Smlouva o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PIM“

(dále též „Smlouva“)

Smluvní strany:

Česká republika – Ministerstvo zemědělství

se sídlem: Těšnov 17, 110 00 Praha 1

IČ: 00020478

bankovní spojení: ČNB, Praha 1, č. účtu: 1226-001/0710

zastoupená: Davidem Šetinou, ředitelem Odboru správy centrálních informačních systémů a kybernetické bezpečnosti (dále jen „**Objednatel**“ nebo též „**Zadavatel**“)

číslo smlouvy Objednatele: S2016-0100, č. sml. DMS 344-2016-13310

a

O2 IT Services s.r.o.

se sídlem: Za Brumlovkou 266/2, 140 22 Praha 4

IČ: 02819678, DIČ: CZ02819678

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze,

oddíl C, vložka 223566

bankovní spojení: PPF banka, a.s., č. účtu: 2019110006/6000

zastoupená: Ing. Václav Provazník, jednatel a Ing. Jan Bechyně, jednatel

(dále jen „**Zhotovitel**“ nebo též „**Dodavatel**“)

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 1746 odst. 2 ve spojení s § 2586 a násl. a s použitím § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník (dále jen „**občanský zákoník**“), postupuje se též dle ustanovení § 2079 a násl. občanského zákoníku.[1]

Touto Smlouvou se realizuje nadlimitní veřejná zakázka ve smyslu ust. § 10 a ust. § 12 odst. 1 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.

Obě smluvní strany, vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto Smlouvou vázány, se dohodly na následujícím znění smlouvy:

[1] V případě, že HW nebude součástí řešení, bude toto ustanovení před podpisem smlouvy vypuštěno.

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je ústředním orgánem státní správy, jehož působnost a zásady činnosti jsou stanoveny zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, a

1.1.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Zhotovitel prohlašuje, že:

1.2.1 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a

1.2.2 ke dni uzavření této Smlouvy není vůči němu vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**Insolvenční zákon**"), a zavazuje se Objednatele bezodkladně informovat o hrozícím úpadku, popř. o vzniku úpadku jeho společnosti, stejně jako o změnách v jeho kvalifikaci, kterou prokázal v rámci své nabídky na plnění Veřejné zakázky v dále uvedeném smyslu.

2. PŘEDMĚT A ÚČEL SMLOUVY

2.1. Účelem této Smlouvy je implementace centrální správy privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům a zaznamenávání aktivit privilegovaných účtů, včetně nahrávek obrazovek a stisků kláves (dále též „**PIM řešení**") v prostředí Objednatele. Účelem této Smlouvy je rovněž splnění veřejné zakázky s názvem „Správa a monitoring privilegovaných účtů – PIM" (dále jen „**Veřejná zakázka**").

2.2. Zhotovitel touto Smlouvou garantuje Objednateli splnění zadání uvedeného v Technické specifikaci v příloze č. 3 této Smlouvy (dále též „**TS**") a všech z toho vyplývajících podmínek a povinností. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:

2.2.1. v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel vyjádřený v TS,

2.2.2. v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení TS,

2.2.3. v případě jakéhokoliv rozporu mezi obsahem přílohy č. 1 této Smlouvy a obsahem TS má přednost obsah TS.

2.3. Zhotovitel se zavazuje provést pro Objednatele dílo spočívající v závazku Zhotovitele:

2.3.1. realizovat pro Objednatele analýzu, návrh řešení, dodávku, instalaci, implementaci PIM řešení, realizovat školení, poskytnout Objednateli časově neomezenou licenci k užívání PIM řešení a další práva dle specifikace v této Smlouvě a provést další činnosti specifikované v této Smlouvě dle specifikace uvedené v příloze č. 1 této Smlouvy a TS (dále jen „**Poskytnutí PIM řešení**");

2.3.2. poskytovat následnou technickou podporu výrobce standardních (generických) softwarových produktů tvořících součást PIM řešení dle parametrů uvedených v této

Smlouvě, zejména v TS a v katalogovém listu PIM02 Maintenance uvedeném ve Specifikaci katalogových listů v příloze č. 2 této Smlouvy (dále též „**Maintenance**") na dobu čtyř let od splnění etapy Instalace uvedené v Harmonogramu plnění (jak je tento pojem definován v odst. 3.1);

2.3.3. poskytovat následnou technickou a metodickou podporu (dále též „**Podpora**") dle parametrů uvedených v této Smlouvě, zejména v TS a v katalogových listech vyjma katalogového listu Maintenance ve Specifikaci katalogových listů v příloze č. 2 této Smlouvy (dále též „**SKL**"), a to od akceptace části Díla spočívající v Poskytnutí PIM řešení bez výhrad, nebo, stanoví-li tak Objednatel, od akceptace části Díla spočívající v Poskytnutí PIM řešení s výhradