení s nasazením do provozu v testovacím prostředí ve smyslu čl. 4.1.1.4, vzniká Objednateli nárok na slevu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení; tyto slevy se kumulují;

14.2.7 v případě prodlení Dodavatele s dodáním PAM v termínech uvedených v čl. 4.1.3 a/nebo prodlení s nasazením do provozu v testovacím prostředí ve smyslu čl. 4.1.1.4, vzniká Objednateli nárok na slevu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení; tyto slevy se kumulují;

14.2.8 v případě prodlení Dodavatele s dodáním pravidelné auditní zprávy, vzniká Objednateli nárok na slevu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.9 v případě nedodržení lhůty k Úpravě směrnic dle čl. 4.1.5 vzniká Objednateli nárok na slevu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.10 v případě nedodržení reakčních lhůt dle čl. 6.1 přílohy č. 1 vzniká Objednateli nárok na slevu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každou i započatou hodinu prodlení;

14.2.11 v případě nedodržení lhůt pro odstranění vad dle čl. 6.1 přílohy č. 1 vzniká Objednateli nárok na slevu ve výši

a) 1.000 Kč (slovy: jeden tisíc korun českých) za každou i započatou hodinu prodlení u lhůt stanovených v hodinách,

b) 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení u lhůt stanovených ve dnech;

14.2.12 v případě nedodržení lhůty k provedení hodnocení dopadů navrhovaných změn předmětu plnění dle čl. 7.2.2 vzniká Objednateli nárok na smluvní pokutu ve výši 500 Kč (slovy: pět set korun českých) za každý i započatý kalendářní den prodlení;

14.2.13 v případě nedodržení lhůt k provedení úprav výstupů dle výhrad a připomínek dle čl. 8.6 a 8.7, případně jinak v souladu s touto Smlouvou stanovených lhůt k provedení úprav výstupů dle výhrad a připomínek v rámci akceptace, vzniká Objednateli nárok na slevu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení;

14.2.14 v případě prodlení Dodavatele s odstraněním vad v záruční době ve smyslu čl. 9.8, vzniká Objednateli nárok na smluvní pokutu ve výši 5.000 Kč (slovy: pět tisíc korun českých) za každý i započatý kalendářní den prodlení;

14.2.15 v případě nedostupnosti služby hotline dle čl. 6.1 přílohy č. 1 déle než 30 minut v provozní době, vzniká Objednateli nárok slevu ve výši 1.000 Kč (slovy: jeden tisíc korun českých) za každých započatých 30 minut nedostupnosti služby Hotline;

14.2.16 v případě porušení povinnosti Dodavatele k oznámení dle čl. 5.9, vzniká Objednateli nárok na smluvní pokutu ve výši ve výši 500 Kč (slovy: pět set korun českých) za každý i započatý kalendářní den prodlení;

14.2.17 v případě, že Dodavatel poruší jakoukoliv povinnost uvedenou v čl. 16.9, vzniká Objednateli nárok na smluvní pokutu ve výši 500.000 Kč (slovy: pět set tisíc korun českých) za každé jednotlivé porušení povinnosti;

14.2.18 v případě, že se jakékoliv prohlášení Dodavatele v čl. 10 ukáže nepravdivým nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy, vzniká Objednateli nárok

na smluvní pokutu ve výši 1.000.000 Kč (slovy: jeden milion korun českých) za každé jednotlivé porušení povinnosti;

14.2.19 v případě prodlení Dodavatele s realizací dílčích objednávek na služby Rozvoje dle čl. 4.1.6, vzniká Objednateli nárok na slevu ve výši ve výši 0,1 % ze sjednané ceny Rozvoje (bez DPH) za každý započatý kalendářní den prodlení s plněním této smluvní povinnosti. Pro účely tohoto článku se za závazné termíny realizace dílčích objednávek na služby Rozvoje považuje dohodnutý termín předání do testovacího prostředí a dohodnutý termín předání do provozu.

14.2.20 v případě porušení povinnosti Dodavatele dle čl. 6.3 a/nebo 6.4 vzniká Objednateli nárok na smluvní pokutu ve výši 50.000 Kč (slovy: padesát tisíc korun českých) za každé takové porušení;

14.2.21 v případě porušení povinnosti Dodavatele dle čl. 9.3 vzniká Objednateli nárok na smluvní pokutu ve výši

a) 100.000 Kč (slovy: sto tisíc korun českých) za každé jednotlivé porušení povinnosti mít sjednané pojištění odpovědnosti,

b) 500 Kč (slovy: pět set korun českých) za každý i započatý den prodlení s předáním pojistné smlouvy (nárok na tuto smluvní pokutu vzniká i v případě, že Dodavatel osvědčí, že neporušil povinnost mít sjednané pojištění, ale byl v prodlení s doložením této skutečnosti);

14.2.22 v případě porušení povinností k ochraně důvěrných informací či ochraně osobních údajů dle čl. 11 je Objednatel oprávněn po Dodavateli požadovat zaplacení smluvní pokuty za podmínek definovaných samostatnou „Dohodou o ochraně důvěrných informací“ a „Smlouvou o zpracování osobních údajů“.

14.2.23 v případě porušení jakékoliv povinnosti Dodavatele stanovené touto Smlouvou nebo na jejím základě, pro kterou není ve Smlouvě stanovena specifická sankce, a její nesplnění Dodavatelem ani v dodatečné přiměřené lhůtě poskytnuté Objednatelem (nevylučuje-li to charakter porušené povinnosti), vzniká Objednateli nárok na smluvní pokutu ve výši

14.2.22.1. 500 Kč (slovy: pět set korun českých) za každou i započatou hodinu prodlení, je-li pro povinnost stanovena lhůta v hodinách;
14.2.22.2. 1.000 Kč (slovy: jeden tisíc korun českých) za každý i započatý den prodlení, je-li pro povinnost stanovena lhůta ve dnech či měsících;
14.2.22.3. 5.000 Kč (slovy: pět tisíc korun českých) za každý jednotlivý případ porušení takové povinnosti, nejde-li o případy popsané v čl. 14.2.22.1 a v čl. 14.2.22.2.

V pochybnostech se má za to, že dodatečná lhůta je přiměřená, pokud činila alespoň 24 (slovy: dvacet čtyři) hodin v případě dle odst. 14.2.22.1 a 5 (slovy: pět) pracovních dnů v ostatních případech.

14.3 Slevy z ceny je Dodavatel povinen zohlednit při nejbližší fakturaci (včetně přiložení tzv. reportu slev), nestane-li se tak, je Objednatel oprávněn slevu z ceny uplatnit písemnou výzvou obdobně jako v případě smluvní pokuty. Sleva z ceny převyšující hodnotu nejbližší faktury bude zohledněna v následujících fakturách a nebude-li v rámci příslušného kalendářního roku fakturované ceny, proti níž může být započtena (zejména cena části předmětu plnění je nižší než sleva, na kterou má Objednatel nárok), stává se smluvní pokutou. Objednatel je dále oprávněn započíst slevu z ceny, smluvní pokutu či případně jiné své peněžité pohledávky vůči Dodavateli proti jakékoliv peněžité pohledávce Dodavatele, na jejíž úhradu má Dodavatel nárok dle této Smlouvy. Objednatel je oprávněn započíst své splatné peněžité pohledávky i vůči neplatným peněžitým pohledávkám Dodavatele.

14.4 Zaplacením smluvní pokuty či poskytnutím slevy z ceny není jakkoliv dotčen nárok Objednatele na náhradu škody; nárok na náhradu škody je Objednatel oprávněn uplatnit vedle smluvní pokuty a/nebo slevy z ceny v plné výši. Zaplacením smluvní pokuty či poskytnutím slevy z ceny není dotčeno splnění povinnosti, která je jejich prostřednictvím zajištěna.

14.5 V případě prodlení kterékoliv Strany se zaplacením peněžité částky vzniká oprávněné straně nárok na úrok z prodlení v zákonné výši počítaný z dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé škody.

15. Ukončení Smlouvy

15.1 Smluvní vztah vzniklý touto Smlouvou lze ukončit těmito způsoby

15.1.1 odstoupením od Smlouvy

i. za podmínek uvedených v OZ v případě porušení Smlouvy druhou Stranou podstatným způsobem,

ii. v případech, které si Strany ujednaly ve Smlouvě;

15.1.2 dohodou Stran;

15.1.3 výpovědí.

15.2 Objednatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Dodavatelem, přičemž za podstatné porušení Smlouvy se bude považovat

15.2.1 prodlení Dodavatele s realizací předmětu plnění (či jeho části) v termínech dle čl. 4 či dalších dílčích termínech stanovených v této Smlouvě, jejích přílohách anebo na jejím základě delšího než 30 (slovy: třicet) kalendářních dnů, pokud Dodavatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 (slovy: deset) pracovních dnů od doručení takovéto výzvy;

15.2.2 nedostupnosti služby hotline v provozní době dle čl. 6.1 přílohy č. 1 delší než půl hodiny, pokud

i. nastala alespoň dvakrát v rámci posledních 30 kalendářních dnů, nebo

ii. nastala alespoň čtyřikrát v rámci posledních 3 kalendářních měsíců;

15.2.3 porušení povinnosti Dodavatele dle odst. 9.3 mít sjednané pojištění odpovědnosti;

15.2.4 ukáže-li se jakékoliv prohlášení Dodavatele v čl. 10 nepravdivým nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy;

15.2.5 porušení jakékoliv povinnosti vyplývající z čl. 11 Dodavatelem;

15.2.6 prodlení Dodavatele s odstraněním vady dle čl. 6.1 přílohy č. 1 delší než 2 (slovy: dva) pracovní dny, pokud Dodavatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 1 (slovy: jeden) pracovní den od doručení takovéto výzvy;

15.2.7 prodlení Dodavatele s provedením úprav výstupů dle výhrad a připomínek dle čl. 8.6 a 8.7 případně jinak v souladu s touto Smlouvou stanovených lhůt k provedení úprav výstupů dle výhrad a připomínek v rámci akceptace delší než 2 (slovy: dva) pracovní dny, pokud Dodavatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu

k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 1 (slovy: jeden) pracovní den od doručení takovéto výzvy;

15.2.8 situace, kdy celková výše smluvních pokut a/nebo slev z cen ve čl. 14, na jejichž zaplacení nebo započtení by měl Objednatel dle Smlouvy nárok, dosáhne 2.000.000 Kč (slovy: dva miliony korun českých).

15.2.9 další případy uvedené ve Smlouvě.

15.3 Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě,

15.3.1 že v insolvenčním řízení bude zjištěn úpadek Dodavatele nebo insolvenční návrh bude zamítnut pro nedostatek majetku Dodavatele v souladu se zněním zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**InsZ**“);

15.3.2 že Dodavatel vstoupí do likvidace;

15.3.3 významné změny ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů (dále jen „**ZOK**“) (významnou změnou ovládání Dodavatele se rozumí vliv, ovládání či řízení dle § 71 a násl. ZOK) nebo v případě změny kontroly zásadních aktiv, využívaných Dodavatelem k předmětu plnění.

15.4 Dodavatel je oprávněn od Smlouvy písemně odstoupit z důvodu jejího podstatného porušení Objednatelem, přičemž za podstatné porušení Smlouvy se bude považovat zejména prodlení Objednatele s úhradou ceny za plnění předmětu Smlouvy delší než 30 (slovy: třicet) kalendářních dnů, pokud Objednatel nezjedná nápravu ani do 10 (slovy: deseti) pracovních dnů od doručení písemného oznámení Dodavatele o takovém prodlení se žádostí o jeho nápravu.

15.5 Objednatel i Dodavatel jsou oprávněni odstoupit od této Smlouvy v případě porušení čl. 16.9 druhou Smluvní stranou.

15.6 Odstoupení od Smlouvy ze strany Objednatele nesmí být spojeno s uložením jakékoliv sankce k tíži Objednatele.

15.7 Smluvní strany se dále dohodly, že odstoupení od Smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé Smluvní straně. Smluvní strany se dohodly, že v případě odstoupení od Smlouvy se nevrací Dodavatelem již provedené a Objednatelem akceptované plnění dle Smlouvy. Dále se Smluvní strany dohodly, že u zbývajícího plnění dle Smlouvy Smluvní strany protokolárně provedou inventarizaci veškerých plnění Dodavatele dle Smlouvy provedených k datu, kdy Smlouva byla ukončena a na tomto základě provedou vyrovnání vzájemných závazků a pohledávek z toho pro ně vyplývajících (výše ceny za Dodavatelem do zániku Smlouvy provedených plnění dle Smlouvy se řídí výší ujednanou pro ně ve Smlouvě, resp. stanoví se poměrem podle rozsahu ukončené části předmětu plnění, přičemž Smluvní strany se výslovně dohodly, že nárok Dodavatele za Dodavatelem do zániku Smlouvy provedených plnění dle Smlouvy vzniká pouze v rozsahu účelně vynaložených nákladů na plnění předmětu plnění a za splnění podmínky, že je taková část plnění ve zhotoveném rozsahu pro Objednatele využitelná). Objednateli vzniká odstoupením od Smlouvy rovněž nárok na náhradu vícenákladů jím prokazatelně vynaložených na řádném splnění předmětu Smlouvy.

15.8 Objednatel je oprávněn Smlouvu písemně vypovědět, a to

15.8.1 do 2 měsíců po dodání počáteční analýzy, pokud v průběhu této lhůty nedošlo k řádnému provedení úprav výstupů dle výhrad a připomínek Objednatele v souladu s čl. 8 Smlouvy; v takovém případě nemá Dodavatel nárok na úhradu žádné části ceny předmětu plnění a výpověď je účinná okamžikem jejího doručení;

15.8.2 do 2 měsíců po dodání počáteční analýzy, pokud Objednatel na základě počáteční analýzy dospěje k závěru, že nemá zájem na pokračování plnění této Smlouvy; v takovém případě má Dodavatel nárok na úhradu 20 % ceny Díla v rozsahu Základních požadavků (položka A.1 dle přílohy č. 2) a výpověď je účinná okamžikem jejího doručení;

15.8.3 i bez udání důvodů, avšak ne dříve než po 12 měsících provozu Díla v rozsahu alespoň Základních požadavků. Taková výpověď je účinná okamžikem jejího doručení Dodavateli. Výpovědní doba činí 6 (slovy: šest) měsíců a počíná běžet prvním dnem měsíce následujícího po tomto doručení.

15.9 Dodavatel je oprávněn Smlouvu písemně vypovědět, a to i bez udání důvodů, avšak ne dříve než po 24 měsících provozu Díla v rozsahu alespoň Základních požadavků. Taková výpověď je účinná okamžikem jejího doručení Dodavateli. Výpovědní doba činí 12 (slovy: dvanáct) měsíců a počíná běžet prvním dnem měsíce následujícího po tomto doručení.

15.10 Zánikem nebo ukončením této Smlouvy nejsou dotčena práva a povinnosti vyplývající z ustanovení Smlouvy, která dle projevené vůle Smluvních stran nebo vzhledem ke své povaze mají trvat i po ukončení Smlouvy, a to zejména práva a povinnosti související s odpovědností za škodu, náhradou škody, slevami z ceny a/nebo smluvními pokutami, fakturací za poskytnuté plnění a realizovaná, byť i jen částečně, dílčí plnění, s úroky z prodlení, dále s odpovědností za vady, zárukou a ochranou osobních údajů a důvěrných informací.

16. Závěrečná ustanovení

16.1 Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv ve smyslu § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

16.2 Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat za Smluvní strany.

16.3 Dodavatel se zavazuje bez předchozího výslovného písemného souhlasu Objednatele nepostoupit ani nepřevést jakákoliv práva či povinnosti vyplývající ze Smlouvy či Smlouvu jako celek na třetí osobu či osoby.

16.4 Dodavatel se zavazuje, že jakoukoliv chystanou změnu ovládání ve smyslu § 71 a násl. ZOK neprodleně písemně oznámí Objednateli, přičemž taková změna ovládání (ať chystaná nebo uskutečněná) opravňuje Objednatele bez zbytečného odkladu od obdržení oznámení podle tohoto ustanovení, resp. od okamžiku, kdy se Objednatel prokazatelně dozví o uskutečnění takové změny, odstoupit od Smlouvy.

16.5 Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, zdánlivým, neúčinným nebo nevynutitelným, netýká se tato neplatnost, zdánlivost, neúčinnost nebo nevynutitelnost zbývajících ustanovení této Smlouvy. Smluvní strany se tímto zavazují nahradit jakékoli takové neplatné, zdánlivé, neúčinné nebo nevynutitelné ustanovení ustanovením, které je platné, nikoli zdánlivé, účinné nebo vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.

16.6 Jednacím jazykem mezi Objednatelem a Dodavatelem bude pro veškerá plnění vyplývající z této Smlouvy výhradně jazyk český.

16.7 Práva a povinnosti vzniklé na základě Smlouvy nebo v souvislosti s ní se řídí českým právním řádem, zejména pak příslušnými ustanoveními OZ, ZOK a ZZVZ. Veškeré případné spory ze Smlouvy budou v prvé řadě řešeny smírem. Pokud smíru nebude dosaženo během 30 (slovy:

třiceti) kalendářních dnů, všechny spory z této Smlouvy a v souvislosti s ní budou řešeny věcně a místně příslušným soudem v České republice. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

16.8 Smluvní strany ve smyslu § 558 odst. 2 OZ vylučují aplikaci obchodních zvyklostí zachovávaných obecně i obchodních zvyklostí zachovávaných v odvětví týkajícím se předmětu této Smlouvy, a to v rozsahu, ve kterém takové obchodní zvyklosti jsou v rozporu s obsahem této Smlouvy nebo příslušnými právními předpisy.

16.9 Dodavatel není bez předchozího písemného souhlasu Objednatele oprávněn po dobu účinnosti Smlouvy a 12 (slovy: dvanáct) měsíců po ukončení trvání Smlouvy zaměstnat zaměstnance Objednatele přímo nebo i nepřímo, a to ani v subjektech, v nichž má rozhodující finanční, majetkovou nebo jinou účast. Za zaměstnance Objednatele se považuje osoba, která byla v pracovním poměru k Objednateli nebo pro Objednatele vykonávala činnost na základě dohody o pracích konaných mimo pracovní poměr v době trvání Smlouvy a přímo se podílela na plnění předmětu této Smlouvy nebo o něm rozhodovala.

16.10 Tato Smlouva je vyhotovena ve 4 (slovy: čtyřech) vyhotoveních, z nichž každé má sílu originálu, přičemž každá ze Smluvních stran obdrží po 2 (slovy: dvou) vyhotoveních.

16.11 Smluvní strany výslovně potvrzují, že při plnění této Smlouvy vystupují v souvislosti se svým vlastním podnikáním a žádná ze Smluvních stran se nenachází v pozici slabší strany ve smyslu ustanovení§ 433 OZ.

16.12 Smluvní strany tímto prodlužují promlčecí lhůtu pro výkon práv podle této Smlouvy, a to na dobu 10 let ode dne, kdy promlčecí lhůta začne běžet.

16.13 Pokud Objednatel nevykoná jakékoli své právo vyplývající z této Smlouvy nebo je vykoná zčásti nebo se zpožděním, nebude to mít účinky vzdání se takového práva a jakýkoliv částečný výkon takového práva nebude překážkou pro jakýkoliv jeho jiný nebo další výkon nebo pro výkon jakéhokoli jiného práva, pokud příslušné právní předpisy nestanoví jinak.

16.14 Smluvní strany výslovně potvrzují, že výše Smluvními stranami v této Smlouvě sjednaných smluvních pokut v každém jednotlivém případě odpovídá závažnosti porušení stanovených závazků a není nepřiměřeně vysoká.

16.15 V případě, kdy bude smluvní pokuta sjednaná Smluvní stranami v této Smlouvě snížená soudem, zůstává zachováno právo na náhradu škody ve výši, v jaké škoda převyšuje částku určenou soudem jako přiměřenou, a to bez jakéhokoliv dalšího omezení.

16.16 Nedílnou součást Smlouvy (tj. součást smluvního vztahu Smluvních stran založeného touto Smlouvou) tvoří Zadávací dokumentace a nabídka Dodavatele na Veřejnou zakázku. Nedílnou součástí Smlouvy jsou dále následující přílohy:

- Příloha č. 1 - Specifikace předmětu plnění
- Příloha č. 2 - Kalkulace ceny
- Příloha č. 4 - Seznam poddodavatelů
- Příloha č. 5 - Seznam členů realizačního týmu
- Příloha č. 6 - Smlouva o zpracování osobních údajů
- Příloha č. 7 - Dohoda o ochraně důvěrných informací (NDA)

Smluvní strany potvrzují, že si přečetly podmínky obsažené v této Smlouvě a že jim porozuměly. Jako důkaz své opravdové vůle přijmout závazky vyplývající z této Smlouvy připojují Smluvní strany k této Smlouvě své podpisy. Smluvní strany tímto potvrzují převzetí příslušného počtu vyhotovení této Smlouvy.

V _____ dne _____

V _____ dne _____

_____

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví

[●], [●]

_____

[DOPLNÍ DODAVATEL]

jméno osoby oprávněné jednat za Dodavatele: [DOPLNÍ DODAVATEL]

funkce: [DOPLNÍ DODAVATEL]

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

veřejné zakázky „Identity Management - realizace“

Příloha č. 8 - Vzor smlouvy o dílo a o poskytování služeb

Příloha č. 1 - Specifikace předmětu plnění

OBSAH

ÚVOD

Tento dokument obsahuje požadavky Objednatele na Dílo a poskytované služby. Používá-li se v tomto dokumentu pojmů „systém“, „produkt“, „IdM“ či „nástroj“, rozumí se jím nástroj pro správu identit, jehož dodání, konfiguraci a implementaci Objednatel požaduje. Tento dokument obsahuje popis požadovaných vlastností. I v případě, že je použit obrat, že nástroj určité vlastnosti má (např. „produkt umožňuje“, „produkt obsahuje“), je tím vyjádřen závazný požadavek Objednatele, aby systém tyto vlastnosti měl.

1 IDM – ZÁKLADNÍ POŽADAVKY

Kapitola popisuje základní požadavky na produkt Identity Manager. Je rozděleno na dvě části – obecné požadavky a požadavky specifické pro Objednatele. Tyto požadavky jsou v celém rozsahu povinné.

1.1 OBECNÉ POŽADAVKY NA PRODUKT IDM

Kapitola popisuje obecné požadavky na produkt Identity Manager.

1.1.1 Systémové požadavky

- Řešení podporuje rozvoj pomocí skriptovacích jazyků.
- Řešení podporuje přístup pomocí zabezpečeného protokolu HTTPS s podporou technologie RSA a ECC.
- Řešení musí být provozováno na aplikačním serveru.
- Řešení podporuje kódování UTF-8 i UTF-16.
- Export/Import konfigurace IdM nástroje v minimálně v těchto uvedených formátech: XML, JSON a YAML.
- Možnost definovat a pravidelně spouštět serverové úlohy v IdM, např. *transformační, kontrolní a notifikační úlohy*.
- Schopnost pracovat v režimu vysoké dostupnosti za pomoci více uzlů aplikace, např. *automatické spuštění úlohy na dostupném uzlu aplikace*.
- Možnost volat jakoukoliv datovou operaci, která je dosažitelná z webového rozhraní pomocí API. Např. *založení uživatele, tvorba rolí, správa organizační struktury.*
- Databáze systému IdM budou využívat platformu MS SQL 2016 nebo vyšší.
- Aplikace bude využívat platformu MS Server 2016 nebo vyšší.

1.1.2 Uživatelské rozhraní IdM

GUI (Graphical User Interface) obsahuje

- kompletní lokalizaci do českého jazyka pro koncové uživatele,
- jednotné webové rozhraní pro administrátory i pro koncové uživatele,
- webové rozhraní bez nutnosti instalovat dodatečný SW,
- vyhledávání ve všech entitách podle jejich atributů,
- vyhledávání ve všech entitách principem „full text“ – hledání jednoho řetězce současně ve více atributech,
- opatření proti útoku typu „Cross-Site Request Forgery“,
- export dat do souboru formátu CSV z obrazovek s výpisem uživatelů a rolí.

1.1.3 Autorizační model v IdM

Autorizační model je založen na RBAC (Role-Based Access Control) a umožňuje nastavit, k jaké části uživatelského rozhraní IdM a k jakým objektům v IdM mají uživatelé přístup až do úrovně atributů entit.

Autorizační model umožní:

- Definovat oprávnění k jednotlivým objektům pomocí aplikačních a business rolí.
- Definovat oprávnění k funkcionalitám IdM pomocí aplikačních a business rolí.
- Nastavovat autorizaci na jednotlivé části GUI nebo pomocí filtrů na jakékoliv entity, které splňují nebo nesplňují definované podmínky.
- Definovat autorizace na základě podmínky, příklad: *vedoucí smí upravovat své podřízené.*
- Vytvořit administrátorská práva nad určitými organizačními jednotkami, koncovými systémy, nad skupinami uživatelů nebo obecně nad definovanými objekty IdM. Účelem je umožnit administrátorovi správu nad uživateli patřícími do samostatného podřízeného celku. Např. *interní entity, externí entity, kterými jsou dodavatelské účty.*
- Konfigurovat práva pro všechny uživatele tak, aby si mohli zobrazit
    - přiřazené koncové systémy,
    - přiřazená oprávnění,
    - přiřazení do organizační struktury.
- Konfigurovat práva pro všechny uživatele tak, aby mohli provést schválení přiřazených požadavků a spouštět reporty.
- Nastavit oprávnění až na úroveň jednotlivých atributů, např. *uživatel si může editovat pouze atribut telefonního čísla.*

1.1.4 Autentizace v IdM

Produkt musí obsahovat access management, jehož funkcí je možnost automatického přihlášení (SSO) pomocí protokolu Kerberos oproti MS Active Directory, kde

- uživatel přihlášený do MS AD je automaticky přihlášen do IdM,
- uživateli, který není zaveden v MS AD doméně, je zobrazen přihlašovací formulář, kde se může přihlásit do IdM pomocí jména a hesla, které je ověřeno proti úložišti IdM.

Operace je vždy logována do auditního logu IdM.

Produkt umožní provést odhlášení uživatele, které vede na přihlašovací formulář.

Produkt umožňuje samo-registraci nového nepřihlášeného uživatele. Samo-registrační formulář obsahuje kontrolu mechanismem CAPTCHA. Uživateli je po potvrzení formuláře z IdM zaslán e-mail obsahující aktivační link.

Produkt podporuje historii hesel uživatelů, v případě změny hesla přes IdM. Nová hesla zadaná v IdM jsou kontrolována proti historii. IdM umožní hesla uživatele ukládat symetrickou šifrou nebo hashem dle globální konfigurace IdM.

1.1.5 Recertifikace oprávnění

Produkt IdM obsahuje nástroj, který provádí recertifikaci přiřazení identita-role. Umožňuje tak v pravidelných intervalech spouštět přeschvalování existujících oprávnění – vazeb identita-role.

Recertifikací se rozumí opětovné schvalování přidělených rolí, organizací nebo koncových systémů. Recertifikace musí umožňovat:

- Plánované nebo automaticky spouštěné certifikace a certifikace na vyžádání,
- schvalování/zamítnutí přístupů jednotlivě,
- automatické akce při zamítnutí přístupu, např. *odebrání role*,
- definovat rozsah recertifikací podle identit, rolí nebo organizační struktury,
- logovat a reportovat stav o krocích a o výsledku recertifikace,
- spouštět neomezený počet současně běžících recertifikací,
- konfigurovat více-krokové workflow s podporou eskalace a delegace.

Produkt rovněž recertifikuje obsah business rolí – vazbu na aplikační role.

Příklady definice recertifikací:

- *Recertifikace existujících přiřazení rolí externistům, schvalovatelem je manažer externisty.*
- *Recertifikace existujících přiřazení rolí v kritické aplikaci s dvoukrokovým ověřením 1. manager, 2. schvalovatel role v délce trvání 14+14 dní.*
- *Automatické zopakování recertifikace pro přiřazení rolí, u kterých nebylo rozhodnuto do 14 dní. Toto lze dle potřeby vícekrát opakovat.*

Stavy recertifikací jednotlivých případů a rozhodnutí lze sledovat v reportech a reagovat tak na případné nestandardní stavy např. *neřešené případy ke schválení*.

1.1.6 Rozhraní pro integraci

Jedná se o rozhraní pro připojení koncových systémů, které se dále využívá pro provisioning a rekonciliaci.

Rozhraní pro integraci musí splňovat níže uvedené požadavky.

- Umožní číst nebo zapisovat všechna data a volat operace nad objekty v IdM pomocí Web service API (SOAP/WSDL) nebo REST API.
- Umožní bezpečný přenos dat mezi IdM a rozhraním koncového systému např. *prostřednictvím SSL/TLS, pro AD Kerberos nebo NTLM2*.
- IdM se k rozhraní koncových systémů autentizuje dedikovaným technickým uživatelem.
- Umožní vystavit aplikační rozhraní (WS SOAP, REST, Java API, Powershell) nebo rozhraní datového úložiště (LDAP, DB procedury, DB tabulka).
- Obsahuje konektory k Active Directory (včetně volání Powershell skriptu a WinRM), k LDAPu a k databázi. Konektory musejí být konfigurovatelné bez nutnosti vývoje.
- Umožní vývoj vlastních konektorů - jedná se minimálně o:
  - Připojení k webovým službám a využití jejich metod.
  - Připojení k databázovým strukturám pro čtení a zápis dat.
  - Připojení pomocí protokolu LDAP.
- Integraci vývojového prostředí IDE, např. *NetBeans, Eclipse, IntelliJ IDEA,* tak, aby bylo možné z IDE přímo nahrávat a číst objekty datového modelu IdM.

Produkt musí obsahovat níže uvedené konektory out-of-the-box:

- Active Directory Connector
- Atlassian JIRA
- CSV Connector
- DatabaseTable Connector
- eDirectory ConnectorExchange (WinRM)
- GitLab
- Google Apps
- LDAP Connector
- Office365
- Oracle Connector
- SCIM connector
- ScriptedSQL Connector
- UNIX

1.1.7 Synchronizace a rekonciliace

Jedná se o funkcionalitu, kdy systém IdM porovnává schválený a skutečný stav na koncovém systému (rekonciliace) a načítání dat z koncových systémů (synchronizace). Tyto funkcionality musí splňovat tyto požadavky:

- Synchronizaci změn v reálném čase podle časové značky u záznamu.
- Vestavěnou podporu opakování propagace změn v případě neúspěchu.
- Obousměrnou synchronizaci dat mezi IdM a koncovým systémem, např. *uživatele a jejich atributy, role v koncovém systému*.
- Mapování atributů mezi koncovými systémy na základě pravidel/vzorců.
- Umožnit práci se složenými i binárními atributy uživatele, např. *certifikáty, fotografie, autentizační tokeny.*
- Rekonciliaci účtů, tzn. pravidelnou automatickou kontrolu stavu účtů na koncových systémech s autoritativním vypořádáním nesouladu.
- Zaznamenání stavu účtu při rekonciliaci vzhledem k ne/existenci vlastníka v IdM.
- Umožnit nastavení automatických akcí pro nespárované účty, např. *zneplatnění*.
- Umožnit nastavení whitelistu účtů, které IdM nikdy nemění, např. *pro technické účty*.
- Umožnit pravidelnou automatickou kontrolu stavu oprávnění na koncových systémech a vynucení stavu chtěného (výmaz nadbytečných oprávnění).
- Umožnit nastavení korelačních pravidel pro párování mezi identitou a jejím účtem, např. *nastavení politiky, že část e-mailové adresy účtu odpovídá username dané identity*.
- Logování veškerých aktivit synchronizací a rekonciliací. Systém umožní reportování výsledků rekonciliací pomocí uživatelsky definovaných reportů dle požadavků v kapitole Reporting.
- Podpora pro objekty v koncovém systému typu uživatel, skupina, role, organizace.
    - Nabízené řešení umožňuje v koncovém systému měnit jiné typy objektů, než je uživatelský účet, např. *role, skupiny, profily*. Jde především o objekty oprávnění a organizačních jednotek. Pro příklad: *IdM umožní vytvořit roli, která je zodpovědná nejen za přiřazení oprávnění uživateli, ale i za existenci objektu oprávnění v koncovém systému.*
- Rekonciliace offline systémů
    - Řešení umožní řízení identit a oprávnění v připojených systémech.
    - Řešení umožní offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou. Offline řízení oprávnění probíhá v GUI rozhraní IdM nebo na základě informací získaných z exportu koncového systému.

- Systém umožňuje spustit každou rekonciliaci tak, aby zpracování objektů koncových systémů běželo ve více vláknech.

- Hromadné akce
  - Nabízené řešení nabízí spouštění hromadných akcí. Minimálně umožní tyto akce:
    - hromadné přiřazení rolí uživatelům, kteří vyhovují podmínkám,
    - hromadnou změnu organizační jednotky vybraných uživatelů,
    - hromadné vytvoření rolí,
    - hromadné schvalování přidělených úkolů.
  - Každá změna hromadné akce je auditovaná.
- Simulace změn
  - Systém poskytuje grafický přehled změn atributů před vlastním uložením vybraného objektu. Tato simulace se týká uživatelů, rolí a organizační struktury.

1.1.8 E-mailové notifikace

Systém umožní

- definovat šablony e-mailů s podporou vícejazyčnosti (*čeština, slovenština, angličtina)* a HTML,
- podporu skriptovacího jazyka s možností čerpání dat ze zdrojové databáze,
- konfiguraci parametrů odesílání zpráv přes SMTP server, např. *jméno serveru, jméno/heslo, SSL*,
- zvolit v nastavení více odesílacích SMTP serverů,
- vkládání hypertextových linků na konkrétní obrazovku v IdM.

Systém bude provádět notifikaci minimálně těchto akcí:

- vytvoření, změna, smazání identity,
- přiřazení a odebrání role,
- výzva k akci pro uživatele,
- zakázání a povolení uživatele,
- přejmenování uživatele,
- požadavek na schválení role nebo na její ověření,
- libovolné akce ve workflow podle nastavení administrátorem IdM,
- změna uživatelského hesla v IdM,
- propagace hesla z IdM do koncového systému.

1.1.9 Workflow

Systém umožní

- vytvářet a modifikovat workflow založené na principech Business Process Management (BPM),
- aktivovat workflow při splnění nastavené podmínky, např. *nastavení hodnoty atributu,*
- aktivovat workflow automaticky při schvalovacím procesu přidělování rolí uživatelům,
- vizualizaci průběhu workflow včetně výhledu do budoucna (přehled budoucích schvalovatelů),
- definovat neomezený počet schvalovacích kroků,
- nastavit neomezený počet schvalovatelů,
- nastavit schválení typu „jeden z X“ nebo typu „všichni musí schválit“,
- nastavit paralelní schvalování nebo step-by-step schvalování,
- definovat schvalovatele na základě jejich členství v roli, nebo v organizační struktuře nebo podle jejich funkce,
- automatické schvalování na základě hodnoty atributů identity,
- automatické schvalování na základě systematizovaného místa (pracovního místa), funkce nebo zařazení v organizační struktuře,
- schvalovateli doplnit další potřebné informace v průběhu schvalování požadavku, např. *číslo místnosti, telefonní číslo*,
- zobrazit přehled úkolů schvalovatele,
- nabídnout schvalovateli schválení či zamítnutí s přidáním odůvodnění.

1.1.10 Správa objektů

Řešení musí podporovat níže uvedené funkce pro správu organizační struktury:

- Administrační webové rozhraní pro správu stromové struktury.
- Správu prostřednictvím integrační vrstvy.
- Umožnit volání funkcionalit IdM prostřednictvím programového rozhraní, např. *REST API, webové služby*.
- Vytváření libovolného počtu stromů organizačních struktur.
- Vytváření nezávislých objektů ve stromě (pracovní pozice, funkční místa).
- Definování atributů těchto objektů (uzlů) ve stromě.
- Přiřazování nezávislých objektů organizačním jednotkám ve stromě, minimálně uživatelů, rolí, uzlů z jiných stromů.
- Vizualizaci entit pomocí stromové struktury.
- Přiřazení identity nebo role do více stromů zároveň, např. *uživatel může být v různých organizačních strukturách v odlišném zařazení s různým oprávněním*.

- Nastavení časové období od-do pro přiřazení identity do stromové struktury. Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení identity do stromu uplatnit.

Řešení musí podporovat níže uvedené funkcionality rolí:

- Administrační webové rozhraní pro správu business a aplikačních rolí.
- Správu prostřednictvím integrační vrstvy včetně možnosti volání funkcí prostřednictvím API.
- Role musí být možné hierarchicky skládat do hloubky minimálně 25 úrovní.
- Přiřazení role na organizační jednotku s jejím promítnutím k uživatelům přiřazeným do organizační jednotky.
- Vazbu uživatele na roli v kardinalitě 1:N s určením typu vazby, např. *vlastník, schvalovatel role*, a s nastavením platnosti přiřazení role od-do.
- Vazbu koncových systémů na roli v kardinalitě 1:N.
- Nastavení platnosti role od-do., Pokud časové období uplyne nebo ještě nenastalo, nesmí se přiřazení role uplatnit.
- Nastavení schvalovacích procesů pro garanty koncových systémů při tvorbě business rolí.
- Správu role vlastníkem bez přiřazení explicitní autorizace.
- Nastavení role jako vlastníka objektu v koncovém systému (oprávnění, účtu) podobně jako uživatel je vlastníkem účtu. Rekonciliace role pak provede aktualizaci objektu v koncovém systému.
- Podporu tzv. parametrické role (hybridní RBAC).
- Nastavení pravidel pro vzájemně se vylučující role Segregation of Duties (SoD),
- Reporting a notifikace konfliktních práv.
- Nastavování povolení/zamítnutí konfliktů SoD ve schvalovacím Workflow.
- Zažádání o kopii vybraných rolí podle existujícího uživatele a spuštění příslušného schvalovacího Workflow jako v případě manuální přiřazení daných rolí.
- Dědičnost vybraných vlastností rolí, např. *atributů a typu schvalování z nadřazené role*.

Řešení musí podporovat níže uvedené funkcionality pro koncové systémy:

- Administrační webové rozhraní pro správu koncových systémů, např. *nastavení parametrů připojení, zobrazení skutečných účtů kontrolou v koncovém systému, a nikoliv v úložišti IdM*.
- Správu prostřednictvím integrační vrstvy včetně volání funkcí prostřednictvím API.
- Evidenci koncových systémů včetně popisných atributů.
- Vazbu na uživatele.

- Vazbu na aplikační role přiřazené ke koncovému systému v kardinalitě 1:N.
- Rozlišení různých kategorií účtů, např. *administrátorské a běžné účty*.
- Různou business logiku plnění atributů pro různé kategorie účtů.
- Povolení jednotlivých operací nad koncovým systémem, např. *dočasně deaktivovat zápis do koncového systému*.
- Využití více nezávislých konektorů z koncového systému do IdM, Např. *CSV soubor pro čtení, webové služby pro zápis*.

1.2 SPECIFICKÉ POŽADAVKY OBJEDNATELE

Kapitola obsahuje požadavky na IdM specifické pro Objednatele

1.2.1 Iniciální konfigurace IdM, počáteční analýza

Součástí dodávky bude detailní počáteční analýza (dále jen „Počáteční analýza“) a následná konfigurace systému IdM podle specifik prostředí Objednatele popsaných v kapitolách **1.5 IdM v prostředí Objednatele** a napojení systémů popsaných v kapitole **1.3 Základní koncové systémy**.

Před vlastní implementací produktu je nezbytné provést Počáteční analýzu stávajícího ICT prostředí Objednatele s cílem definovat riziková místa zneužitelná k případnému útoku. V Počáteční analýze musí být zahrnuty jak uživatelské stanice, tak linux/unix/windows a aplikační servery. Výsledkem analýzy bude report s jasným přehledem nalezených účtů, stanic, serverů, hashů hesel a dalších detailních informací pomocí nichž bude možné zmapovat potenciální vektory útoků typu pass-the-hash, analyzovat stáří hesel, místa s uloženými údaji k privilegovaným účtům, jako jsou skripty, konfigurace aplikačních serverů, naplánované úlohy atp. Analýza bude obsahovat i mapu důvěry SSH klíčů, která graficky znázorní systémy a účty v prostředí Objednatele a vztahy mezi nimi zjištěnými korelací nalezených klíčů.

Výstup z Počáteční analýzy bude prezentován Objednateli jak prostřednictvím separátní auditní zprávy, tak osobně pracovníkem Dodavatele.

1.2.2 Akceptační testování

Kapitola popisuje scénáře a testy, které řešení musí splňovat, než může být akceptováno.

1.2.2.1 Uživatelské akceptační scénáře

Součástí dodávky je dodání uživatelských akceptačních scénářů pro oblasti níže.

Identita

- Nástup zaměstnance
- Aktualizace údajů zaměstnance
- Změna pozice zaměstnance
- Přejmenování zaměstnance
- Ukončení pracovního poměru zaměstnance
- Ukončení privilegované identity při zániku běžného účtu
- Návrat zaměstnance
- Založení externisty
- Aktualizace externisty
- Ukončení smlouvy externisty
- Založení technického účtu
- Aktualizace technického účtu
- Zrušení technického účtu
- Změna hesla a propagace
- Reset hesla

Oprávnění

- Žádost o přidělení role
- Žádost o privilegovanou identitu
- Vícestupňové schvalovací workflow
- Odebrání oprávnění

Role

- Vytvoření role
- Aktualizace role
- Zakázání role
- Povolení role
- Archivace role

Rekonciliace

- Spuštění rekonciliace IdM a koncového systému

Recertifikace

- Nová definice recertifikace
- Spuštění recertifikace
- Provedení ověřování přidělení rolí uživatelů
- Znovuspuštění recertifikace pro nerozhodnuté případy po časovém limitu

Reporty

- Spuštění reportu s výstupem do souboru na sdíleném úložišti
- Spuštění reportu s výstupem jako příloha emailu
- Spuštění reportu s výstupem jako zazipovaná příloha emailu

Přístup privilegovaných identit ke koncovému systému v režimu monitoringu

- Přihlášení identity ke koncovému systému
- Monitoring aktivity identity přihlášení
- Vynucování bezpečnostních politik

1.2.2.2 Zátěžové testy

Řešení je navržené na zvládání následující zátěže:

- 800 změn za hodinu na vstupu z personálního systému.
- 100 současně přihlášených uživatelů do IdM.
- 50 současně přihlášených privilegovaných identit na koncové servery v monitorovaném režimu.

1.2.3 Podpora migrace

V rámci Počáteční analýzy Dodavatel kromě jiného popíše kroky nezbytně nutné ke korektnímu přechodu do provozu (migrace). Dodavatel poskytne podporu pro tyto oblasti (součinnost Objednateli pro provedení migrace).

1.2.4 Zasílání SMS

Řešení umožní zasílat SMS zprávy přes OZP SMS gateway – REST rozhraní přes HTTP s autentizací.

1.2.5 Iniciální načtení IdM

Iniciální načtení IdM představuje úsilí nutné pro synchronizaci systému IdM se stavem odpovídajícím prostředí Objednatele. V rámci Počáteční analýzy Dodavatele provede analýzu dopadů do stávajících systémů, přičemž zohlední, že v nejmenším rozsahu je zapotřebí provést následující:

- Načíst do IdM identity a role.
- Naimportovat vazby identity-role, tj. kdo má jaká oprávnění pro spravované role.
- Je třeba také načíst aktuální lidi mimo stav, např. *na mateřské*, aby správně fungovaly návraty.

1.2.6 Změna syntaxe přihlašovacích jmen

Návrh IdM definuje syntaxi uživatelských jmen. Existují dva přístupy k řešení této otázky:

- Změnit v jeden okamžik přihlašovací jména uživatelů (přejmenovat).
- Nechat dožít stávající přihlašovací jména a nová zakládat až novým identitám.

V případě změny stávajících přihlašovacích jmen je Objednatelem navržen tento postup:

1. Provést přejmenování na malém reprezentativním vzorku, např. *pracovníci IT úseku*.
2. Uživatele odhlásit od Windows stanic
3. V prostředí IdM převést na novou syntaxi
    - Zkontrolovat, zda se správně zaktualizovaly atributy
4. Uživatele nechat přihlásit pod novým loginem.
5. Ověřit funkcionalitu pod přihlášeným uživatelem:
    - Přístup k Exchange schránce
    - Přístup ke sdíleným složkám a Intranetu
    - Přístup k aplikacím
6. Řešení narolovat na ostatní uživatele.

V rámci Počáteční analýzy Dodavatel ověří, zda Objednatelem navržený postup je proveditelným a vhodným řešením, případně navrhne jiné řešení změny syntaxe přihlašovacích jmen.

1.2.7 Požadavky na dokumentaci

Jako součást dodávky bude dodána dokumentace:

- „Dokumentace skutečného provedení (dále „DSP“)“
    - DSP obsahuje popis úprav provedených oproti standardnímu produktu.
    - DSP bude dodána v českém jazyce.
- Dokumentace produktu
    - Obsahuje administrační dokumentaci produktu.
    - Bude dodána v českém nebo anglickém jazyce.
- Uživatelskou příručku
    - Obsahuje příručku pro uživatele.
    - Bude dodána v českém jazyce.

Dokumentace je dodána ve formě MS Office nebo alternativní k MS Office.

1.3 ZÁKLADNÍ KONCOVÉ SYSTÉMY

V současné době se v OZP provozují následující systémy, které Objednatel požaduje v rámci základní fáze napojit na systém IdM.

1.3.1 MS Active Directory 2016

Koncový systém MS Active Directory 2016

- Napojena je doména OZP.
- V doméně OZP je subdoména ICIS vyhrazená pro nový Integrovaný Centrální Informační Systém (ICIS).
- V doméně je zhruba 650 identit.
- Obsahuje cca 500 skupin pro přidělování oprávnění.
- Řízení oprávnění pomocí členství v AD skupinách.
- Přihlašování je realizováno jménem a heslem.
- Používá se stromová struktura pro správu uživatelů.
- Rozdělení podle lokalit – pobočky a centrála, není dělení podle odborů.
- Speciální účty mají vlastní složky – podle funkcionality a významu.
- AD obsahuje interní i externí identity.
- Externí účty jsou ve skupině Externí účty.
- V popisu externí identity je uveden popis činnosti.
- AD neobsahuje organizační strukturu.
- Základní nastavení přístupů je realizováno prostřednictvím GPO.

Rozhraní k IdM:

- Proprietární AD konektor nebo LDAP konektor

Prostředí:

- Produkční: Ano
- Testovací: Ano, nutné zařídit
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano

Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ano
Řízení oprávnění	Ano, přes skupiny, cca 500
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je zachován, oprávnění jsou odebrána, heslo je změněno

1.3.2 MS Exchange 2016

Koncový systém MS Exchange 2016

- Všichni zaměstnanci a externisté mají e-mail
- Účet v AD = e-mailová schránka
- U speciálních účtů jsou e-mailové schránky většinou zakázané (záleží na účelu účtu).
- E-mailové schránky jsou rozděleny do třech skupin:
- Běžný uživatel – velikost schránky 500 MB.
- Střední management – velikost schránky 1 GB.
- Top management – velikost schránky 2 GB.
- Speciální účty jsou ve stejné kategorii jako top management.
- E-maily nad limit jsou v lokálních PST.
- K e-mailové schránce lze přistupovat i přes webové rozhraní OWA.

Rozhraní k IdM:

- Proprietární Exchange konektor nebo připojení přes Exchange Powershell skripty.

Prostředí:

- Produkční: Ano
- Testovací: Ano, nutné zařídit
- Vývojové: Ne

Úroveň podpory operací s účtem (účet zde = e-mailová schránka):

Operace s účtem	Podporováno? Případně jak

Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano, změna emailové adresy, původní do alternativního emailu
Změna hesla	Ne, SSO s AD
Řízení oprávnění	Ano, řízení kvót k emailům
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	E-mailová schránka je nastavena na neaktivní.

1.3.3 MS SharePoint

Koncový systém MS SharePoint:

- MS SharePoint je využíván jako Intranet.
- Přístup mají všichni zaměstnanci a vybraní externí pracovníci s přiděleným loginem, s výjimkou pracovníků OZP Expres.
- Uživatelé jsou vytváření přes AD.
- Pro autentizaci je používáno AD.
- Přihlášení do SharePoint je realizováno pomocí SSO.
- Nemá vlastní databázi uživatelů, přístup je řešen přes AD.
- V AD je cca 136 skupin zajišťujících přístup do SharePointu.
- Každá skupina je navázána na příslušnou část SharePointu.
- Existuje přesný popis, co jednotlivé skupiny umožňují.

Rozhraní k IdM:

- Webové služby (REST) nebo Sharepoint konektor

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ne, SSO s AD
Řízení oprávnění	Ano, podle skupin AD.
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je deaktivován

1.3.4 ICIS

Koncový systém ICIS = Integrovaný Centrální Informační Systém.

- Hlavní IT systém shromažďující data o pojištěncích, PZS, poskytnuté péči, výdajích a účetní informace.
- Nový systém, který nahradí stávající hlavní systémy IZOP, WOIS, RIS2000 a IS CALL (během roku 2020).
- Základem je MS Navision, který je obohacen o moduly s dalšími funkcionalitami, vyvinuté na platformě .NET. Databáze je MS SQL.
- Přístup do ICIS budou mít všichni zaměstnanci a vybraní externí pracovníci s přiděleným loginem, s výjimkou pracovníků OZP Expres.
- Práva budou nastavena na základě systemizovaných míst.
- ICIS má vlastní databázi uživatelů.
- ICIS má vlastní role management.

Rozhraní k IdM:

- ICIS poskytuje API přes webové služby a dávkové vstupy

Prostředí:

- Produkční: Ano
- Testovací: Ano, plus školicí
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ne, SSO s AD
Řízení oprávnění	Nepřímo, přes AD skupiny, existují případy Segregation of Duties rolí. Přímo v ICISu dokonfigurace přes lokálního admina.
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je deaktivován

1.3.5 DMS SAFE

Koncový systém DMS SAFE je Document Management Systém a Spisová služba od firmy AiP SAFE:

- Ukládají se zde dokumenty (elektronicky čitelné, naskenované).
- Přístup mají všichni zaměstnanci a vybraní externí pracovníci s přiděleným loginem, s výjimkou pracovníků OZP Expres.
- Má vlastní databázi uživatelů.
- Má vlastní role management.
- Pro autentizaci je používáno AD.
- Přihlášení do DMS je realizováno pomocí SSO.

Rozhraní k IdM:

- Webové služby

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ne, SSO s AD
Řízení oprávnění	Ano, vazba na systemizované místo
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je uzamčen a náležící písemnosti jsou přiděleny jinému zaměstnanci.

1.3.6 KS – import

Koncový systém KS je využíván jako zdroj dat o interních zaměstnancích.

Systém KS bude výhledově nahrazen jiným HR systémem. V takovém případě budou potřebné úpravy IdM prováděny Dodavatelem na základě požadavků Objednatele na Rozvoj.

Rozhraní k IdM:

- Databázový pohled – je třeba ošetřit případy, kdy by došlo k chybě importu na straně KS – nastavit limity pro zpracování DB úloh (threshold).

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ne
Aktualizace účtu	Jen pro čtení

Změna loginu účtu	Jen pro čtení
Změna hesla	Ne
Řízení oprávnění	Ne
Povolení/Zakázání účtu	Jen pro čtení
Zánik nároku na účet	Ne

1.4 POŽADAVKY NA ŠKOLENÍ

Je poptáváno proškolení těchto osob pro zajištění práce s řešením na straně Objednatele:

- Proškolení základní uživatelské funkčnosti IdM – 100 uživatelů – školení bude trvat alespoň 2 hodiny.
- Privilegovaní uživatelé – 100 uživatelů – školení bude trvat alespoň 4 hodiny.
- Administrátoři řešení – 25 uživatelů – školení bude trvat alespoň 8 hodin.

Školení bude realizováno prezenční formou s přítomností školitele v sídle Objednatele s možností využití videonávodů a/nebo webinářů, a to pro skupiny nejvýše 20 účastníků, nestanoví-li Objednatel větší počet účastníků ve skupině nebo kratší rozsah školení. Po realizovaném školení bude Objednateli předán školicí materiál, videonávody a/nebo webináře k dalšímu využití.

V případě potřeby školení nad rámec výše uvedeného rozsahu toto bude realizováno a hrazeno v rámci služeb Rozvoje.

1.5 IDM V PROSTŘEDÍ OBJEDNATELE

1.5.1 Architektura IdM

Kapitola popisuje architekturu IdM řešení – schéma, požadavky na připojení koncových systémů, bezpečnost řešení, řízení zálohování a odstávek řešení.

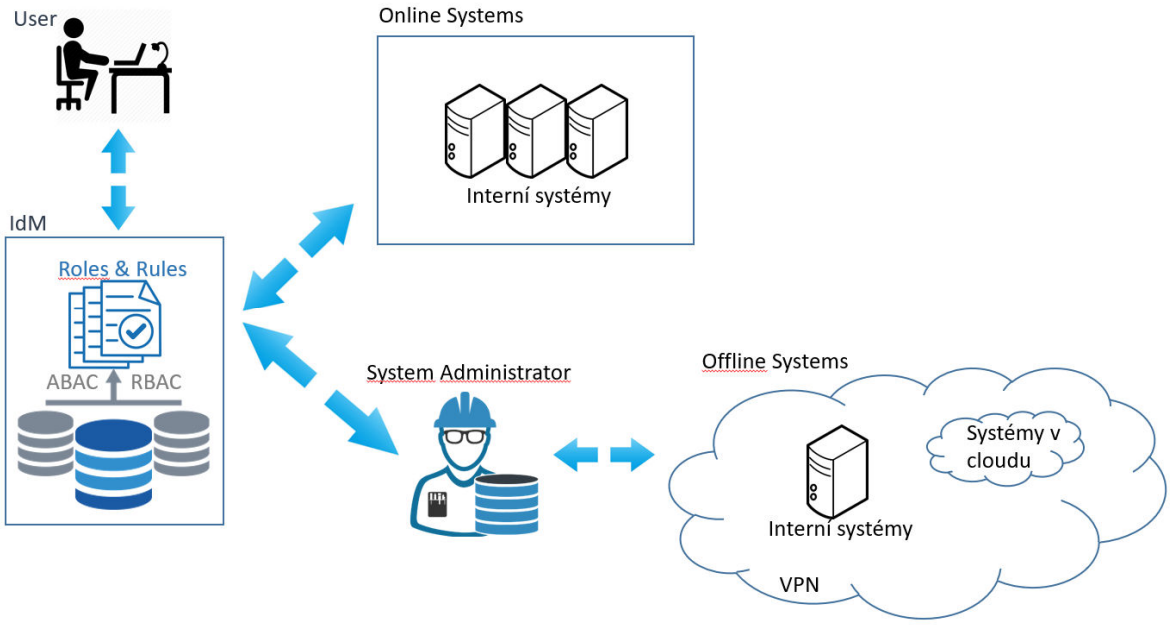
1.5.1.1 Celkové schéma

Celkové koncepční schéma IdM řešení je na obrázku *Obrázek 1 Základní schéma IdM*. Online systémy jsou řízeny systémem IdM přímo, offline systémy nepřímo přes úkolované systémové administrátory.

Architektura bude provozována ve dvou prostředích:

- Testovací – slouží pro testování řešení.
- Produkční – slouží pro živý běh systémů.

Stav koncových systémů a jejich prostředí je popsán v kapitole *Koncové systémy*.



Obrázek 1 Základní schéma IdM

1.5.1.2 Manuálně řízené (offline) systémy

V manuálně řízených systémech produkt IdM účty eviduje, ale fyzicky je neřídí. Stejně tak neeviduje, ale neřídí přidělení či odebrání rolí.

Systémy správy identit a oprávnění v těchto systémech probíhají obdobně. Namísto online realizace změny (automaticky iniciované z IdM) je v IdM vygenerován úkol pro správce daného systému, o kterém je správce notifikován emailem. Správce operaci provede přímo nad koncovým systémem a následně úkol v IdM potvrdí. Tím zůstává evidence o změně uchována v IdM.

1.5.1.3 Bezpečnost informací

Osobní údaje jsou v IdM zabezpečeny tak, aby k nim mohla jen oprávněná osoba – uživatel vidí svoje údaje nebo údaje svých podřízených vyjma vyjmenovaných informací, např. *heslo*.

Pro testovací prostředí je použita kopie produkčních dat s pseudonymizací. Na testovacím prostředí je politika přístupů stejná, jako na produkčním prostředí.

Hesla jsou v IdM řešení uložena ve formě odolné proti offline útokům, např. *brute-force útok, slovníkový útok*. Šifrování hesla musí být na minimální bezpečnosti šifry AES 256 bit. Způsob uložení hesla je v souladu s ISO 27001 a požadavkem § 26 písm. d) vyhlášky o kybernetické bezpečnosti.

1.5.1.4 IdM oprávnění

V rámci systému IdM Objednatel požaduje následující oprávnění, kterým odpovídá role v IdM:

- Správce IdM – má neomezený přístup, administrátor systému.
- Metodik IdM – má přístup ke správě rolí (více viz Metodik).
- IT Helpdesk – má přístup k seznamu uživatelů, vidí detaily uživatelů.
- Gestor aktiva – vidí své role a jejich členy, schvaluje žádosti o role na své schvalovací úrovni.
- Licenční specialista – vidí své role a jejich členy, schvaluje žádosti o role na své schvalovací úrovni.
- Compliance/Bezpečnost ICT – vidí své role a jejich členy, schvaluje žádosti o role na své schvalovací úrovni.
- Školitel – schvaluje žádosti o role na své schvalovací úrovni.
- Manažer – vidí podřízené identity, může pro tyto uživatele žádat o roli, schvaluje žádosti o role na své schvalovací úrovni.
- Běžný uživatel – může zobrazit informace o sobě, žádat o roli a měnit si heslo + některé „jemu povolené“ údaje o sobě; oprávnění běžného uživatele je součástí všech výše zmíněných oprávnění (každý uživatel má tuto roli).

1.5.1.5 Retence dat

Data v systému IdM jsou uchovávána po neomezenou dobu. Výjimku z toho tvoří dvě oblasti:

- auditní záznamy (viz *Auditní reporty*) – retence dat 1 rok,
- výsledky operací a workflow – retence dat 1 měsíc.

1.5.1.6 Verzování, zálohování a obnova

IdM bude verzováno v Git repository OZP a bude nasazováno do jednotlivých prostředí z Gitu pomocí nasazovacích nástrojů, např. *Jenkins*. Zálohování bude prováděno nástroji EMC – Dell Networker.

V IdM je zálohování na dvou úrovních:

- Záloha souborového systému aplikačního serveru.
- Pravidelným exportem dat z IdM databáze.

Řešení IdM splňuje tyto požadavky obnovy:

- RTO 1 den (Recovery Time Objective, čas na obnovu systému po výpadku)
- RPO 4 hodiny (Recovery Point Objective, maximální povolená ztráta dat po výpadku)

1.5.1.7 Odstávka

Pro IdM řešení jsou vyhrazena servisní okna pro údržbu a aktualizace. Výpadky v tuto dobu se nepočítají do SLA:

- Pracovní dny 20:00 – 06:00
- Víkendy

1.5.1.8 Požadavky na monitoring

Pro zdravý běh IdM systému je třeba monitorovat některé parametry. OZP využívá pro monitoring nástroj MONET. Objednatel požaduje napojení IdM a PAM na nástroj MONET. IdM řešení poskytuje možnost monitoringu těchto kategorií:

- Životaschopnost aplikační vrstvy na aplikačních portech.
- Volné místo na diskových oddílech IdM serverů – minimálně 80 %.
- Využití procesoru IdM serveru – v rozpětí jedné hodiny by nemělo překračovat 80 %.
- Využití paměti serveru – v rozpětí jedné hodiny by nemělo překračovat 80 %.

1.5.1.9 Uživatelské rozhraní

Uživatelské rozhraní IdM splňuje tyto požadavky:

- Je podporováno rozlišení 1280 x 768 a vyšší.
- Vyhledávání informací (uživatelé, role) je fulltextové.

1.5.1.10 Notifikace

Uživatel IdM je informován o vybraných událostech. Notifikace probíhá zasláním emailu na emailovou adresu nebo SMS zprávou.

Notifikace e-mailem:

- Nový úkol pro správce offline koncového systému.
- Manuálně řízené (offline) systémy.
- Iniciální heslo, viz *Vznik identity*.
- Resetované heslo, viz *Reset hesla*.
- Upozornění před vypršením hesla, viz *Heslo*.
- Založení identity – zaměstnanec, externista, privilegovaná identita, viz *Vznik identity*.
- Časové omezení role, např. *při změně pracovní pozice,* viz *Aktualizace identity*.
- Žádost o přidělení role ke schválení, viz *Přidání oprávnění*.
- Výsledek schvalování žádosti, viz *Přidání oprávnění*.

- Přidělení/odebrání oprávnění, viz *Řízení oprávnění*.
- Změna platnosti identity, viz *Platnost identity*.
- Zánik identity – zaměstnanec, externista, privilegovaná identita, viz *Zánik identity*.
- Exspirující identity, viz *Archivace*.
- Notifikace pro podezřelé chování včetně možnosti automatického nebo manuálního ukončení relace, viz *Notifikace*.

Notifikace SMS zprávou:

- Iniciální heslo, viz *Vznik identity*.
- Resetované heslo, viz *Reset hesla*.

1.5.2 Identita

Kapitola popisuje objekt identity v intencích IdM řešení.

Vysvětlení klíčových pojmů:

- V dokumentu je slovo „identita“ používáno ve smyslu objektu osoby v systému IdM (v jeho databázi)
- Slovo „uživatel“ používáme ve významu osoby, která se systémem IdM pracuje.
- Například *hovoříme o uživateli, který žádá o přístupová práva pro identitu.*
- V tomto dokumentu jsou slova identita a uživatel používána jako synonyma.

1.5.2.1 Typy identit

Základními typy identit v OZP jsou kmenoví zaměstnanci, zaměstnanci pracující na základě DPČ/DPP a uživatelé třetích stran, dále jen „externisté“. Ty představují běžné identity. Běžné identity mohou mít privilegovanou identitu, která představuje zvýšené právo osoby v nějakém koncovém systému.

Dalším typem identit jsou technické účty – registrované identity pro účty aplikací v koncových systémech.

Přibližné počty uživatelů jsou následující:

- Zaměstnanci na HPP: cca 400
- Zaměstnanci na DPČ/DPP: cca 250
- Externisté: cca 150
- Privilegovaní uživatelé: cca 125
- Technické účty: cca 30-50

Vlastnictví účtu:

- Technický účet: vlastníkem je manažer identity.
- Ostatní identity: vlastníkem je osoba, na kterou je identita napsána.

Významnější fluktuace:

- Každý měsíc dochází k cca 20 nástupům nových pracovníků a 10 odchodům (HPP, DPČ a DPP).

Interní identity

Interní identity jsou kmenoví zaměstnanci OZP a zaměstnanci OZP pracující na základě DPČ/DPP.

Zdrojem těchto identit je personální systém KS.

Externí identity

Externí identity, jinak také externisté, jsou uživatelé třetích stran (dodavatelů), s přístupem do koncových systémů OZP.

Zdrojem těchto identit je manuální vstup z rozhraní IdM.

Privilegované identity

Privilegovaná identita představuje uživatele s vyššími právy v systému IdM nebo koncovém systému. Privilegovaná identita i účet jsou jmenné – jednoznačně přiřaditelné konkrétní osobě. Praxe sdílených privilegovaných účtů podporována není.

Výchozí sdílené privilegované účty, které systémy mají z výroby (administrator, root, sa a podobné) mají „obálkové“ heslo (neznámé, uložené na chráněném místě pro případ nouze) a běžně se nepoužívají. Tyto výchozí účty jsou v IdM v režimu „chráněných“ účtů – IdM si jich nevšímá.

Základní princip práce s vyššími oprávněními je následující:

1. Uživatel si pod svou běžnou identitou požádá o privilegovanou identitu.
    - Toto se děje pomocí role.
    - Po schválení role vzniká v IdM privilegovaná identita.
2. Uživatel se přihlásí pod privilegovanou identitou a zde si žádá o vyšší oprávnění do koncových systémů.

Technické účty

Technické účty představují typ identity, pod kterou se hlásí jeden systém do jiného. Příkladem *je IdM, které se hlásí do koncových systémů, aby zde mohlo pracovat s uživatelskými účty.* Technický účet spravuje správce IdM. Specifikem technického účtu je, že se pod ním nikdo nehlásí do IdM. Z toho důvodu nemá technický účet přidělenou roli „Běžného uživatele IdM“.

Zákaznické identity

Zákaznické identity, například *v aplikaci Vitakarta*, nejsou systémem IdM řízeny.

1.5.2.2 Atributy identity

O identitě jsou v IdM udržovány následující informace:

- Přihlašovací jméno (login)
- Plné jméno
- Křestní jméno
- Příjmení
- Titul před jménem
- Titul za jménem
- E-mailová adresa – privilegovaná identita nemá e-mailovou adresu (tzn. nemá mailbox)
- Alternativní e-mailové adresy
- Typ identity
  - ZAM – běžný zaměstnanec
  - EXT – externista, dodavatel
  - ADM – privilegovaná identita
  - SVC – technické účty
- Název organizační jednotky
- Systemizované místo – současná pozice
  - Kód systemizovaného místa
  - Platnost od
  - Platnost do
- Systemizované místo – budoucí pozice
  - Kód systemizovaného místa
  - Platnost od
  - Platnost do
- Manažer (login)
- Telefonní číslo – pevná linka
- Autentizační mobilní telefon

        - Chodí na něj SMS zprávy z IdM
        - Uživatel může atribut editovat
    - Hesla identity
        - Zašifrované aktuálního heslo
        - Datum změny hesla
        - Zašifrovaná předchozí hesla
    - Přidělený token pro druhý faktor přihlášení
    - Přidělená karta pro SSO do pracovní stanice
    - Přidělený vstupní čip
    - Stav identity – povolená, zakázaná, archivovaná
    - Platnost identity od
    - Platnost identity do
    - Metadata o identitě
        - Datum a čas žádosti o identitu
        - Kdo žádal o identitu + zdůvodnění
        - Datum a čas schválení žádosti o identitu
        - Seznam schvalovatelů + komentáře
        - Datum a čas vytvoření
        - Kdo vytvořil
        - Datum a čas poslední úpravy
        - Kdo upravil

1.5.2.3 Autoritativní zdroje

Autoritativním zdrojem atributů identit je:

- Systém KS pro interní identity.
- Manuální vstup pro externí identity a technické účty přes rozhraní (frontend) IdM.
- Běžná identita pro privilegovanou identitu.

1.5.2.4 Politiky

Politiky určují pravidla pro tvorbu uživatelského jména a hesla. Politiky splňují § 19 vyhlášky o kybernetické bezpečnosti a čl. 9.3.1 „Bezpečnostní politiky informací OZP“ (BPI OZP) v platném znění.

1.5.2.5 Aktuální znění odstavce 9.3.1 BPI OZP platnost a účinnost od 1. 2. 2019

(1) Všichni uživatelé (zaměstnanci OZP i zástupci třetích stran) musí při výběru a používání hesel dodržovat následující bezpečnostní postupy a pravidla, se kterými musí být náležitě srozuměni:

- Uživatelé jsou povinni udržovat svá hesla v naprosté tajnosti a nakládat s nimi tak, aby nemohlo jejich prozrazením dojít ke zneužití uživatelských účtů neoprávněným vstupem do systému jinou osobou. Tato povinnost představuje zejména:
  - nezaznamenávat hesla v čitelné formě např. na papír, do souborů nebo do mobilních výpočetních prostředků, pokud není uložení provedeno schváleným bezpečným způsobem,
  - neprozrazovat hesla žádné další osobě,
  - nezadávat hesla v případech, může-li dojít k jejich odpozorování.
- V případě prozrazení nebo podezření na kompromitaci hesla je uživatel povinen heslo okamžitě změnit a neprodleně informovat bezpečnostního správce ÚI.
- Bezodkladně zneplatnit heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření.
- V případě zapomenutí hesla nebo vypršení jeho platnosti musí uživatel požádat o přidělení nového hesla a zpřístupnění účtu příslušného správce IS. Bezpečnostní správce ÚI posoudí možnost bezpečnostního incidentu. Jedná-li se o prosté zapomenutí hesla, bere tento případ pouze na vědomí. Dodržet důvěrnost autentizačních údajů při obnově přístupu.
- Pro ověření identity uživatelů, správců a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.
- Do doby splnění požadavku podle předchozího bodu musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat autentizaci pomocí kryptografických klíčů a zaručit obdobnou úroveň bezpečnosti.
- Do doby splnění požadavků podle předchozích dvou bodů musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, vynucovat pravidla délky hesla alespoň 12 znaků u uživatelů a 17 znaků u administrátorů.
- systém pro řízení přístupu:
  - musí umožnit zadat heslo o délce alespoň 64 znaků, neomezující použití malých a velkých písmen, číslic a speciálních znaků,
  - musí umožnit uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,
  - nesmí umožnit uživatelům a správcům IS zvolit si nejčastěji používaná hesla, tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem, opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel,
  - v případě používání autentizace pouze účtem a heslem dále vynutit bezodkladnou změnu výchozího hesla po jeho prvním použití.
- Uživatelská hesla by měla splňovat následující předpoklady:
  - budou zapamatovatelná,
  - nebudou založena na skutečnostech, které může někdo snadno odhadnout nebo je získat z osobních informací uživatelů, např. jméno, příjmení, telefonní číslo, datum narození, oblíbená barva, film apod.
  - nebudou obsahovat po sobě jdoucí stejné numerické nebo číselné znaky,
  - uživatel je povinen vytvářet kvalitní silná (obtížně uhodnutelná) hesla a při jejich vytváření dodržovat následující pravidla:
  - minimální složitost hesla: heslo bude obsahovat alespoň 3 z následujících čtyř požadavků:
    * alespoň jedno malé písmeno (a-z),

    * alespoň jedno velké písmeno (A-Z),
    * alespoň jednu číslici (0-9),
    * alespoň jeden speciální znak (např. !@#$%&*.-+),
  - nevytvářet jednoduchá hesla typu 12345Abc+, Abcdef12+ apod.
  - heslem nesmí být jednoduché slovníkové výrazy (například jméno nebo příjmení uživatele ani uživatelské jméno účtu uživatele, jména rodinných příslušníků, jména měst, známých osobností, data narození apod.).
- Uživatel je povinen pravidelně měnit svá hesla. Doba platnosti hesla je omezena na 90 dnů a po uplynutí této lhůty je změna hesla vynucena operačním systémem, IS, aplikací nebo uzamčením účtu uživatele. U jednotlivých IS se může tato doba exspirace hesel pro specifické skupiny uživatelů lišit, musí však být uvedena v dokumentaci daného IS.
- Privilegovaný uživatel (správce IS) je povinen měnit svá hesla pravidelně, minimálně jednou za 90 dní.
- Uživatel je povinen změnit dočasné heslo ihned po prvním přihlášení s tímto dočasným heslem.
- Při změně hesla nesmí uživatel použít opakovaně stejné heslo (systém nedovolí použít opakovaně stejné heslo pouze doplněné např. číselnou řadou).
- Uživatelé nesmí začleňovat (ukládat) svá hesla do jakýchkoliv automatizovaných přihlášení, např. uložením hesel v makrech nebo ve správcích hesel některých aplikací např. internetových prohlížečích.
- Uživatelé nesmí sdílet individuálně přidělená hesla.
- Uživatelé nesmí používat stejná hesla pro různé systémy (zejména nepoužívat stejná hesla jako v soukromé činnosti).
- Úsek informatiky zajišťuje, všude tam kde je to možné s ohledem na technologické možnosti, vynucení výše uvedených pravidel práce s heslem odpovídajícími nástroji pro ověřování identity uživatelů. Primárně se jedná o přístup do domény OZP (přihlášení do PC).
- Systém ukládá historii hesla (systém uživateli nedovolí při změně použít heslo naposledy použité).
- Po 3 neúspěšných pokusech o přihlášení dojde k uzamčení účtu. Pro odblokování účtu musí být požádán příslušný správce IS. Bezpečnostní správce ÚI posoudí možnost bezpečnostního incidentu. Jedná-li se o chybu oprávněného uživatele, bere tento případ pouze na vědomí.
- Nastavit pravidla pro opětovné ověření identity po 30 minutách nečinnosti.
- Zajistit centralizovanou správu interních a externích identit.

(2) Uživatel je povinen dodržovat pravidla a postupy správného užívání předepsané pro ostatní prostředky užívané k autentizaci (magnetické a čipové karty, soukromé elektronické klíče apod.).

E-mailová adresa

E-mailovou adresu generuje systém IdM ve formátu <Jméno>.<Příjmení>@ozp.cz. V případě shody doplní na konec <Příjmení> pořadovou číslici, počínaje dvojkou. Shoda se provádí nad současnými i alternativními emailovými adresami (loginy) identit (např. *nad emailovými adresami uživatelek „za svobodna“*).

Příklady

- Jan.Novak@ozp.cz
- Jan.Novak2@ozp.cz

Přihlašovací jméno

Přihlašovací jméno má následující strukturu:

- [<prefix>.]<emailová adresa>

Prefix je stanoven dle typu identity:

- bez prefixu – běžný zaměstnanec pro všechny typy smluv
  - Jan.Novak@ozp.cz
  - *Poznámka: po zavedení čipových karet nebude muset zaměstnanec přihlašovací jméno psát vůbec*
- adm – administrátorská, privilegovaná identita běžného zaměstnance
  - adm.Jan.Novak@ozp.cz

Pro dodavatelské identity má přihlašovací jméno tuto strukturu:

- <e-mailová adresa> – e-mailová adresa dodavatele
  - Jan.Novak@it-experti.cz
- adm.<e-mailová adresa> – administrátorská, privilegovaná identita dodavatele
  - adm.Jan.Novak@it-experti.cz

Pro technické účty je stanovena struktura:

- svc.<zkratka názvu systému> – příklad
  - svc.IdM –účet produkčního IdM v koncovém systému
  - účty nejsou rozlišovány podle prostředí,

Heslo

Kapitola popisuje politiky hesel. Politika se může lišit podle prostředí (vývojové, testovací, produkční). Politika je v souladu s Viz §19 vyhlášky a čl. 9.3.1 „Bezpečnostní politiky informací OZP“, viz *Politiky*.

Obecné předpoklady k politice hesel:

- Nejsou založena na osobních informacích uživatelů: login, jméno, příjmení.
- Neobsahuje po sobě jdoucí stejné numerické nebo číselné znaky.

- Neobsahuje vydefinovaná zakázaná slovníková hesla.
- Heslo se neshoduje s 12 předchozími hesly.
- Uživatel je povinen změnit dočasné heslo ihned po prvním přihlášení s tímto dočasným heslem.

1.5.2.6 Organizační struktura

IdM si pro své potřeby udržuje efektivní stromovou strukturu identit.

Strom organizační struktury získává systém IdM z personálního systému. V rámci pravidelného přenosu dat se jednou denně aktualizuje.

Externisti

Pro správu externistů je v IdM udržovaná struktura smluv.

Při vzniku smluvního vztahu je založena odpovídající organizace do IdM.

Každá organizace má uvedeno

- Platnost od
- Platnost do
- Manažer externistů (pracovník OZP)

Po uplynutí doby platnosti jsou identity v této organizaci zneplatněny, viz Zánik identity.

1.5.3 Procesy

1.5.3.1 Vznik identity

Zaměstnanec

Vznik nové identity zaměstnance začíná v personálním úseku založením v personálním a mzdovém systému KS.

- U identity je mimo jiné uvedeno:
  - osobní číslo,
  - název systemizovaného místa,
  - umístění v organizační struktuře.
- Po založení uživatele vygeneruje personální úsek osobní číslo uživatele.
- Osobní číslo je unikátní.
- Založení uživatele je většinou provedeno před nástupem, nejpozději v den nástupu.

Z personálního systému KS je identita automaticky v rámci pravidelné synchronizace založena do systému IdM. Zde dojde k následující posloupnosti kroků:

1. Vygenerování přihlašovacího jména (loginu) systémem IdM.
2. Vygenerování iniciálního hesla systémem IdM.
3. Přidělení základních zaměstnaneckých rolí.
    - Spuštění schvalovacího workflow.
    - Role reprezentují základní oprávnění a nastavení zaměstnance, kvótu na emailovou schránku a podobně.
4. Notifikace nadřízenému pracovníkovi o založení identity.

Externista

Založení identity externisty probíhá v systému IdM:

1. Pověřená osoba založí novou identitu ve speciální struktuře pro externisty v IdM odpovídající smlouvě s externistou.
    - Pokud není struktura pro vedení Externistů založena, je třeba iniciovat její založení, včetně správného nastavení času „platnost do“
2. Dále pověřená osoba vyplní základní informace o externistovi.
3. Systém IdM spustí schvalovací workflow:
    - Krok 1: schvaluje manažer
    - Krok 2: schvaluje „speciální role“ za smluvní a právní oblast (potvrzení NDA)
4. Systém IdM vygeneruje přihlašovací jméno (login) a identitu založí.
5. Systém IdM vygeneruje iniciální heslo.
6. Manažer externisty je informován o založení identity externisty.

Privilegovaná identita

Založení privilegovaného uživatele probíhá v systému IdM:

1. Uživatel pod svým běžným účtem požádá v aplikaci IdM o přidělení privilegované identity pomocí žádosti o roli.
2. Žádost prochází procesem schvalování.
3. Po dokončení schvalování systém IdM vygeneruje přihlašovací jméno (login) a identitu založí.
4. Systém IdM vygeneruje iniciální heslo.
5. Žadatel o privilegovanou identitu je informován o založení identity (IdM zašle notifikaci).

Technický účet

Založení technického účtu probíhá v systému IdM:

1. Pověřená osoba založí novou identitu v organizační složce pro systém, pod který technický účet patří.
   - Pokud není struktura pro systém technického účtu založena, je třeba nejprve iniciovat její založení.
2. Pověřená osoba vyplní základní informace o technickém účtu, především login a manažera účtu.
3. Systém IdM vygeneruje iniciální heslo.
4. Manažer technického účtu (manažer organizační složky pro technické účty) je informován o založení identity technického účtu.

1.5.3.2 Předání iniciálního hesla

Vygenerované iniciální heslo je uživateli předáno následujícím způsobem:

1. Zaměstnanec
   - Iniciální heslo je zasláno uživateli a jeho manažerovi emailem.
2. Privilegovaná identita
   - Iniciální heslo je zasláno uživateli běžné identitě.
3. Externista
   - Iniciální heslo je zasláno uživateli a jeho manažerovi emailem.
   - Má-li uživatel uvedeno mobilní telefonní číslo, je mu zasláno heslo SMS zprávou.
4. Technický účet
   - Iniciální heslo je zasláno uživateli běžné identity a jeho manažerovi emailem.

Změna hesla je vynucena při prvním přihlášení do systému IdM.

1.5.3.3 Návraty

V případě návratu identity, např. *mateřská dovolen*á, je proces obdobný, jako při vzniku identity zaměstnance, s rozdíly:

- Není vytvářena nová identita, ale je obnovena archivní identita.
- Emailová schránka uživatele již existuje, je připojena k identitě a nastavena na aktivní.

1.5.3.4 Aktualizace identity

Zaměstnanec

Změny v atributech zaměstnance jsou propisovány do systému IdM z personálního systému při pravidelné aktualizaci. V dalších kapitolách jsou uvedena některá specifika změny atributů.

Změna jména a příjmení manuálně

V případě indikace změny jména a příjmení dochází k

- automatické aktualizaci atributů identity a jejich propagaci do koncových systémů – kromě loginu a e-mailové adresy,
- vytvoření úlohy pro správce IdM k aktualizaci loginu a e-mailové adresy.

Login a e-mailová adresa je nastavena správcem IdM po dohodě s uživatelem. Poté správce IdM úlohu zakončí.

Externista

Změnu atributů identity externisty provádí manuálně manažer externisty. Za aktuálnost údajů je zodpovědný manažer externisty.

Privilegovaná identita

Atributy privilegované identity jsou automaticky měněny na základě změny atributů běžné identity. Změna jména, příjmení a loginu probíhá stejně jako při změněn běžného účtu zaměstnance, viz *Zaměstnanec*.

1.5.3.5 Změna hesla v online systémech

Změna hesla je centrální přes IdM a je synchronizována do všech napojených online systémů.

Přímá změna hesla v napojených aplikacích k IdM je zakázána následujícími způsoby:

- Změna hesla ve Windows je zakázána pomocí GPO (globální politika).
- Pokud je technicky možné zakázat změnu hesla v systémech, je toto provedeno.
- V ostatních případech je změna hesla zakázána organizačně směrnicí. Pokud si uživatel přesto heslo lokálně změní, činí tak z vlastního rozhodnutí.

1.5.3.6 Reset hesla

Pokud uživatel zapomene heslo, pro obnovení má tyto možnosti:

1. Reset hesla uživatelem – nové náhodně vygenerované heslo.
2. Uživatel má také možnost kontaktovat svého manažera.
    - Manažer v IdM provede reset hesla uživatele.

Distribuce hesla:

1. Má-li uživatel uvedeno mobilní telefonní číslo, je mu zasláno heslo SMS zprávou.
2. Zároveň je heslo zasláno uživateli emailem s instrukcemi, jak heslo změnit přes IdM.
3. Po přihlášení uživatele do IdM, je vynucena změna hesla.

1.5.3.7 Řízení oprávnění

Přidání oprávnění

O nová oprávnění žádá uživatel v rozhraní systému IdM. Požádat může pro sebe nebo pro libovolného jiného uživatele IdM.

- Systém IdM uživateli nabízí strukturovaný katalog rolí, ze kterého si uživatel vybírá.
- Uživatel vyplní žádost o přidělení oprávnění a žádost odešle. Součástí žádosti je výběr role a zdůvodnění pro přidělení role.
- Systém IdM spustí schvalovací workflow.
- Workflow dle konfigurace jednotlivých rolí obsahuje definované schvalovací úrovně viz níže.
- Jednotliví schvalovatelé obdrží notifikační emaily o potřebě schválit žádost v IdM s odkazem do IdM.
- Při více schvalovatelích je konfiguračně možné nastavit, zda stačí schválení jednoho z nich nebo je třeba schválení všemi.
- Po dokončení schvalovacího workflow je role přiřazena identitě buď automaticky pomocí IdM nebo ručně administrátorem daného systému.
- V případě, že role vyžaduje vytvoření účtu v koncovém systému, je tento účet založen.
- Po přidělení role je žadatel systémem IdM informován o výsledku schvalování notifikačním e-mailem.

Schvalovací úrovně

- Manažer identity.
- Garant aktiva – schvaluje přístupy uživatelů k dané části koncového systému.
- Licenční specialista – kontroluje, zda je na daném koncovém systému dostupná licence pro uživatele.
- Compliance/Bezpečnost ICT – schvaluje přístupy z pohledu bezpečnosti ICT. Např. *schválení VPN pro dodavatele*.
- Školitel – po proškolení uživatele schválí požadavek. Díky tomuto je účet v daném systému založen až po proškolení. Školení samotné probíhá v testovacím/školícím prostření na testovacím účtu k tomu určeném.
- Speciální schvalovací role – role zavedená pro potřeby řešení ad hoc schválení mimo uvedené úrovně. Např. *Generální ředitel společnosti OZP.*

Odebrání oprávnění

Odebrání oprávnění může proběhnout jedním ze dvou způsobů:

- automatickým procesem jako následek změny v autoritativním systému (typicky personální systém KS)
- nebo z uživatelského rozhraní – uživatelem, jeho manažerem nebo správcem IdM.

Odebrání automatickým procesem probíhá následovně:

- Systém IdM detekuje změnu v autoritativním systému, která vede k odebrání oprávnění.
- Systém IdM notifikuje uživatele a jeho manažera o odebrání oprávnění.
- V případě, že oprávnění nárokovalo účet v koncovém systému, tento nárok zaniká (viz *Koncové systémy* / zánik nároku na účet).

Odebrání z uživatelského rozhraní probíhá následovně:

- Oprávněný uživatel žádá o odebrání oprávnění.
- Systém IdM spustí žádost o odebrání oprávnění.
- Schvalování je spuštěno na speciální roli „Schvalovatel odebrání role“.
- Po schválení je role odebrána identitě. V opačném případě se nic neděje.
- Systém IdM informuje uživatele a jeho manažera e-mailovou notifikací o odebrání oprávnění.
- V případě, že oprávnění nárokovalo účet na koncovém systému, tento nárok zaniká (viz *Koncové systémy* / zánik nároku na účet).

Změna oprávnění

Změna oprávnění je prováděna atomicky odebráním jedné a přidělením druhé role.

1.5.3.8 Platnost identity

Platnost identity v IdM určuje platnost účtů identity v napojených koncových systémech. Identity, expirující v nejbližším měsíci jsou pro kontrolu zasílány reportem, viz *Reporty o uživatelích*.

Zaměstnanec

Platnost identity je řízena z personálního systému KS – atributy platnosti od-do.

- Tuto platnost je možno přetížit v systému IdM manuální akcí správce IdM.
- O exspirujících identitách chodí manažerovi předem report.

Externista

Platnost identity externisty je řízena ručně manažerem externisty.

Privilegovaná identita

Platnost privilegované identity kopíruje platnost běžné identity.

Ad hoc

Platnosti identity je možno řídit manuálně v rozhraní správcem IdM.

Nastavení platnosti od nebo platnosti do:

1. Požadavkem mimo IdM je správce IdM požádán o nastavení platnosti identity.
2. Správce IdM nastaví platnost dle požadavku.
3. IdM notifikuje uživatele měněné identity a jeho manažera o nastavení platnosti.

1.5.3.9 Zánik identity

Zánik identity – možnosti:

- Konec smluvního vztahu se zaměstnancem – v systému KS.
- Konec smluvního vztahu s dodavatelem.
- Ad hoc zásah administrátora.

Konec smluvního vztahu se zaměstnancem

Zánik pracovního vztahu zaměstnance je indikován v systému KS. Na straně IdM je provedeno:

- Systém IdM změní heslo identity automaticky na náhodné.
- Platnost rolí je automaticky nastavena na D+7 (týdenní platnost).
- IdM zašle notifikační e-mail na manažera.

Po uplynutí doby D+7:

- Identita je v IdM archivována – viz kapitola *Ad hoc zánik*.

Konec smluvního vztahu s dodavatelem

Při ukončení platnosti smlouvy jsou účty pod příslušnou organizační složkou (ta reprezentuje smlouvu) v IdM automaticky ukončeny:

- Systém IdM změní heslo identity automaticky na náhodné.

- Platnost rolí je automaticky nastavena na D+14 (dvoutýdenní platnost).
- IdM zašle notifikační e-mail na manažera a na externistu.

Po uplynutí doby D+14:

- Identita je v IdM archivována – viz kapitola *Ad hoc zánik*.

Privilegovaná identita

Zánik privilegované identity je iniciován

- buď odebráním role privilegované identity od běžné identity,
- nebo zánikem běžné identity.

Na straně IdM je provedeno:

- Systém IdM změní heslo identity automaticky na náhodné.
- Platnost rolí je automaticky nastavena na D+1 (denní platnost).
- IdM zašle notifikační e-mail na uživatele běžné identity a jeho manažera.

Po uplynutí doby D+1:

- Identita je v IdM archivována – viz kapitola *Ad hoc zánik*.

Ad hoc zánik

Zánik identity je možno provést manuálně v rozhraní správcem IdM:

- Správce manuálně změní heslo na náhodné.
- Správce zneplatnění identitu.
- Platnost rolí je ručně nastavena na D+7 (týdenní platnost).

Po uplynutí doby D+7 od zneplatnění identity:

- Identita je v IdM archivována – viz kapitola *Archivace*.

1.5.3.10 Archivace

Při archivaci identit dochází k následujícím krokům:

- Role a oprávnění v koncových systémech jsou odebrány
  - Jedinou výjimkou je role do systému Exchange.
- E-mailová schránka Exchange je nastavena na neaktivní.
- Osobní data identity jsou vyčištěna.

Čištění osobních dat

U archivované identity dochází k čištění osobních dat. To pobíhá jedním ze způsobu:

- Odstranění informace.
- Anonymizace informace.
- Stanovení účelu dalšího uchování a ponechání informace.

Mazání emailových schránek

V rámci práce s archivovanými identitami probíhá v IdM pravidelná úloha na kontrolu emailových schránek:

- Pokud byla provedena archivace identity před 30 a více dny,
- Exchange schránka identity je smazána,
- identitě je odebrána role Exchange.

1.5.4 Role a oprávnění

1.5.4.1 Metodik IdM

Metodik IdM je externí konzultant (pracovník na straně Dodavatele) pro návrh a změny procesů systému IdM. Mezi jeho odpovědnosti patří:

- Komplexní zodpovědnost za Identity Management.
- Koncepční dohled nad rozvojem IdM systému.
- Navrhovat procesy v Identity Managementu a procesy související.
- Dávat podněty ke změn vnitřních předpisů, směrnic a metodik Objednatele v souvislosti se změnami v IdM.
- Zodpovídá za zajištění souladu systému IdM s legislativou a dává podněty k jeho úpravám.
- Dohlížet nad dodržováním nastavených architektonických pravidel v IdM, například:
  - *dodržování pravidel pro pojmenování rolí a loginů,*
  - *zavádění nových systémů do IdM (role)*.
- Dohlížet nad dodržováním nastavených neautomatizovaných procesů, týkajících se IdM, například:
  - *centrální změna hesla,*
  - *evidence externích identit.*
- Návrh a aktualizace matice přístupových práv dle systemizovaných místa.
- Návrh matice vlastníků přístupových práv a správa schvalovacích workflow.
- Analýza a návrh přístupových práv pro nové systémy.
- Správa rolí v prostředí IdM.

- Skládání aplikačních rolí do business rolí s ohledem na klasifikaci aktiva (veřejné, interní, důvěrné).

1.5.4.2 Principy správy rolí

Správa rolí z pohledu IdM:

- IdM zajišťuje řízení oprávnění v koncových systémech, tzn. jeho úkolem je
  - přidělit/odebrat aplikační role,
  - zajistit schvalování žádostí o oprávnění,
  - zajistit recertifikaci oprávnění.
- IdM umožní
  - skládání aplikačních rolí do business rolí,
  - vytvoření a použití hierarchie Business rolí.
- Katalog business rolí je umístěn v IdM.
- IdM umožňuje aplikační a business role
  - vytvořit,
  - recertifikovat obsah,
  - měnit.

Role v systému IdM definuje a spravuje Metodik IdM.

1.5.4.3 Struktura rolí a oprávnění

Systém IdM spravuje role. Role se dělí na dvě skupiny: aplikační a business role.

Aplikační role

Aplikační role představují oprávnění v koncových systémech a mohou být svázány s vytvářením účtu nebo s nastavováním atributů na koncových systémech.

Business role

Business role představují jednotlivé činnosti a pozice v rámci business procesů ve firmě. Business role se skládají z aplikačních a dalších business rolí.

1.5.4.4 Autorizační koncept IdM

Autorizační koncept určuje:

- Kdo může vidět jaké informace v IdM (např. *atributy identity v koncovém systému*).
- Jaké operace s nimi může provádět (číst, změnit, mazat).

Autorizační koncept popisuje základní sadu autorizací pomocí přidělených rolí. Autorizační koncept definuje Metodik IdM.

1.5.4.5 Atributy rolí

Role v IdM obsahují atributy níže. Na atributy role jsou nadefinována validační pravidla.

- Název role – název dle konvence.
- Popis – uživatelský popis, např. *pro koho je role určena a co umožňuje*.
- Vlastník role – identita, která je vlastníkem role a je zodpovědná za její obsah.
- Příznaky
  - Přidělení role schvaluje manažer (A/N).
  - Přidělení role schvaluje garant aktiva (A/N).
  - Přidělení role schvaluje licenční specialista (A/N).
  - Přidělení role schvaluje Compliance/Bezpečnost ICT (A/N) – je zavedena 1 v systému.
  - Přidělení role podléhá proškolení (A/N)
  - Přidělení role schvaluje „speciální role“ (A/N) – je zavedena 1 v systému
  - O roli lze žádat (A/N) – roli lze vybrat v Katalogu požadavků, tj. uživatel o ni může žádat.
- Garant aktiva – role
- Licenční specialista – role
- Školitel – role
- Typ role – pro jakou skupinu identit je role určena
- Stav identity – povolená, zakázaná, archivovaná
- Datum platnosti role od
- Datum platnosti role do
- Metadata o roli:
  - Datum a čas vytvoření
  - Kdo vytvořil roli
  - Datum a čas poslední úpravy
  - Kdo provedl poslední úpravu role
  - Kdo schválil poslední úpravu role
  - Datum poslední recertifikace role
  - Komentář ověřovatele poslední recertifikace
  - Poslední ověřovatel recertifikace
  - Výsledek poslední recertifikace

1.5.4.6 Atributy vazby uživatel-role

Oprávnění představuje vazbu mezi identitou a rolí. Atributy této vazby v IdM jsou:

- Stav přidělení role (platné, neplatné, archivované oprávnění)
- Atributy žádosti o roli
- Žadatel – login toho, kdo o oprávnění žádal
- Datum žádosti o roli
- Důvod žádosti – text ze zdůvodnění žádosti o roli
- Atributy schvalovacího workflow
- Komentáře a data (časy) schválení od jednotlivých schvalovatelů
- Datum a čas přidělení nároku na roli
- Platnost přidělení role od
- Platnost přidělení role do
- Metadata recertifikace:
  - Datum poslední recertifikace vazby
  - Komentář ověřovatele poslední recertifikace
  - Poslední ověřovatel recertifikace
  - Výsledek poslední recertifikace

1.5.5 Audit a reporting

Kapitola popisuje náležitosti, které IdM řešení splňuje v oblasti logování, auditu a reportingu.

- Produkt umožňuje generovat reporty do formátů PDF, CSV, HTML, XML, XLS, XLSX, DOCX
- Reporty je možné na vyžádání zasílat emailem jako přílohu.
- Tuto přílohu je možné na vyžádání zazipovat.

1.5.5.1 Auditní logy IdM

Systém IdM eviduje všechny změny nad spravovanými objekty (identita, role, oprávnění, koncový systém, organizační jednotka) v této formě detailu o jednotlivém záznamu:

- Kdo (identifikátor)
- Odkud (zdrojová IP adresa)
- Kdy (datum a čas)
- Pro koho/co (pro identitu, roli, …)
- Co (operace)
- S jakým výsledkem – kód + zpráva

1.5.5.2 Auditní reporty

Auditní reporty umožní vygenerovat informace z těchto oblastí:

- IdM versus koncový systém: Kompletní přehled historie událostí mezi IdM a koncovým systémem včetně informací, kdo změnu provedl, kdy ji provedl, na kterém systému a na základě čeho.
- Role a organizace: Kompletní přehled historie změn provedených nad libovolnými rolemi a organizacemi včetně informací, kdo změnu provedl, kdy ji provedl a na základě čeho.
- Identita: Kompletní přehled historie změn provedených nad identitou, např. *synchronizace atributů, přidělení role, změn atd. včetně informací kdo změnu provedl, kdy ji provedl a na základě čeho*.
- Auditní záznamy: Report z auditních záznamů.
- Auditní report je navíc možné procházet v GUI IdM.

1.5.5.3 Reporty o uživatelích a rolích

Reporty o uživatelích a rolích v IdM jsou:

- Přehled organizační struktury i s přiřazenými identitami.
- Přehled rolí s přímo i nepřímo přiřazenými identitami.
- Report identit s filtrováním dle kritérií.
- Manažerský přehled podřízených identit exspirujících na konci daného měsíce.
- Kontrola konzistence IdM – primárně pro vyhledávání chyb, např. *role má neplatného vlastníka, manažer je neplatný atd*. Příjemcem je Metodik IdM.
- Kontrolní export rolí – kontrola správnosti přiřazení aplikačních rolí do business rolí, kontrola atributů rolí, např. *schvalovatelé atd.*

1.5.5.4 Rekonciliační reporty

Rekonciliační reporty slouží k prozkoumání srovnání stavu mezi IdM a koncovými systémy:

- Identifikace účtů, ke kterým nebyl v IdM nalezen vlastník (nespárované účty).
- Přehled účtů v koncových systémech a jejich napojení na identity v IdM.
- Rekonciliační report pro vybraný koncový systém – chronologický seznam akcí nad koncovým systémem.

1.5.5.5 Recertifikační reporty

Recertifikační reporty doplňují funkcionalitu recertifikací vazeb identita-role:

- Všechny recertifikační kampaně a jejich stav.
- Řešené případy v recertifikačních kampaních.
- Rozhodnutí jednotlivých ověřovatelů.

1.5.6 Parametry řešení

IdM řešení musí být naceněno a bude spuštěno s těmito parametry:

Uživatelé / identity	**Aktuální stav**	**Celkový plánovaný stav**
Počet aktivních uživatelů	800	1000
Počet privilegovaných identit	125	185
Počet koncových systémů připojených k IdM	6	20

Produkt musí podporovat výše uvedené parametry a zároveň musí být výkonově dimenzován na variantu celkového plánovaného (budoucího) stavu a Objednatel tak nebude akceptovat požadavky na změnu architektury. Cena dle přílohy č. 2 Smlouvy je stanovena jednak ve výši pro aktuální stav. Dále je uvedena částka tzv. inkrementálního nárůstu cen licencí a podpory pro případ navýšení počtu uživatelů, identit či systémů. V případě snížení počtu uživatelů, identit či systémů dojde k tzv. inkrementálnímu snížení cen licencí a podpory, a to za podmínek dle čl. 5.1.12 Smlouvy.

2 IDM – DALŠÍ POŽADAVKY

Kapitola obsahuje další požadavky Objednatele, které nejsou základní součástí Díla a Objednatel je může, ale nemusí požadovat a odebrat.

2.1 ROZŠÍŘENÉ ATRIBUTY

Rozšíření modelu IdM o atributy:

- Čísla certifikátů PostSignum
- Tokeny přidělené identitě
- Karty přidělené identitě
- Vstupní čipy přidělené identitě

2.2 SYSTEMIZOVANÁ MÍSTA

2.2.1 Hierarchie v IdM

Systém IdM spravuje systemizovaná místa zaměstnanců. Realizuje je stromovou strukturou ve zjednodušené formě. Pro příklad uvádíme *strukturu tří organizačních jednotek, přičemž pod každou jsou dvě až tři systemizovaná místa:*

- *Organizační složka úrovně 1*
  - *Systemizované místo 1.A*
  - *Systemizované místo 1.B*
  - *Organizační složka úrovně 2*
    - *Systemizované místo 2.A*
    - *Systemizované místo 2.B*
      - *Organizační složka úrovně 3*
      - *Systemizované místo 3.A*
      - *Systemizované místo 3.B*
      - *Systemizované místo 3.C*

2.2.2 Přidělování rolí dle míst

Hierarchie v IdM umožňuje definovat základní oprávnění, která patří systemizovanému místu, přičemž platí, že:

- oprávnění definovaná na Organizační složku se dědí na podřízené Organizační složky a systemizovaná místa,
- oprávnění definovaná na systemizované místo se dále nedědí.

Strom systemizovaných míst získává systém IdM z personálního systému. V rámci pravidelného přenosu dat se jednou denně aktualizuje.

2.3 ZMĚNA LOGINU A E-MAILOVÉ ADRESY AUTOMATICKY

V případě indikace změny jména a příjmení dochází k

- přejmenování přihlašovacího jména v systému IdM (e-mailová adresa),
- propagaci nového přihlašovacího jména a atributů do koncových systémů,
- Staré přihlašovací jméno je uloženo v systému Exchange jako alternativní e-mailová adresa (kontinuita v zasílání emailů).

2.4 ZMĚNA OPRÁVNĚNÍ PŘI ZMĚNĚ SYSTEMIZOVANÉHO MÍSTA

Při změně systemizovaného místa (pozice) dojde k:

1. Přidělení rolí odpovídajících nové pozici.
2. Informace přijde ze systému KS, systém IdM dle nové pozice zažádá o nové role.
3. Alternativně lze toto provést manuálním vstupem ve formě žádosti v IdM.
4. Spustí se schvalování na nové role.
5. Posouzení původně přidělených rolí:
    - Při provedení změny pozice se původní role časově omezí a systém IdM o tomto informuje uživatele a jeho manažera (zašle notifikaci).
    - Na původní role se spustí recertifikační kampaň – nový vedoucí tyto role potvrdí nebo zamítne.

2.5 EDITOVATELNÉ ŠABLONY NOTIFIKACÍ

Systém umožní editaci textových notifikačních šablon.

2.6 VERZOVÁNÍ ROLÍ

Systém musí pokrýt tyto základní funkčnosti:

- Produkt IDM umožňuje spravovat verze rolí.
- Je navržen postup, jak evidovat aktuální a předchozí verzi rolí.
- Je navržen postup, jak bezpečně nahradit roli novější verzí.

2.7 KONTROLNÍ PRAVIDLA

Systém IDM umožní definovat kontrolní pravidla nad rolemi, která jsou aplikována při žádosti nebo přidělení role identitě:

- Pravidlo „oddělení povinností“ – Segregation of Duties, výlučnost rolí, přidělení role způsobí odebrání ostatních rolí ze stejné skupiny rolí.
- Pravidlo „podmínky přidělení“ – Slouží k podmíněnému přiřazení role. Identita, která pravidlo nesplňuje, nemůže mít podmíněnou roli přiřazenou. Např. *role může být přiřazena pouze vybrané organizační jednotce a TPÚ třídy*.
- Pravidlo „aspoň jeden uživatel“ – Alespoň jeden uživatel má roli přiřazenou. Slouží k zajištění obsazení klíčových schvalovacích a kontrolních rolí.

2.8 DELEGACE OPRÁVNĚNÍ

Systém musí pokrýt tyto funkčnosti:

- Delegování vybraného požadavku nebo skupiny požadavků ke schválení na jiného schvalovatele.
- Na definovanou dobu (od-do) nastavit zástupce pro všechny požadavky, které budou v definované době (od-do) směrované na vybraného schvalovatele.
    - Zastupování musí být aditivní – původní schvalovatel musí být schopen požadavek schválit stejně, jako kdyby zástup nebyl nastaven.
- Po definovanou dobu nastavit plnou zastupitelnost na zvoleného uživatele.
- Možnost nastavení delegace na nové i rozpracované požadavky.
- Možnost tranzitivní delegace – původní schvalovatel A nastaví delegaci na uživatele B, který nastaví delegaci na jiného uživatele C.
- O delegaci je elektronická stopa v auditním deníku systému IdM.
- Tímto způsobem lze delegovat i přidělené role, které odpovídají oprávněním v koncových systémech.
- Tuto akci může provést i správce IdM na vyžádání – toto musí být ošetřeno směrnicí, kdy a jak to lze udělat. Této možnosti se typicky používá v případech, kdy je třeba předat práva ke schvalování jiné identitě (např. *nemoc schvalovatele*).

2.9 PLNÁ PROJEKCE IDENTIT NA KONCOVÉ SYSTÉMY

Produkt IdM umožňuje plnou projekci identit na koncové systémy:

- Stav IdM systému je porovnán vůči koncovému systému, kde IdM systém má plný dohled nad účty.
- Nadbytečné účty jsou odstraněny, chybějící účty jsou založeny.

2.10 RESPONSIVNÍ DESIGN, CORPORATE BRANDING

Produkt umožňuje:

- responzivní design,
- možnost grafického přizpůsobení identitě firemní značky.

2.11 NAPOJENÍ NA MONITOROVACÍ NÁSTROJE FLOWMON A MONET

Auditní zprávy je možné zasílat do syslogu na aplikačním serveru IdM ve formátu CEF, odkud jsou směrovány do SIEM řešení Objednatele.

2.12 KONCOVÉ SYSTÉMY

Kapitola popisuje technické připojení koncových systémů k systému IdM.

2.12.1 VPN

Koncový systém VPN:

- Pro přístup přes VPN se pro druhý faktor používá HW tokenu (DataTravel).
- Po schválení žádosti IT administrátor nastaví token, vytvoří certifikát, nastaví prostupy na FW a na pracovní stanici uživatele povolí vzdálený přístup.
- Celkem cca 150 běžných uživatelů.
- V případě dodavatelských firem je možné zřídit pro VPN WAN uzel (stejný princip jako pobočka) nebo IPSEC tunel.

Rozhraní k IdM:

- Offline systém

Prostředí:

- Produkční: Ano

- Testovací: Ne
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano, úkol pro správce
Aktualizace účtu	Ano, úkol pro správce
Změna loginu účtu	Ano, úkol pro správce
Změna hesla	Ne
Řízení oprávnění	Ano, úkol pro správce
Povolení/Zakázání účtu	Ano, úkol pro správce
Zánik nároku na účet	Ano, úkol pro správce

2.12.2 HelpDesk

Koncový systém HelpDesk od firmy MiCoS Software s.r.o.:

- Slouží pro hlášení chyb všeho druhu, jak pro IT, tak i pro provozní oddělení.
- Obsahuje moduly HelpDesk, Evidence PC a Aktivity
- Samostatná aplikace nad MS SQL.
- Přístup mají všichni zaměstnanci a vybraní externí pracovníci s přiděleným loginem, s výjimkou pracovníků OZP Expres.
- Všichni zaměstnanci mají defaultně nastavenu roli Zadavatel.
- Řešitelé požadavků mají minimálně roli Řešitel.
- Pro autentizaci je používáno AD.
- Přihlášení do HelpDesku je realizováno pomocí SSO.
- Má vlastní databázi uživatelů.
- Má vlastní role management, ale navázaný na skupiny v AD
- Každá role v HD má svoji skupinu v AD.

Rozhraní k IdM:

- Databázový přístup nebo offline systém

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ne, SSO s AD
Řízení oprávnění	Ano, podle skupin AD
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je deaktivován

2.12.3 TIC

Koncový systém TIC je telefonní informační centrum:

- Telefonní informační centrum
- Aplikace pro interní Call centrum
- Uživatelé jsou vytvářeni automaticky, data se přebírají z AD.
- Role a práva jsou přiřazovány manuálně administrátorem aplikace, nepřebírají se z AD.
- Pro autentizaci je používáno AD.
- Přihlášení do aplikace je realizováno pomocí SSO.
- Má vlastní databázi uživatelů

Rozhraní k IdM:

- Offline aplikace

Prostředí:

- Produkční: Ano
- Testovací: Ano

- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ne, automaticky z AD
Aktualizace účtu	Ne
Změna loginu účtu	Ne
Změna hesla	Ne
Řízení oprávnění	Ano, úkol pro správce
Povolení/Zakázání účtu	Ne
Zánik nároku na účet	Ne

2.12.4 MS SQL server

Koncový systém MS SQL server je databázový systém:

- MS SQL se používá pro několik databází pro různé účely.
- MS SQL DB bude využívat i nový systém ICIS.
- DB pro reporting.
- DB pro KS a mzdy.
- Přístup je realizován hlavně technickými účty a technickými uživateli.
- Do některých DB mají přístup i obyčejní uživatelé a IT administrátoři.

Rozhraní k IdM:

- MS SQL konektor / DB konektor

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ano
Řízení oprávnění	Ano
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je deaktivován

2.12.5 Základní registry

Koncový systém Základní registry – systém třetí strany:

- Přístup má každé systemizované místo, které je potřebuje pro výkon práce.
- Jedná se hlavně o oddělení registrů a plateb, kde se ověřují informace o zákaznících.
- Přístup je realizován prostřednictvím ICIS, ICIS ale účty nevytváří.
- Pro přístup musí mít uživatel zřízeny certifikáty PostSignum – kvalifikovaný a komerční certifikáty.

Rozhraní k IdM:

- Offline aplikace

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano, úkol pro správce

Aktualizace účtu	Ano, úkol pro správce
Změna loginu účtu	Ano, úkol pro správce
Změna hesla	Ne
Řízení oprávnění	Ano, úkol pro správce
Povolení/Zakázání účtu	Ano, úkol pro správce
Zánik nároku na účet	Ano, úkol pro správce

2.12.6 Juno

Koncový systém Juno:

- ServiceDesk pro IT aplikace.
  - Obsahuje provozní deník.
- Nasazení v rámci testování ICIS.
- Krabicové řešení upravené pro potřeby Objednatele.
- Samostatná aplikace nad MySQL, případný přechod na PostGreSQL.

Rozhraní k IdM:

- Bude upřesněno v realizaci (dle analýzy), může být online/offline

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ano

Řízení oprávnění	Ano
Povolení/Zakázání účtu	Ano
;	Ano

2.12.7 KS

Personální systém KS:

- HR aplikace, mzdový a docházkový systém.
- Přístup mají všichni uživatelé, práva jsou nastavena podle systemizovaného místa.
- Všichni zaměstnanci mají právo nahlížet na svoje data.
- Zaměstnanci HR mají právo na správu mezd.
- IT administrátor má administrátorská práva k aplikaci s výjimkou správy mezd.
- Přístup do aplikace je dvojí.
- Přes intranet (KS portál) pro náhled na data zaměstnance, náhled na výplatní pásky a zadávání/schvalování dovolené.
- Pomocí aplikace (tlustý klient) pro správu HR dat a mezd a pro administraci systému.
- Má vlastní databázi uživatelů.
- Má vlastní role management.
- Systém KS bude výhledově nahrazen jiným HR systémem.
- Součástí KS systému je KS portál.

Rozhraní k IdM:

- Databázový přístup k tabulkám a pohledům (MS SQL Server)

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano

Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ano, výhledově přechod na AD SSO
Řízení oprávnění	Ano, přes AD skupiny
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Účet je deaktivován

2.12.8 Evidence 2000

Koncový systém Evidence 2000:

- Systém pro evidenci vstupních karet/čipů
- Obsahuje údaje o průchodech přes turnikety v budově.
- Obsahuje základní data o pracovnících (jméno, příjmení, osobní číslo, druh pracovního poměru a oddělení, kde pracuje).
- Každý zaměstnanec dostane vstupní čip
- Každý čip má unikátní číslo.
- Čip je přidělen na základě schválené žádosti v IdM.
- Pracovník čip přebere osobně nebo je čip předán na personální oddělení, které čip předá pracovníkovi.
    - V případě externistů, kteří nejsou v personálním systému, žádá o čip příslušný vedoucí oddělení, který čip posléze přebírá.
- Přístupy do budovy jsou nastaveny podle oddělení pracovníka

Rozhraní k IdM:

- Offline systém

Prostředí:

- Produkční: Ano
- Testovací: Ne
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak

Založení účtu	Ano, úkol pro správce
Aktualizace účtu	Ano, úkol pro správce
Změna loginu účtu	Ano, úkol pro správce
Změna hesla	Ne
Řízení oprávnění	Ano, úkol pro správce
Povolení/Zakázání účtu	Ano, úkol pro správce
Zánik nároku na účet	Ano, úkol pro správce

2.12.9 ČiSoft

Koncový systém ČiSoft:

- Obsahuje mapy pro Sanitky.
- Aplikace pro měření vzdáleností v km při převozech pacientů nebo cest pacientů do nemocnice.

Rozhraní k IdM:

- Offline rozhraní

Prostředí:

- Produkční: Ano
- Testovací: Ne
- Vývojové: Ne

Úroveň podpory operací s účtem:

Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano
Změna hesla	Ano

Řízení oprávnění	Ano
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Ano

*Scope se může změnit s ohledem na finální podobu systému ČiSoft.

2.12.10 OZP Express

Koncový systém OZP Express:

- Aplikace pro externí pracovníky OZP Expres i interní pracovníky OZP.
- Jde o zjednodušenou aplikaci pro jednoduchou správu klientských požadavků.
- Plánuje se nasazení v budoucnu, jako možný front-end pro obsluhu zákaznických požadavků.
- Zůstane zachována i po nasazení ICIS.
- Má vlastní databázi uživatelů
- Role a práva jsou přidělovány administrátorem aplikace OZP Expres.
- Zatím existuje jen jedna role.
- S nasazením na pobočky se plánuje více rolí a tím i napojení na IdM.

Rozhraní k IdM:

- Ano

Prostředí:

- Produkční: Ano
- Testovací: Ano
- Vývojové: Ne

Úroveň podpory operací s účtem:

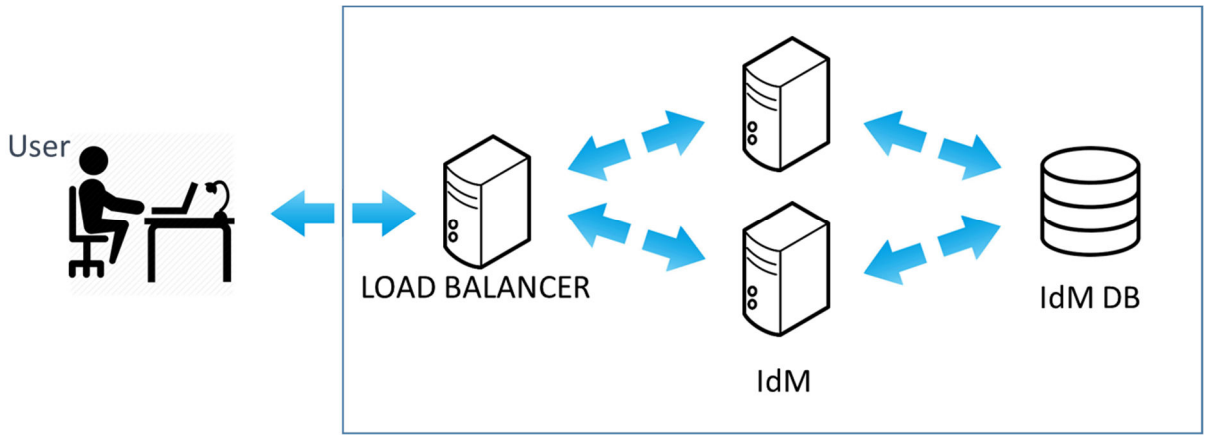
Operace s účtem	Podporováno? Případně jak
Založení účtu	Ano
Aktualizace účtu	Ano
Změna loginu účtu	Ano

Změna hesla	Ano
Řízení oprávnění	Ano
Povolení/Zakázání účtu	Ano
Zánik nároku na účet	Ano

2.13 VYSOKÁ DOSTUPNOST

Servery jsou provozovány ve virtualizovaném prostředí Objednatele.

Vysoká dostupnost je zajištěna zdvojením aplikačních serverů řešení a použitím virtuální IP adresy (VIP). Nabízené řešení vysoké dostupnosti je včetně dodávky vhodného Load balanceru.



Obrázek 2 Vysoká dostupnost IdM

Vysoká dostupnost je pro jednotlivá prostředí nasazena následovně:

- Produkční prostředí: load balancer + dva aplikační servery
- Testovací prostředí: load balancer + dva aplikační servery

Databázová vrstva nemá podporu vysoké dostupnosti na žádném prostředí.

3 ZABEZPEČENÍ PRIVILEGOVANÝCH ÚČTŮ

V rámci prostředí Objednatele je provozováno velké množství informačních a komunikačních systémů. Jednotlivé informační a komunikační systémy v sobě obsahují privilegované účty, které jsou využívány pro jejich správu, nebo se jedná o servisní účty aplikací nebo systémových služeb. Privilegované účty existují na všech vrstvách ICT – od operačních systémů, databází, komunikačních a bezpečnostních prvků až po uživatelské aplikace. Privilegované účty jsou využívány administrátory, kteří se podílejí na provozu a rozvoji informačních systémů a technologií. Jedná se jak o interní zaměstnance, tak o externí dodavatele. Privilegované účty představují významné bezpečnostní riziko pro každou organizaci, neboť:

- umožňují téměř neomezený přístup a manipulaci s informačními aktivy organizace. V případě kompromitace privilegovaného účtu je organizace vystavena velkému riziku neautorizovaného zneužití nebo vyzrazení kritických informačních aktiv,
- privilegované účty jsou v praxi často sdíleny mezi více administrátory, proto je obtížné určit odpovědnost za případné zneužití ze strany interního zaměstnance,
- hesla u privilegovaných účtů administrátorů a servisních účtů služeb a aplikací nejsou obvykle pravidelně měněna a často na ně není aplikována bezpečná politika hesel,
- je obtížné v reálném čase monitorovat nebo aktivně zasahovat do probíhajících relací u privilegovaných účtů v případě podezření na zneužití oprávnění

Z výše uvedených důvodů požaduje Objednatel komplexní řešení pro zabezpečení privilegovaných účtů a nahrávání privilegovaných relací. Cena uvedená v příloze č. 2 Smlouvy zahrnuje cenu za dodání, konfiguraci a implementaci všech vybraných zabezpečení privilegovaných účtů produktu v prostředí Objednatele.

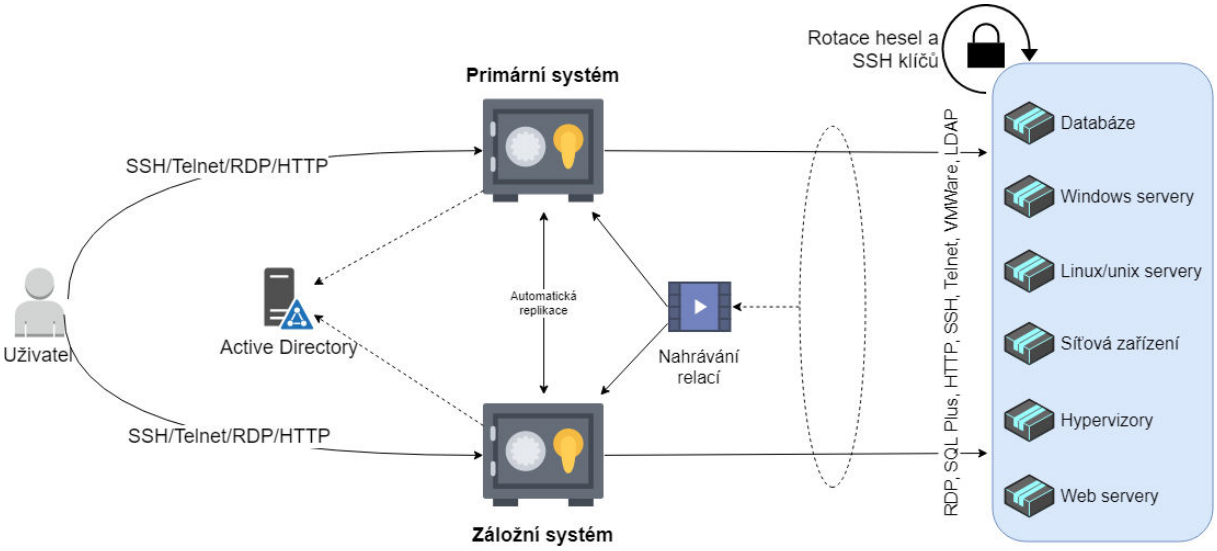
3.1 ZÁKLADNÍ POŽADAVKY NA ZABEZPEČENÍ PRIVILEGOVANÝCH ÚČTŮ

3.1.1 Obecné požadavky na poptávané řešení

Komplexním řešením zabezpečení privilegovaných účtů se rozumí hlavně:

- ochrana privilegovaných účtů, nahrávek a dalších citlivých dat v šifrovaném a zabezpečeném úložišti s mezinárodně uznávanou certifikací pro zabezpečení, např. FIPS 140-2, ISO/IEC 15408 nebo odpovídající

- centralizovaná správa privilegovaných účtů, hesel a SSH klíčů a automatická rotace hesel a SSH klíčů na koncových systémech na základě definovaných pravidel (časový interval, aktivita uživatele, detekce hrozeb) v řešení bez nutnosti instalovat na koncový systém softwarového agenta
- poskytnutí rozhraní pro umožnění bezpečného nakládání s hesly ve zdrojových kódech skriptů a aplikací, které zajišťuje nemožnost jejich zneužití
- zajištění přístupu pro uživatele na koncový systém prostřednictvím zvoleného privilegovaného účtu a protokolu skrze zabezpečený server včetně/bez možnosti zobrazit uživateli heslo k privilegovanému účtu
- poskytnutí grafického rozhraní pro administraci systému obsahující možnost řízení oprávnění uživatelů, nastavení pravidel pro rotaci hesel a jejich komplexnost, sledování událostí spojených s přístupem k privilegovaným účtům atp.
- nahrávání a živý monitoring vzdálených relací uživatelů včetně zaznamenávání metadat (typicky spuštěné programy, stlačené klávesy) s možností vyhledávání v zaznamenaných videonahrávkách skrze administrační rozhraní
- funkci automatického objevování nově vytvořených účtů a jejich případné automatické převzetí pod správu
- zachování kompletní a nezpochybnitelné auditní stopy
- průběžná analýza využívání privilegovaných účtů, vyhodnocování a odhalování potenciálně škodlivého chování uživatelů a zároveň odhalování útoků na zranitelnosti autentizačních protokolů NTLM a Kerberos typu Pass-the-hash, Golden Ticket atp.
- podpora ověření identity uživatele pomocí druhého faktoru



Obrázek 3 Architektura zabezpečení privilegovaných účtů

3.1.2 Specifické požadavky Objednatele

3.1.2.1 Možnosti přístupu

Požadavkem na produkt je minimální vliv na dosavadní styl práce administrátorů. Administrátor musí mít pro přihlášení ke koncovému systému možnost využít jak nativní prostředí produktu, tak stávající aplikace a protokoly pro přístup ke vzdáleným systémům. Pro vzdálený přístup k windows systémům je to minimálně RDP a pro vzdálený přístup k Linux/Unix systémům je to minimálně SSH. Administrátorům tedy musí zůstat možnost využití těchto protokolů přímo z jejich pracovních stanic.

3.1.2.2 Vysoká dostupnost – HA

Produkt bude součástí kritické infrastruktury Objednatele, proto je požadavek v produkčním prostředí na jeho vysokou dostupnost. Řešení vysoké dostupnosti musí být plně automatické a nesmí tak vyžadovat ruční zásah operátora dohledového centra nebo bezpečnostního správce. Zároveň nesmí obsahovat tzv. single-point-of-failure, tzn. součást, která při vadě způsobí dlouhodobou nefunkčnost celého systému.

Součástí nabízeného řešení je dodávka, implementace a konfigurace load-balanceru.

Produkt bude implementován i v testovacím prostředí, kde ale není požadavek na jeho vysokou dostupnost.

3.1.2.3 Dvoufaktorová autentizace – 2FA

Ve stávajícím prostředí Objednatele je provozováno přihlašování pomocí druhého faktoru metodou Čipová karta ProID+Q . Požadavkem na produkt je integrovaná podpora tohoto systému.

3.1.2.4 Adresářové služby

Produkt bude provozován v prostředí MS Active Directory, požadavkem na produkt je tedy možnost autentizovat a autorizovat administrátory vůči AD a zároveň na administrátory aplikovat pravidla na základě jejich členství v příslušných uživatelských skupinách.

3.1.2.5 LOGmanager

V prostředí Objednatele je provozován systém na centrální správu a analýzu událostí LOGmanager (logmanager.cz) Součástí dodávky bude napojení Produktu na tento systém – události z Produktu tedy budou zaznamenávány jak interně, tak v systému LOGmanager.

3.1.2.6 HSM

V prostředí Objednatele bude provozován síťový HSM modul. Produkt musí být schopen využít Objednatelův HSM modul k ukládání (jednoho, nebo více) šifrovacích klíčů, kterými jsou zabezpečeny informace v úložišti Produktu.

3.1.2.7 Skripty

Součástí produktu bude nástroj umožňující bezpečné nakládání s hesly ve zdrojových kódech skriptů a aplikacích, kterým pomocí rozhraní poskytne přístup k těmto údajům a eliminuje nutnost mít přístupové údaje napevno zadané ať už v těle aplikace, nebo v jiných konfiguračních souborech.

Dodavatel poskytne zaškolení Objednateli formou asistované úpravy 10 vybraných skriptů včetně prokázání, že identifikátory použité pro získání přihlašovacích údajů nebudou v jiném skriptu funkční (platí i pro skripty spouštěné na témže operačním systému). Skripty na dalších systémech budou svépomocí upravovat zaškolení administrátoři Objednatele.

3.1.2.8 Parametry řešení

Řešení zabezpečení privilegovaných účtů musí být naceněno pro spuštění s následujícími parametry:

Privilegovaní uživatelé / privilegované identity v infrastruktuře	**Aktuální stav**	**Celkový plánovaný stav**
Počet administrátorů (správců + externistů)	25	65
Počet privilegovaných účtů na koncových systémech	100	120

Koncový systém / služba / zařízení	**Aktuální počet**	**Celkový plánovaný počet**
Linux RHEL 6/7	29	60
Windows Server 2008/12/16	102	150
Microsoft SQL Server 2016	16	25
VMware ESXi / vSphere	9	15
ERP icis	0	1
Firewall	4	8
Aktivní prvky	35	50
Aplikace/skripty ** využívající privilegované účty k přístupu k lokálním i vzdáleným službám nebo systémům	10	500

** tyto skripty jsou spouštěny ručně nebo automaticky na následujícím počtu operačních systémů	50	50

Produkt musí podporovat výše uvedené prostředí a zároveň musí být výkonově dimenzován na variantu celkového plánovaného (budoucího) stavu a Objednatel tak nebude akceptovat požadavky na změnu architektury. Cena dle přílohy č. 2 Smlouvy je stanovena jednak ve výši pro aktuální stav. Dále je uvedena částka tzv. inkrementálního nárůstu cen licencí pro případ navýšení počtu uživatelů, účtů, služeb, zařízení či systémů. V případě snížení počtu uživatelů, účtů, služeb, zařízení či systémů dojde k tzv. inkrementálnímu snížení cen licencí, a to za podmínek dle čl. 5.1.12 Smlouvy.

4 PRAVIDELNÁ AUDITNÍ ZPRÁVA

V rámci procesu kontinuální kontroly a zlepšování zabezpečení bude prováděn audit prostředí, a to 1x za 6 měsíců ve formě pravidelné auditní zprávy. Pravidelná auditní zpráva bude věcně navazovat na Počáteční analýzu ve smyslu čl. 1.2.1 této přílohy č. 1 a na předchozí pravidelnou auditní zprávu. Cena pravidelné auditní zprávy bude hrazena vždy po její akceptaci bez výhrad.

5 ÚPRAVA SMĚRNIC

Interní směrnice měněné v rámci realizace Identity Managementu bude upravovat metodik IdM. Objednatel předpokládá potřebnou spolupráci metodika IdM v rozsahu 240 člověkohodin za dobu účinnosti Smlouvy. Tato činnost bude hrazena v rozsahu skutečně poskytnutých služeb.

6 TECHNICKÁ PODPORA A ROZVOJ

Spolehlivý provoz řešení je zajištěn službou technické podpory, která zajistí garanci základních servisních parametrů. Jejím cílem je zajistit co nejrychlejší obnovení dostupnosti služby a současně minimalizovat důsledky jejího výpadku na Objednatele a uživatele spravované aplikace.

6.1 SLA, REAKČNÍ DOBY PŘI NEFUNKČNOSTI

Technická podpora je poskytována dle parametrů uvedených níže. Součástí technické podpory jsou následující položky:

- garance reakční doby a řešení incidentů
- hlášení požadavků v helpdesku/telefonicky
- pravidelný měsíční report řešených incidentů

Technická podpora zahrnuje podporu produktu výrobcem i servisní podporu, cena za tyto podpory je společná.

6.1.1 Kategorie závady

A. IdM nebo jeho část/služba není použitelná ve svých základních funkcích a parametrech nebo se vyskytuje funkční závada znemožňující činnost a řádné užití IdM nebo jeho části/služby. Tento stav ohrožuje nebo znemožňuje běžný provoz IdM, případně může Objednateli nebo dalším subjektům způsobit větší finanční nebo jiné škody. Tento stav může ohrozit běžný provoz Objednatele a nelze jej dočasně řešit organizačním opatřením.
B. Funkčnost IdM nebo jeho části/služby nebo rozsah služeb Objednatele je ve svých funkcích a parametrech degradována tak, že tento stav omezuje běžný provoz IdM nebo omezuje řádné užití IdM nebo jeho části/služby a nebo služeb Objednatele. Existuje náhradní pracovní postup (work-around) pro obejití závady, případně organizační opatření.
C. Ostatní – drobné závady, které nespadají do kategorie A a/nebo B.
D. Požadavek na změnu nebo rozšíření vlastností oproti zadání.

Zařazení vady do jednotlivých kategorií určuje Objednatel.

6.1.2 Režim podpory IdM

Režim podpory řešení Identity Manager:

- 5x8, tj. v pracovní době 9:00 – 17:00 v pracovních dnech (dále jen „provozní doba“).

Parametry SLA:

Kategorie vady	Reakční lhůty	Doba odstranění vady na produkčním prostředí

	v pracovní době	
A - Vysoká	4 hodiny	Do 48 hodin
B - Střední	8 hodin	Do 5 pracovních dní
C - Nízká	16 hodin	Do 30 kalendářních dnů

Reakční lhůtou se rozumí doba od zahájení požadavku do doby potvrzení zahájení jeho řešení. Reakční lhůta běží pouze v pracovní době.

6.1.3 Režim podpory zabezpečení privilegovaných účtů

Režim podpory zabezpečení privilegovaných účtů:

- 7x12, tj. v pondělí až neděle 6:00 – 18:00 (dále jen „provozní doba“).

Parametry SLA:

Kategorie vady	Reakční lhůty v pracovní době	Doba odstranění vada na produkčním prostředí
A - Vysoká	2 hodiny	Do 24 hodin
B - Střední	4 hodin	Do 48 hodin
C - Nízká	16 hodin	Do 15 kalendářních dnů

Reakční lhůtou se rozumí doba od zahájení požadavku do doby potvrzení zahájení jeho řešení. Reakční lhůta běží pouze v provozní době.

6.1.4 Hlášení požadavků

Primárním komunikačním kanálem je helpdesk/service desk Objednatele. Zároveň Dodavatel zajistí telefonickou hotline v provozní době dle odst. 6.1.2 a 6.1.3. Všechny požadavky zadané přes hotline budou zadané Dodavatelem do service desku Objednatele (Objednatel je však oprávněn zadávat požadavky, např. v případě výpadku helpdesk/service desk).

6.2 ROZVOJ, ZMĚNOVÉ POŽADAVKY, KONZULTACE

Dodavatel poskytne služby svých expertů pro rozšiřování implementovaných funkcionalit nebo při konzultaci k řešení.

Čerpání bude oboustranně evidováno a odsouhlasováno. Doby vyřešení těchto požadavků budou vždy stanoveny po vzájemné dohodě.

V průběhu produkčního běhu díla je Objednatel oprávněn poptávat konzultace IDM metodika / procesního analytika na specifikaci procesních a metodických změn. Činnost IdM metodika je hrazena dle toho článku pouze v případě, že se nejedná o činnost dle čl. 1.5.4.1 této přílohy č. 1.

Rozvoj, změnové požadavky a konzultace bude hrazeny v rozsahu skutečně poskytnutých služeb, Předpokládaný rozsah těchto služeb je **150 hodin** / **měsíc**; Objednatel však může objednat větší, menší nebo žádný rozsah těchto služeb měsíčně.

7 TECHNICKÉ PROSTŘEDKY

V souladu se zadávacími podmínkami veřejné zakázky je Dodavatel oprávněn využít stávající architekturu Objednatele (licenční zajištění této infrastruktury dodá Objednatel) níže uvedenou v tomto článku Smlouvy. Pokud pro plnění předmětu Smlouvy dle nabídky Dodavatele nebyl HW a SW nabízený Objednatelem dostatečný, je součástí předmětu plnění i dodávka HW a SW v souladu s nabídkou Dodavatele a přílohou č. 2 Smlouvy. Dodavatel garantuje funkčnost řešení s jím dodaným HW a SW. Pokud Dodavatel při plnění Smlouvy nevyužije HW nebo SW jím nabídnutý nebo jejich část (např. v případě zjištění, že k plnění postačuje stávající architektura Objednatele dále v tomto článku uvedené nebo Objednatelem samostatně obstaraná), nemá nárok na úhradu ceny za toto neodebrané plnění.

Stávající architektura Objednatele je tato:

- VM WARE, vSAN virtualizace prostředí Windows i Linux

Licenční zajištění:

- Windows Server 2016 Standard a vyšší
- Microsoft SQL Server 2016/2018 a vyšší

Vypsat konfiguraci HW, které Objednatel dává k dispozici (pro informaci uvádíme naše požadavky)

IdM (v režimu vysoké dostupnosti variantně, základní požadavek je IDM bez HA)
Minimální hodnoty poskytovaných virtuálních serverů

	Vývoj		Test		Produkce	
	Aplikace	Databáze	Aplikace	Databáze	Aplikace	Databáze
Počet virtuálních serverů	1	1	2	1	2	1
CPU [jádra]	4	4	4	4	4	4
RAM [GB]	8	8	8	16	8	16
HDD [GB]	100	100	100	200	100	200

PAM (v režimu vysoké dostupnosti)

- 2x fyzický server pro trezory: 4core CPU, 32GB RAM, 2x1TB HDD (RAID1), 2x1Gbit NET
- 2x virtuální server pro ostatní komponenty: 16core CPU, 64GB RAM, 2x1TB SSD (RAID1), 2x1Gbit NET

8 SLOVNÍK

Kapitola popisuje zkratky použitá v rámci dokumentu a také terminologické pojmy.

8.1 POUŽITÉ ZKRATKY

Slovník zkratek použitých v tomto dokumentu:

- Administrátor – Interní zaměstnanec nebo externí dodavatel, který využívá privilegované účty pro správu koncových zařízení
- Bezpečnostní správce – Bezpečnostní správce dodaného řešení ochrany privilegovaných účtů, který má na starosti jeho správu a konfiguraci
- Dodavatel / Zhotovitel – Subjekt, který se v rámci tohoto výběrového řízení uchází o dodávku řešení IdM a zabezpečení privilegovaných účtů. Dodavatel, který bude vybrán, se stane Zhotovitelem.
- GUI (Graphical User Interface) – grafické uživatelské rozhraní.
- HA – Režim vysoké dostupnosti (High Availability)
- HW – Hardware
- ICT – Informační a komunikační technologie
- Koncový systém – Systém, jehož privilegované účty a relace budou řízeny pomocí Produktu (např. databáze, aplikace, komunikační a bezpečnostní prvky atd.)
- KS – personální systém, zdroj identit pro zaměstnance.
- LDAP – systém kompatibilní s LDAP protokolem (Lightweight Directory Access Protocol).
- MS AD – Microsoft Active Directory
- MTBF – Mean Time Between Failures - střední doba mezi poruchami
- RDP – Remote Desktop Protocol (zkratka RDP) je v informatice proprietární síťový protokol, který umožňuje uživateli využívat ovládat vzdálený počítač prostřednictvím grafického uživatelského prostředí, které je spuštěno na vzdáleném počítači.
- SSH – Zabezpečený komunikační protokol
- SW – Software
- VNC – Virtual Network Computing je grafický program, který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní pomocí počítačové sítě.
- ZoKB – zákon o Kybernetické bezpečnosti.

8.2 TERMINOLOGICKÉ POJMY

8.2.1 ACCESS MANAGEMENT

Systém či služba, která zprostředkovává autentizaci vůči autentizačním zdrojům, např. *MS AD, LDAP*. Je možné definovat podmínky autentizace na základě zjištěných parametrů během procesu autentizace, např. *vynucení dvou-faktorové autentizace na základě lokality či domény uživatele*.

8.2.2 ARCHIVACE

Finální fáze životního cyklu objektu (identity, role, vazby identita-role, organizace). V tomto stavu je objekt „zaparkovaný“, není „živý“. Hlavní důvod archivace je audit.

8.2.3 ATRIBUT IDENTITY

Vlastnost svázaná s určitou osobou. Např. *telefonní číslo, adresa trvalého bydliště, e-mailová adresa apod.*

8.2.4 AUTENTIZACE

Ověření uživatele pomocí přihlašovacích údajů, typicky jména a hesla.

8.2.5 AUTORITATIVNÍ ZDROJ

Systémové úložiště (případně systém), které slouží jako zdroj informací o definovaných atributech identity. Rozdílné atributy identity mohou mít rozdílné autoritativní zdroje. Příklad: *personální systém je autoritativním zdrojem pro osobní informace o zaměstnanci.*

8.2.6 AUTORIZACE

Bezpečnostní mechanismus, který povoluje nebo odpírá práva ke zdrojům, jako jsou aplikace, soubory a data.

8.2.7 AUTORIZAČNÍ AUDIT

Report s přehledem všech uživatelů a jim přiřazených rolí. Používá se zejména při kontrole oprávnění.

8.2.8 BLACKLIST

Blacklist (černá listina) nebo též blocklist je v informatice označení pro seznam obvykle osob nebo účtů, kterým zakazujeme vybranou činnost.

8.2.9 BUSINESS PROCESS MANAGEMENT

Procesní řízení neboli Business Process Management (BPM) je soubor činností, které se týkají plánování a sledování výkonnosti realizačních firemních procesů. Využívá znalostí, zkušeností, dovedností, nástrojů, technik a systémů k tomu, aby definoval, vizualizoval, měřil, kontroloval, a reportoval stav firemních procesů za účelem jejich optimalizace. .

8.2.10 CAPTCHA

CAPTCHA je Turingův test, který se používá ve snaze automaticky odlišit skutečné uživatele od robotů. CAPTCHA je akronym pro „completely automated public Turing test to tell computers and humans apart“, tedy „plně automatický veřejný Turingův test k odlišení počítačů a lidí“.

8.2.11 CROSS-SITE REQUEST FORGERY (CSRF)

Cross-site Request Forgery (CSRF nebo také XSRF) metoda útoku do internetových aplikací pracující na bázi nezamýšleného požadavku pro vykonání určité akce v této aplikaci, který pochází z nelegitimního zdroje. Obvykle nejde o útok směřující k získání přístupu do aplikace. Většinou zneužívá akce uživatelů, kteří jsou k ní v okamžiku útoku přihlášeni.

8.2.12 DELEGACE

Princip delegace přiděluje definované sady činností jinému uživateli. Tím se z něj stává pověřená osoba pro danou oblast. Delegovat je možné buď funkčnosti, např. *právo resetovat hesla, právo zakládat uživatele, právo přiřadit uživateli roli* nebo rozsah práv např. *právo spravovat uživatele nad určitou organizací*.

8.2.13 DISCOVERY

Mechanismus Discovery se používá pro objevování nových účtů. Principem je rozpoznání, že v rozhodném připojeném systému vznikl nový účet a jeho propagace do IdM nástroje.

8.2.14 ENTITA

V prostředí IdM entitou míníme buď osobu ve vztahu k informačnímu systému, nebo organizační jednotku nebo objekt oprávnění.

8.2.15 ESKALACE

Eskalace je sada akcí, které se provedou, pokud očekávaný výsledek nebyl dosažen v nastaveném časovém úseku. Např. *v případě, kdy schvalovatel neprovede včas rozhodnutí o žádosti (schváleni nebo zamítnutí).* Příkladem akcí jsou *připomenutí emailem, postoupení na nadřízeného pracovníka nebo automatické schválení/zamítnutí žádosti*.

8.2.16 HASH

Hashovací (hešovací) funkce je funkce, která určitým složitým matematickým postupem převede vstupní data (text, obrázek nebo jiný soubor) do speciálního čísla. Toto číslo se nazývá HASH nebo otisk. Je to tzv "kontrolní součet". Hash se používá k porovnávání dat bez nutnosti znát jejich obsah. Běžně se hash používá pro bezpečné ukládání hesel.

8.2.17 IDENTITA

Identitou se rozumí jednotka, která reprezentuje konkrétního fyzického uživatele, pro vyloučení pochybností. Pokud má jeden uživatel více účtů v systému, jedná se stále o jednu identitu.

8.2.18 IDENTITY MANAGEMENT, SPRÁVA IDENTIT

Identity Management je informační systém, který spravuje životní cyklus uživatelů, definuje přístupy uživatelů a jejich rolí v koncových systémech.

8.2.19 KONCOVÝ SYSTÉM

Jedná se o systémy, aplikace či databáze, které obsahují samostatné úložiště uživatelských účtů či jiných objektů. Koncový systém je samostatnou aplikací, která je provozně nezávislá na IdM systému, např. *účetní systém napojený k IdM*.

8.2.20 KORELACE, KORELAČNÍ PRAVIDLO

Korelace znamená vzájemný vztah mezi dvěma procesy nebo veličinami. Pokud se jedna z nich mění, mění se i druhá a naopak.

8.2.21 LOGIN

Přihlašovací jméno uživatele do aplikace.

8.2.22 MANAŽER

Nadřízená identita, jedná se buď o vedoucího pro zaměstnance, nebo o manažera pro ostatní identity (externista, technický účet). Pro externistu se jedná o oprávněnou osobu uvedenou ve Smlouvě.

8.2.23 OFFLINE ÚTOK NA HESLA

Útok hrubou silou proti datům získaným z DB IDM (brute-force, slovník a podobně).

8.2.24 PARAMETRICKÉ ROLE (HYBRIDNÍ RBAC).

Business role může mít proměnné složení (vazbu na aplikační role) podle atributu uživatele, kterému je role přiřazena. Příkladem je *role pro referenta na pobočce, která je jedna, a pobočka je parametr této role*.

8.2.25 PLNÁ PROJEKCE IDENTIT

Plná projekce identit na koncové systémy je mechanismus, díky kterému má IdM systém plný dohled nad účty. Nadbytečné účty odstraňuje, chybějící zakládá, udržuje konzistenci mezi přidělenými rolemi a stavem koncového systému. Prerekvizitou je pokročilý stupeň zavedení IdM systému.

8.2.26 PRIVILEGOVANÝ ÚČET

Jedná se o uživatelský účet, který má přiděleno vyšší oprávnění, než kterým disponuje běžný uživatel. Může se např. jednat o oprávnění na instalaci software, úpravy nastavení systému či aplikací, změnu konfigurace síťových zařízení atp.

8.2.27 PROVISIONING

Provisioning zajišťuje řízení životního cyklu, uživatelských účtů či jiných objektů v koncových systémech pomocí konektorů, např. *vznik, editaci, zneplatnění apod*. Tato akce je vyvolána z IdM systému.

8.2.28 RBAC, ROLE-BASED ACCESS CONTROL

Model, který uživateli přiřazuje role, které mu dávají určitý stupeň přístupu ke zdroji. Přiřazení role garantuje uživateli definovanou sadu nároků na oprávnění, které jsou přiřazeny buď automaticky, nebo po splnění určité podmínky, nebo na základě schválení odpovědnými osobami.

8.2.29 RECERTIFIKACE

Proces znovuspuštění schvalovacích workflow nad skupinou oprávnění za účelem potvrzení aktuálnosti a oprávněnosti těchto oprávnění.

8.2.30 REKONCILIACE

Rekonciliací se rozumí porovnání schváleného stavu v IdM systému se skutečným stavem na koncovém systému. Výstupem je automatické narovnání případných nesrovnalostí, tzn. úprava stavu v koncovém systému dle schváleného stavu v IdM.

8.2.31 RESET HESLA

Proces, kterým si uživatel mění vlastní heslo obvykle samoobslužným procesem prostřednictvím formuláře v prohlížeči. Cílem je redukovat čas, který věnují IT administrátoři odpovídáním na žádosti o podporu. .

8.2.32 ROLE, BUSINESS ROLE

Samostatná entita, která nese oprávnění do aplikace nebo označuje skupinu uživatelů, pokud skupina definuje uživatele s úmyslem zajistit jim stejnou sadu privilegií. Role je základ autorizace v moderních informačních systémech.

V případě business role se jedná o nadřazenou roli, která může obsahovat N rolí v M úrovních.

8.2.33 SKUPINA, GROUP

Softwarově vytvořená skupina, která umožňuje společnou správu obsahujících identit nebo účtů. Skupiny se používají například na definici rolí a jiných příslušností. Skupiny zjednodušují řízení přístupu. Např. *seznam e-mailových adres v rámci jednoho newsletteru, seznam lidí, kteří smějí vstoupit do budovy*.

8.2.34 SOD

Segregation of Duties je typ omezujícího pravidla, které zamezuje nebo upozorňuje na kumulaci definovaných rolí u jednoho uživatele.

8.2.35 SSO, SINGLE SIGN-ON

SSO je služba, která uživatelům zajišťuje automatické přihlášení do aplikací bez nutnosti zadávat přihlašovací údaje do zvolené aplikace.

Jedná se o zprostředkovatele přihlášení, který předává jednotlivým aplikacím informaci o úspěšně provedeném ověření vůči definovanému úložišti. V tomto modelu uživatel používá pouze jednu sadu přihlašovacích údajů, nemusí si pamatovat heslo do každé aplikace zvlášť.

8.2.36 WHITELIST

Whitelist (bílá listina) je v informatice označení pro seznam obvykle osob nebo účtů, kterým povolujeme vybranou činnost.

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

Veřejné zakázky „Identity Management – realizace“

Příloha č. 8 - Vzor smlouvy o dílo a o poskytování služeb

Příloha č. 5 – Smlouva o zpracování osobních údajů

Smlouva o zpracování osobních údajů

Tato Smlouva o zpracování osobních údajů, (dále jen „**Smlouva**“), se uzavírá mezi následujícími smluvními stranami:

(1) **Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví**, se sídlem Praha 4, Roškotova 1225/1, PSČ 140 00, IČO: 471 14 321, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl A, vložka 7232, zastoupená panem Ing. Radovanem Kouřilem, generálním ředitelem, (dále jen „**Správce**"), na straně jedné;

a

(2) **[DOPLNÍ DODAVATEL],** se sídlem: [DOPLNÍ DODAVATEL], IČO: [DOPLNÍ DODAVATEL], zápis v OR: [DOPLNÍ DODAVATEL], zastoupen: [DOPLNÍ DODAVATEL], (dále jen „**Zpracovatel**"), na straně druhé;

(Správce a Zpracovatel jsou dále označováni společně též jako „**Smluvní strany**” a každá jednotlivě jako „**Smluvní strana**”).

PREAMBULE

Vzhledem k tomu, že:

(A) Správce je zadavatelem a Zpracovatel je vybraným dodavatelem Veřejné zakázky s názvem „Identity Management – realizace“, ev. č. VZ: [●] (dále jen „**Veřejná zakázka**“).

(B) V rámci plnění předmětu Veřejné zakázky bude docházet k dodání díla a poskytování služeb sjednaných ve Smlouvě o dílo a o poskytování služeb „Identity Management – realizace“ uzavřené mezi Správcem a Zpracovatelem (dále jen „**Smlouva o dílo**“ a „**Služby**“[1]).

(C) Zpracovatel v souvislosti s poskytováním Služeb Správci dle Smlouvy o dílo bude zpracovávat na základě pokynů Správce osobní údaje pojištěnců (klientů) Správce, kteří jsou fyzickými osobami (dále jen „**Subjekty údajů**“).

(D) Strany si přejí upravit vzájemná práva a povinnosti při poskytování Služeb tak, aby zpracování osobních údajů probíhalo v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Nařízení“) a s obecně závaznými předpisy České republiky.

Proto nyní Smluvní strany ujednaly následující:

[1] Je-li v této Smlouvě používán pojem „Služby“, rozumí se tím veškeré plnění předmětu Smlouvy o dílo, tj. dodání díla a s ním související činnosti.

1. PŘEDMĚT SMLOUVY

Předmětem této Smlouvy je úprava vzájemných práv a povinností Smluvních stran při Zpracování osobních údajů, se kterými Zpracovatel může nakládat v souvislosti s poskytováním Služeb. Smluvní strany tímto konstatují, že může nastat situace, kdy Zpracovatel bude pro Správce formou nahodilého nahlédnutí na data provádět Zpracování osobních údajů, které jsou definovány níže v článku 2 této Smlouvy, výhradně za účelem zajištění poskytování Služeb, (dále také jen „**Účel**").

Smluvní strany se tímto dohodly, že Zpracovatel bude pro Správce provádět Zpracování osobních údajů, které jsou definovány níže v článku 2 této Smlouvy, výhradně za uvedeným Účelem, způsobem a na základě doložených pokynů a podmínek Správce a v souladu s nimi tak, jak vyplývají z této Smlouvy a Smlouvy o dílo.

2. ROZSAH ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ

2.1 Zpracovavatel bude pro Správce provádět Zpracování osobních údajů následujících subjektů osobních údajů:

- zaměstnanci Správce,
- pojištěnci Správce,
- poskytovatelé zdravotní péče Správce,
- fyzické osoby bez vztahu ke Správci.

(dále jen jako „**Subjekty osobních údajů**“).

2.2 Zpracovavatel bude u Subjektů osobních údajů pro Správce provádět Zpracování následujících osobních údajů:

- identifikační údaje Subjektů osobních údajů (zejména titul, jméno a příjmení, datum narození),
- adresní údaje Subjektů osobních údajů (zejména adresa trvalého pobytu, doručovací adresa),
- elektronické údaje Subjektů osobních údajů (zejména e-mail),
- identifikační údaje Subjektů osobních údajů vydané státem (rodné číslo, DIČ),

(dále společně jen jako „**Osobní údaje“**).

2.3 Zpracovatel bude provádět Zpracování na serverech umístěných v sídle Správce prostřednictvím vzdáleného přístupu zabezpečeného Správcem.

2.4 Pokud bude Zpracovatel provádět Zpracování na základě výslovného pokynu Správce, které tato Smlouva v bodě 2.2 výslovně neuvádí, bude provádět Zpracování těchto nových osobních údajů za stejných podmínek.

3. DOBA ZPRACOVÁNÍ

3.1 Tato Smlouva se uzavírá na dobu trvání Smlouvy o dílo.

4. PROHLÁŠENÍ SPRÁVCE A NAVAZUJÍCÍ ZABEZPEČENÍ ZPRACOVATELE

4.1 Správce prohlašuje, že s Osobními údaji nakládá plně v souladu s Nařízením. Zpracovatel se zavazuje přijmout přiměřená relevantní technická a organizační opatření k zajištění odpovídající bezpečnosti Osobních údajů při jejich Zpracování a k zamezení nahodilého nebo neoprávněného přístupu k Osobním údajům, jejich pozměňování, zničení nebo ztrátě, neoprávněnému přenosu nebo jinému neoprávněnému zpřístupnění nebo zpracování předávaných Osobních údajů. Pro tyto účely Zpracovatel přijme technická a organizační opatření ujednaná v Příloze č. 1 této Smlouvy.

4.2 Zpracovatel je povinen poskytnout svým zaměstnancům a ostatnímu personálu, který se podílí na Zpracování, přiměřené pokyny pro jejich Zpracování, zejména povinnost dodržovat mlčenlivost ve vztahu ke všem Osobním údajům nebo důvěrným informacím, u kterých prování Zpracování na základě této Smlouvy a/nebo Smlouvy o dílo, a dále poskytnout svým zaměstnancům a ostatnímu personálu dostatečné pokyny k technickým a organizačním bezpečnostním opatřením přijatým pro ochranu a zabezpečení Osobních údajů.

4.3 Zpracovatel je povinen zavázat dohodou o mlčenlivosti své zaměstnance a ostatní personál, který se podílí na Zpracování, aby dodržovali povinnost mlčenlivosti ve vztahu ke všem Osobním údajům nebo důvěrným informacím, jako i k dodržování relevantních požadavků a norem Zpracovatele, v souvislosti s poskytováním Služeb Zpracovatele za účelem Zpracování pro Správce na základě této Smlouvy. Nedodržení zásad podle tohoto odstavce Smlouvy, norem nebo požadavků opravňuje Správce k jednostranné výpovědi této Smlouvy ke dni zjištění porušení povinnosti Zpracovatele. Správce může požádat Zpracovatele o předložení důkazů k ověření výše uvedených skutečností.

5. POVINNOSTI ZPRACOVATELE

5.1 Zpracovatel se zavazuje provádět Zpracování v souladu s platnými a účinnými právními předpisy.

5.2 Zpracovatel má povinnost poskytnout Správci přiměřenou požadovanou součinnost při plnění Účelu této Smlouvy, ochraně Osobních údajů před jakýmkoli zneužitím nebo neoprávněným přístupem a dodržováním příslušných právních předpisů při provádění Zpracování Osobních údajů.

5.3 Za účelem plnění této Smlouvy podle Nařízení poskytne Zpracovatel Správci bez zbytečného odkladu přiměřenou součinnost k usnadnění povinností Správce při zpracování Osobních údajů podle platných a účinných právních předpisů včetně, nikoliv však výlučně:

5.3.1 při přijímání vhodných technických a organizačních opatření k zajištění úrovně bezpečnosti odpovídající možným rizikům při Zpracování Osobních údajů podle této Smlouvy.

V případě, že Správce požaduje spolupráci nebo součinnost podle tohoto odstavce, je Správce povinen písemně oznámit Zpracovateli veškeré své požadavky k součinnosti nebo spolupráci a doložit je přesnými pokyny v souladu s Nařízením při Zpracování. V případě, že by součinnost při Zpracování vyžadovala úkony nad rámec Nařízení při Zpracování, Zpracovatel poskytne takovou součinnost za úplatu, která bude sjednána dohodou smluvních stran.

5.4 Zpracovatel je povinen provádět Zpracování pouze v rozsahu, po dobu a k Účelu stanovenému touto Smlouvou, nebo na základě písemných pokynů Správce. Tam, kde by písemné pokyny Správce byly nad rámec požadavků stanovených Nařízením při Zpracování, součinnost Zpracovatele bude poskytnuta za úplatu určenou dohodou smluvních stran.

5.5 Zpracovatel se zavazuje, že neposkytne Osobní údaje třetí straně, a to ani pro nekomerční účely, vyjma případů, kdy takové poskytnutí vyžadují platné a účinné právní předpisy nebo Správce dal předem k poskytnutí výslovný písemný souhlas.

5.6 Zpracovatel je povinen umožnit Správci během běžné pracovní doby Zpracovatele provést v sídle Zpracovatele kontrolu dodržování povinností týkajících se provádění Zpracování vyplývajících z této Smlouvy a Nařízení (zejména článku 28 a 32 Nařízení). Správce písemně oznámí Zpracovateli provedení kontroly podle tohoto odstavce nejpozději 5 dnů před jejím provedením. Zpracovatel následně zpřístupní Správci přiměřené informace k doložení plnění svých povinností podle této Smlouvy a poskytne Správci přiměřený přístup ke všem prostorům, zařízením a záznamům, které umožní Správci provedení ověřovací kontroly s přiměřeným dohledem předem určeného zástupce Zpracovatele, který bude zodpovědný, aby byla kontrola prováděna v rozsahu a v souladu s podmínkami této Smlouvy a Smlouvy o dílo.

5.7 Zpracovatel se zavazuje, že bude řádně a bez zbytečného prodlení odpovídat na veškeré relevantní dotazy ze strany Správce a Úřadu pro ochranu osobních údajů ohledně jakéhokoli Narušení bezpečnosti způsobeného Zpracovatelem, jak je definováno v článku 6.1 této Smlouvy, nebo jakéhokoli jiného aspektu Zpracování nebo ochrany osobních údajů. Zpracovatel má povinnost notifikovat Správce do 24 hodin od obdržení jakéhokoli předvolání, soudního příkazu nebo správního příkazu vládním nebo správním orgánem, který požaduje přístup k Osobním údajům nebo jejich zveřejnění. V takových případech má Zpracovatel povinnost umožnit Správci, aby Správce na vlastní náklady provedl ochranné opatření proti předvolání, soudnímu příkazu nebo správnímu příkazu, přičemž Zpracovatel poskytne Správci odpovídající potřebnou součinnost.

5.8 Zpracovatel neprodleně notifikuje Správce o jakýchkoli překážkách při plnění této Smlouvy a o veškerých okolnostech týkajících se závažného porušení povinností Zpracovatele ohledně Zpracování a ochrany Osobních údajů stanovenými touto Smlouvou. Zpracovatel je dále povinen neprodleně poskytnout Správci přiměřenou součinnost k odstranění překážek a/nebo případnému zabránění nebo nápravě porušení povinností Zpracovatele.

5.9 Správce se zavazuje upravovat data, která bude případně předávat Zpracovateli pro potřeby dalšího vývoje a testování systému SAFE Správce, procesem pseudonymizace, resp. anonymizace, takovým způsobem, aby předmětná data neobsahovala žádné

Osobní údaje. Smluvní strany sjednávají, že se nejpozději do uskutečnění prvního takového předání předmětných dat po nabytí účinnosti Smlouvy dohodnou na nastavení procesu pseudonymizace, resp. anonymizace předávaných dat a jeho protokolování.

5.10 Po ukončení práce s předanými daty podle předchozího odstavce této Smlouvy je Zpracovatel povinen poskytnout Správci všechna zařízení obsahující taková předaná data, pokud je to možné, a vymazat všechna taková předaná data ze všech svých systémů nebo databází, včetně vymazání všech záložních kopií, s výjimkou, kdy uchovávání vyžaduje platný a účinný právní předpis, nebo k tomu dal písemný souhlas Správce.

6. NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

6.1 Narušení bezpečnosti osobních údajů znamená jakýkoli bezpečnostní incident zahrnující skutečné, předpokládané nebo potenciální ohrožení důvěrnosti, integrity nebo dostupnosti Osobních údajů nebo sítě, systémů nebo databází, na kterých jsou Osobní údaje uloženy, přenášeny nebo zpracovávány, včetně jakéhokoli nahodilého, neoprávněného, nepovoleného nebo protiprávního zničení, použití, získávání, ukládání, prohlížení, pořizování kopií, ztráty, krádeže, změně, zpřístupnění zveřejněním nebo přístupu k Osobním údajům (dále jen „**Narušení bezpečnosti**“).

6.2 Při Narušení bezpečnosti Zpracovatel notifikuje bez zbytečného odkladu Správce na adrese dpo@ozp.cz a v každém jednotlivém případě bez zbytečného odkladu, nejpozději do 72 hodin po zjištění Narušení bezpečnosti způsobené Zpracovatelem, resp. jeho zaměstnanci, a poskytne Správci podrobný popis Narušení bezpečnosti, kategorie a typ Osobních údajů, které byly předmětem Narušení bezpečnosti, identitu každého dotčeného Subjektu osobních údajů a veškeré další informace, které může Správce nebo Úřad pro ochranu osobních údajů důvodně požadovat v souvislosti s dotčenými Subjekty osobních údajů a Narušením bezpečnosti. V případě porušení zabezpečení osobních údajů ze strany Správce není dotčeno ustanovení článku 33, resp. článku 34 Nařízení.

6.3 Zpracovatel se zavazuje, že neprodleně a na vlastní náklady provede opatření potřebné k:

(a) vlastnímu vyšetření Narušení bezpečnosti způsobeného Zpracovatelem;

(b) identifikaci, předcházení a zmírnění účinků jakéhokoli Narušení bezpečnosti způsobeného Zpracovatelem;

(c) poskytnutí přiměřené součinnosti Správci při oznamování Narušení bezpečnosti Úřadu pro ochranu osobních údajů a/nebo dotčeným Subjektům osobních údajů;

(d) k nápravě Narušení bezpečnosti způsobeného Zpracovatelem.

Před jakýmkoli zveřejněním nebo sdělením třetí osobě o výše uvedených oznámeních a/nebo podáních, sděleních, notifikacích nebo tiskových zprávách souvisejících s jakýmkoli Narušením bezpečnosti způsobeném Zpracovatelem, (dále jen „**Oznámení**

o narušení"), je Zpracovatel povinen obdržet písemný souhlas Správce, a to v případě kdy

(i) může být Správce konkrétně jmenován nebo odkazován v souvislosti s Oznámením o narušení;

(ii) jsou zapojeny nebo ovlivněny Osobní údaje a/nebo systémy Správce;

(iii) Oznámení o narušení je zaměřeno na Subjekty osobních údajů; nebo

(iv) Správce má nebo může mít určité nezávislé právní, smluvní nebo jiné závazky v důsledku Narušení bezpečnosti.

6.4 Zpracovatel se dále zavazuje, že bude řádně a bez prodlení odpovídat na veškeré relevantní dotazy ze strany Správce, Úřadu pro ochranu osobních údajů, vládních orgánů nebo správních orgánů, a poskytovat nezbytnou součinnost, pokud jde o jakékoli Narušení bezpečnosti způsobené Zpracovatelem. Zpracovatel je povinen poskytnout Správci na jeho žádost, nejpozději do 24 hodin od doručení této žádosti, informace o stavu Narušení bezpečnosti způsobené Zpracovatelem, a to i opakovaně až do doby odstranění stavu Narušení bezpečnosti způsobené Zpracovatelem nebo sjednání nápravy. Oznámení o narušení a každé jiné oznámení nebo notifikace s tím související bude Správci poskytnuto na jeho datovou schránku **q9iadw9** ve lhůtě nejméně 2 dny při předpokládaném ohrožení nebo Narušení bezpečnosti způsobeném Zpracovatelem, a nejvíce 24 hodin po dni, kdy k Narušení bezpečnosti způsobeném Zpracovatelem skutečně došlo.

6.5 Správce je povinen Zpracovatele bezodkladně informovat, v případě, že zjistí nebo předpokládá Narušení bezpečnosti, které může ovlivnit poskytování Služeb Zpracovatele v jakémkoli rozsahu. Oznámení musí být Zpracovateli poskytnuto na jeho datovou schránku hgaj3yx ve lhůtě nejméně 2 dny při předpokládaném ohrožení nebo Narušení bezpečnosti, a nejvíce 24 hodin po dni, kdy k Narušení bezpečnosti skutečně došlo. Výše uvedené informace Správce zároveň zadá formou hlášení v Informačním systému hlášení, který je provozován v souladu se Smlouvou o podpoře.

6.6 Zpracovatel uhradí Správci veškeré náklady, ztráty, způsobenou újmu a výdaje, které se vztahují nebo jsou výsledkem jakéhokoli prokázaného Narušení bezpečnosti vzniklého výhradně na straně Zpracovatele nebo jakéhokoli jiného porušení závazků Zpracovatele podle této Smlouvy. Výše uvedené zahrnuje mimo jiné také náklady na Oznámení o narušení, služeb pro styk s veřejností a dalších krizových opatření a/nebo konzultační, účetní nebo auditorské náklady týkající se nebo vyplývající z vyšetřování a opatření Správce k Narušení bezpečnosti a/nebo pokuty uložené Správci Úřadem pro ochranu osobních údajů v souvislosti s jednáním nebo opomenutím povinností Zpracovatele podle této Smlouvy a/nebo platných a účinných právních předpisů vztahujících se k ochraně osobních údajů.

7. SMLUVNÍ POKUTA

7.1 Pokud Zpracovatel poruší jakoukoli povinnost podle ustanovení článků 5 a/nebo 6 této Smlouvy, je Zpracovatel povinen uhradit smluvní pokutu Správci ve výši 250.000 Kč za

každé jednotlivé porušení. Smluvní pokuta je splatná do 20 dnů ode dne doručení žádosti o platbu zaslané Správcem na základě tohoto ustanovení Zpracovateli.

7.2 Zaplacením smluvní pokuty, jak je popsána v odstavci 7.1 výše, není dotčeno právo Správce požadovat náhradu újmy způsobenou porušením ustanovení této Smlouvy.

8. ZÁVĚREČNÁ USTANOVENÍ

8.1 Tato Smlouva může být měněna pouze formou písemných dodatků. Práva a povinnosti ujednané touto Smlouvou nejsou převoditelná bez předchozího písemného svolení druhé Smluvní strany.

8.2 Tato Smlouva je vyhotovena ve 4 stejnopisech. Každá Smluvní strana obdrží po 2 vyhotoveních.

8.3 Tato Smlouva se řídí právem České republiky. K řešení sporů vyplývajících z této Smlouvy nebo v souvislosti s ní jsou příslušné obecné soudy České republiky.

V Praze dne _____ 2019

Za Oborovou zdravotní pojišťovnu zaměstnanců bank, pojišťoven a stavebnictví

_____
Ing. Radovan Kouřil
generální ředitel

V Praze dne _____ 2019

Za _____

_____
_____
_____

Příloha č. 1
TECHNICKÉ A ORGANIZAČNÍ OPATŘENÍ OCHRANY A BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

1. POVINNOSTI ZPRACOVATELE

1.1 Zpracovatel je povinen:

(a) přijmout přiměřená opatření k zabránění neoprávněnému přístupu při Zpracování;

(b) přijmout veškerá přiměřená organizační opatření k zabránění neoprávněnému prohlížení, vytváření, pořizování kopií, přenášení, změnám nebo výmazům záznamů, které obsahují Osobní údaje;

(c) stanovit pravidla určující podmínky přístupu a případné další podmínky Zpracování.

2. ZVLÁŠTNÍ OPATŘENÍ ZPRACOVATELE K ZAJIŠTĚNÍ OCHRANY OSOBNÍCH ÚDAJŮ

2.1 Fyzický přístup

Zpracovatel má zaveden bezpečnostní standard fyzické ostrahy, který má zabránit neoprávněnému fyzickému přístupu do prostor a k zařízením Zpracovatele. Toho je dosaženo následujícími způsoby, příkladně:

- fyzický přístup do prostor Zpracovatele je omezen na jeho zaměstnance, subdodavatele a ohlášené návštěvy;
- monitorování přístupu do prostor Zpracovatele;
- prostory jsou zabezpečeny elektronickým systémem napojeným na pult centrální ochrany.

2.2 Řízení přístupů a jejich správa

Zpracovatel má zavedeny následující standardy pro řízení přístupu a správu IT prostředí s ohledem na obecné zabezpečení Zpracování:

- účty s oprávněním správce by měly být používány jenom pro potřeby administrátorské činnosti;

- každý účet s oprávněním správce je vysledovatelný k jedinečně identifikovatelnému jednotlivci;
- veškerý přístup k počítačům a serverům musí být nastaven podle pracovního zařazení zaměstnance;
- počáteční hesla musí být uživatelem změněna při prvním použití;
- zobrazení hesel musí být maskované nebo jinak zakryté tak, aby neoprávněné strany nebyly schopny je pozorovat nebo je následně obnovit;
- hesla musí být při jejich přenosu nebo uložení v databázi šifrovaná;
- složitost hesla by nikdy neměla být menší než 3 ze 4 tříd znaků a musí mít volby třídy znaků, jako jsou velká písmena, malá písmena, číslice nebo speciální znaky;
- délka hesla musí být nakonfigurována tak, aby obsahovala nejméně 8 znaků;
- hesla musí vypršet každých 365 dnů;
- automatizovaný časový limit přístupu uživatele k počítačům a serverům, tj. v případě nečinnosti uživatele je požadováno heslo pro obnovení přístupu;
- účty musí být nastaveny na zablokování po několika chybných pokusech o přihlášení.

2.3 Zabezpečení proti virům

Počítače a servery Zpracovatele mají přiměřeně aktuální verze softwaru zabezpečení, který může obsahovat firewall, antivirovou ochranu a aktualizované databáze a definice virů. Tento software je nakonfigurován tak, aby vyhledával a okamžitě odstranil nebo opravil zjištěné nálezy virů.

2.4 Personál Zpracovatele

Zaměstnanci Zpracovatele jsou vyškoleni v zásadách ochrany a bezpečnosti informací a seznámili se s jejich odpovědností v oblasti ochrany soukromí a bezpečnosti.

Zaměstnanci Zpracovatele jsou smluvně zavázáni k zachování důvěrnosti Osobních údajů Správce nebo jiných důvěrných informací a dodržování příslušných zásad, norem nebo požadavků Zpracovatele v souvislosti se Zpracováním. Nedodržení těchto zásad, norem nebo požadavků bude předmětem šetření, které může vést k disciplinárním opatřením nebo ukončení pracovního poměru ze strany Zpracovatele.

OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA
ZAMĚSTNANCŮ BANK, POJIŠŤOVEN
A STAVEBNICTVÍ

ZADÁVACÍ DOKUMENTACE

Veřejné zakázky „Identity Management – realizace“

Příloha č. 8 - Vzor smlouvy o dílo a o poskytování služeb

Příloha č. 6 – Dohoda o ochraně důvěrných informací

OZP OBOROVÁ ZDRAVOTNÍ POJIŠŤOVNA ZAMĚSTNANCŮ BANK, POJIŠŤOVEN A STAVEBNICTVÍ

TATO **DOHODA O OCHRANĚ DŮVĚRNÝCH INFORMACÍ** (dále jen „**Dohoda**“) je uzavřena níže uvedeného dne, měsíce a roku v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění

MEZI

Oborovou zdravotní pojišťovnou zaměstnanců bank, pojišťoven a stavebnictví
se sídlem Roškotova 1225/1, 140 21 Praha 4,
IČO: 47114321,
zapsanou v obchodním rejstříku vedeném Městským soudem v Praze pod sp. zn. A 7232,
zastoupenou [●], [●]

DÁLE JEN „**Objednatel**“
NA STRANĚ JEDNÉ

A

[DOPLNÍ DODAVATEL]
se sídlem: [DOPLNÍ DODAVATEL]
IČO: [DOPLNÍ DODAVATEL]
zápis v OR: [DOPLNÍ DODAVATEL]
zastoupen: [DOPLNÍ DODAVATEL]

DÁLE JEN „**Dodavatel**“
NA STRANĚ DRUHÉ

OBJEDNATEL A DODAVATEL DÁLE SPOLEČNĚ JEN „**Smluvní strany**“
NEBO SAMOSTATNĚ „**Smluvní strana**“

VZHLEDEM K TOMU, ŽE:

(A) Smluvní strany uzavřely smlouvu o dílo a o poskytování služeb „Identity Management – realizace“, v jejímž rámci bude docházet k dodání díla a poskytování služeb (dále jen „**Smlouva o dílo**“ a „**Služby**“[1]). Objednatel v souvislosti s plněním Smlouvy o dílo poskytne Dodavateli souhrn dokumentů a informací, které jsou podkladem pro Dodavatele k poskytování Služeb. Smluvní strany se dále dohodly, že jejich jednání o možnostech vzájemné spolupráce a/nebo poskytování Služeb bude podléhat režimu dodržování níže uvedených bezpečnostních ujednání.

(B) Účelem této Dohody je definovat v souvislosti v souvislosti s plněním práv a povinností při poskytování Služeb postupy a základní principy zajištění bezpečnosti a ochrany informací s cílem umožnit naplňování dlouhodobých a strategických plánů Objednatele, dosažení právní shody s národní a nadnárodní legislativou relevantní pro činnost Objednatele a zajištění dostupnosti, integrity a důvěrnosti aktiv Objednatele, především informačních.

(C) Smluvní strany dále předpokládají, že v souvislosti s poskytováním Služeb budou ze strany Objednatele předány Dodavateli informace a dokumenty, které mohou obsahovat Důvěrné informace (jak je tento pojem definován v článku 1.1 níže) týkající se Objednatele, jeho činnosti a mají zájem na zachování jejich důvěrnosti a ochrany před třetími stranami.

[1] Je-li v této Smlouvě používán pojem „Služby“, rozumí se tím veškeré plnění předmětu Smlouvy o dílo, tj. dodání díla a s ním související činnosti.

TÍMTO SE SMLUVNÍ STRANY DOHODLY NA NÁSLEDUJÍCÍM:

1. DEFINICE

V této Dohodě, pokud z jejího kontextu nevyplývá jinak, mají níže uvedené pojmy následující význam:

1.1 „**Důvěrné informace**“ znamená zejména Obchodní tajemství a dále pak veškeré dokumenty, data a informace související s plněním Smlouvy o dílo, které poskytne Objednatel (a to prostřednictvím jeho zaměstnanců, zástupců, poradců nebo jakékoli jiné Objednatelem pověřené osoby) Dodavateli (a to i jakýmkoli jeho zaměstnancům, zástupcům, poradcům nebo jiné Dodavatelem pověřené osobě) nebo je Dodavatel vlastní činností od Objednatele získá a které jsou či budou součástí smluvní dokumentace ohledně Služeb nebo budou souviset s plněním práv a povinností Dodavatele při poskytování Služeb, ať už k takovému poskytnutí nebo získání dokumentů a informací dojde písemně, obrazově či strojově čitelnou formou anebo ústně v rámci jakéhokoli jednání mezi Smluvními stranami, a to bez ohledu na to, zda tyto informace či skutečnosti byly výslovně Objednatelem označeny za důvěrné a bez ohledu na způsob zaznamenání a uchovávání těchto informací. Jedná se rovněž o informace, které mohou, ale nemusí, být chráněny rovněž právní úpravou obsaženou v Občanském zákoníku, v právních předpisech vztahujících se k ochraně osobních údajů, zejména v nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a v zákoně č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů. Důvěrné informace zahrnují rovněž informace chráněné zvláštní zákonnou a smluvní povinností mlčenlivosti Dodavatele. Důvěrné informace nezahrnují:

(i) informace, které jsou v okamžiku jejich poskytnutí Dodavateli veřejně dostupné, nebo

(ii) informace, které se stanou veřejně dostupnými poté, co budou poskytnuty Dodavateli jinak než jako výsledek porušení právní povinnosti Dodavatelem z této Dohody, nebo

(iii) údaje, které byly výslovně a písemně označeny ze strany Objednatele jako údaje, které nemají důvěrnou povahu.

1.2 „**Občanský zákoník**“ znamená zákon č. 89/2012 Sb., občanský zákoník, v platném znění.

1.3 „**Obchodní tajemství**“ znamená ve smyslu § 504 Občanského zákoníku jakékoli informace a skutečnosti, které jsou konkurenčně významné, určitelné, ocenitelné, v příslušných obchodních kruzích běžně nedostupné, které souvisejí se společností Objednatele či jejím obchodním závodem a jejichž utajení Objednatel ve svém zájmu odpovídajícím způsobem zajišťuje.

1.4 „**Poddodavatel**“ znamená jakoukoliv osobu anebo subjekt, který je v postavení anebo který bude v postavení poddodavatele Dodavatele v rámci nebo v souvislosti s poskytováním Služeb.

2. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

2.1 Důvěrné informace jsou a zůstanou předmětem práv, resp. ve vlastnictví Objednatele, který má zájem na jejich utajení. Poskytnutí Důvěrných informací Dodavateli nezakládá a nebude zakládat jakákoliv práva Dodavatele nebo jeho zaměstnanců, zástupců, poradců či jiných Dodavatelem pověřených osob (včetně jakýchkoliv práv duševního vlastnictví) k Důvěrným informacím s výjimkou omezeného práva nakládat s Důvěrnými informacemi podle této Dohody.

2.2 Dodavatel se zavazuje, že:

2.2.1 bude zachovávat mlčenlivost o všech Důvěrných informacích;

2.2.2 bez předchozí písemné dohody neučiní žádné tiskové prohlášení, veřejné nebo jiné oznámení týkající se smluv uzavřených mezi Smluvními stranami a jejich plnění;

2.2.3 bude využívat Důvěrné informace pouze pro účely anebo v souvislosti s jednáním o vzájemné spolupráci Smluvních stran a/nebo v souvislosti s poskytováním Služeb a nikoliv pro jiné účely;

2.2.4 nepoužije Důvěrné informace ke své vlastní podnikatelské činnosti, investiční nebo jiné činnosti, s výjimkou činností prováděných v souvislosti s realizací smluv uzavřených se Objednatelem;

2.2.5 neučiní vůči jiným osobám žádné prohlášení týkající se správnosti nebo jiných aspektů Důvěrných informací;

2.2.6 bude zacházet s Důvěrnými informacemi s odbornou péčí a tak, aby byla zachována jejich důvěrná povaha, a učiní veškerá opatření, která od něj lze rozumně požadovat, aby nedošlo k prozrazení či zneužití Důvěrných informací, jakož i k možnosti neoprávněného přístupu k nim, nebo jejich použití jinou osobou;

2.2.7 bez předchozího písemného souhlasu Objednatele neposkytne Důvěrné informace jakékoliv jiné osobě s výjimkou svých zaměstnanců, poradců anebo Poddodavatelů, kteří v souladu s jejich povinnostmi potřebují znát a využívat Důvěrné informace pro účely jednání o vzájemné spolupráci a/nebo poskytování Služeb;

2.2.8 bude informovat všechny své zaměstnance, zástupce, poradce a Poddodavatele, kteří by mohli obdržet Důvěrné informace pro účely uvedené v článku 2.2.7, o důvěrné povaze Důvěrných informací a zajistí, že tito zaměstnanci, zástupci, poradci a Poddodavatelé budou dodržovat podmínky této Dohody a že budou zavázáni zachovávat mlčenlivost ve vztahu k Důvěrným informacím alespoň v rozsahu ochrany Důvěrných informací podle této Dohody. Dodavatel odpovídá za jakákoliv porušení závazku zachovávat mlčenlivost ve vztahu k Důvěrným informacím jeho zaměstnanci, poradci a Poddodavateli;

2.2.9 povinnost mlčenlivosti trvá i po skončení poskytování Služeb Dodavatelem pro Objednatele, jakož i v případě, že jednání o vzájemné spolupráci mezi Smluvními stranami budou ukončena, aniž by byla vzájemná spolupráce Smluvních stran byla dojednána.

2.3 Dodavatel se zavazuje, že po ukončení poskytování Služeb okamžitě učiní následující opatření:

2.3.1 zničí anebo vymaže veškeré originály, kopie a/nebo záznamy jakéhokoliv dokumentu, disku nebo jiného nosiče dat anebo jakéhokoliv jiného materiálu obdrženého nebo zpřístupněného ze strany Objednatele, jeho zaměstnanců, zástupců, poradců či jiných Objednatelem pověřených osob nebo jiným způsobem, který obsahuje Důvěrné informace nebo ze kterého je možné vyvodit Důvěrné informace nebo který byl vytvořen na základě Důvěrných informací; toto ustanovení se nevztahuje na zálohy emailové korespondence;

2.3.2 vymaže veškeré Důvěrné informace z jakéhokoliv počítače, textového procesoru anebo jakéhokoliv zařízení, ve kterém by mohly být Důvěrné informace nahrány či uloženy v jakékoliv formě; a

2.3.3 do 14 dní po obdržení žádosti ze strany Objednatele poskytne Objednateli písemné potvrzení učiněné osobou oprávněnou jednat jménem či za Dodavatele, že veškeré Důvěrné informace byly zničeny v souladu s touto Dohodou, nebylo-li Smluvními stranami výslovně dohodnuto jinak.

2.4 Dodavatel se zavazuje zajistit, že jeho zaměstnanci, zástupci, poradci a Poddodavatelé splní obdobně závazky uvedené v článcích 2.2 a 2.3. O splnění této povinnosti je Dodavatel povinen pořídit písemný záznam.

2.5 Dodavatel je povinen neprodleně (nejpozději den následující po dni, kdy předmětnou událost zjistí) informovat Objednatele o každé mimořádné události, která může mít vliv na poskytování Služeb nebo na bezpečnost Důvěrných informací (zejména na jejich důvěrnost, dostupnost a integritu) ze strany Dodavatele a poskytnout Objednateli všechny dostupné informace pro objasnění možných příčin jejich vzniku, předpokládaného trvání a rozsahu a dále podniknout veškeré kroky potřebné k zabránění vzniku škody, nebo k jejímu maximálnímu omezení.

2.6 Za porušení této Dohody se nepovažuje, pokud Dodavatel poskytne Důvěrné informace v souladu se svou zákonnou povinností na žádost oprávněných orgánů veřejné správy. V takovém případě je Dodavatel povinen vyrozumět Objednatele neprodleně (nejpozději do druhého dne od obdržení žádosti) o obdržení takové žádosti, a pokud to bude možné, požádat Objednatele o stanovisko před poskytnutím Důvěrných informací.

2.7 Dodavatel je povinen zajistit ochranu Důvěrných informací ve smlouvách se třetími osobami, jakož i poučení těchto osob o důvěrné povaze jim předávaných informací a následcích porušení povinnosti mlčenlivosti.

2.8 Objednatel je oprávněn provádět prověrky ochrany Důvěrných informací u Dodavatele a Dodavatel je povinen takové prověrky umožnit.

3. VZÁJEMNÁ KOMUNIKACE

3.1 Není-li touto Dohodou stanoveno jinak, jakákoliv komunikace, která má být činěna podle této Dohody, musí být učiněna v písemné formě a může být doručena osobně nebo dopisem prostřednictvím pošty, doručovatelské služby, e-mailem do jejíchž rukou je určena.

3.2 Jakákoliv komunikace, která má být činěna podle této Dohody, bude považována za doručenou, v případě (i) komunikace prostřednictvím faxu po obdržení příslušného potvrzení o bezchybném přenosu dat, (ii) komunikace prostřednictvím e-mailu po obdržení e-mailu, kterým jeho původní adresát potvrdí doručení, (iii) osobního doručení jeho doručením adresátovi s tím, že bude-li se v jakémkoliv z těchto případů jednat o doručení mimo obvyklou pracovní dobu, bude se mít za to, že k doručení došlo na začátku následujícího pracovního dne, a (iv) komunikace formou dopisu doručením tohoto dopisu.

3.3 Nebude-li Smluvními stranami písemně dohodnuto jinak, bude písemná komunikace doručována podle této Dohody v českém jazyce.

4. SMLUVNÍ POKUTA

4.1 V případě, kdy Dodavatel jakkoli poruší závazek podle článků 2.2 až 2.48, je Objednatel oprávněn požadovat po Dodavateli zaplacení smluvní pokuty ve výši 1.000.000 Kč (slovy: jeden milion korun českých) (dále jen „**Smluvní pokuta**“) za každé jednotlivé porušení této Dohody. Zaplacením Smluvní pokuty Dodavatelem není dotčeno právo Objednatele na náhradu škody, přičemž Dodavatel odpovídá za škodu maximálně do výše limitu pojistného plnění dle čl. 9.3 Smlouvy o dílo. Smluvní strany výslovně potvrzují, že výše Smluvními stranami sjednané Smluvní pokuty odpovídá závažnosti porušení stanovených závazků a není nepřiměřeně vysoká.

4.2 Toto ustanovení nevylučuje sankční ustanovení v dalších smlouvách uzavřených mezi Objednatelem a Dodavatelem.

4.3 Smluvní strany mohou uplatnit Smluvní pokutu písemnou žádostí doručenou druhé Smluvní straně. Uplatnění Smluvní pokuty vyžaduje předchozí písemné upozornění na porušení Dohody, ve kterém bude stanovena lhůta pro jeho odstranění, ne kratší než pět pracovních dní. Smluvní pokuta je splatná do 14 dnů od dne uplynutí lhůty pro odstranění porušení Dohody podle předchozí věty.

5. UKONČENÍ DOHODY

5.1 Smluvní strany se výslovně dohodly, že tuto Dohodu není možné ukončit.

6. ZÁVĚREČNÁ USTANOVENÍ

6.1 Tato Dohoda nabývá platnosti a účinnosti dnem jejího podpisu všemi Smluvními stranami.

6.2 Dodavatel se výslovně a při plném vědomí vzdává práva dovolat se jakýchkoli zvyklostí zachovávaných obecně, v daném odvětví, nebo z předchozí spolupráce se Objednatelem. Tato Dohoda, jakož i veškeré právní vztahy z ní plynoucí, se řídí a je vykládána v souladu právními předpisy České republiky.

6.3 Tato Dohoda může být měněna pouze formou písemných a vzestupně číslovaných dodatků.

6.4 Bude-li jedno nebo více ustanovení této Dohody neplatné, neúčinné, zdánlivé nebo nevymahatelné, nebude to mít za následek neplatnost, neúčinnost, zdánlivost ani nevymahatelnost celé této Dohody. V takovém případě Smluvní strany nahradí takovéto neplatné, neúčinné, zdánlivé nebo nevymahatelné ustanovení ustanovením, které bude nejlépe odpovídat smyslu takového neplatného, neúčinného, zdánlivého a/nebo nevymahatelného ustanovení.

6.5 Tato Dohoda je vyhotovena ve čtyřech (4) stejnopisech v českém jazyce, z nichž každý má právní sílu originálu. Po uzavření této Dohody obdrží každá ze Smluvních stran po dvou (2) vyhotovení Dohody.

Smluvní strany potvrzují, že si přečetly podmínky obsažené v této Dohodě a že jim porozuměly. Jako důkaz své opravdové vůle přijmout závazky vyplývající z této Dohody připojují Smluvní strany k této Dohodě své podpisy. Smluvní strany tímto potvrzují převzetí příslušného počtu vyhotovení této Dohody.

V _____ dne _____ V _____ dne _____

_____	_____
Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví	**[DOPLNÍ DODAVATEL]**
Ing. Radovan Kouřil	jméno osoby oprávněné jednat za Dodavatele: [DOPLNÍ DODAVATEL]
generální ředitel	funkce: [DOPLNÍ DODAVATEL]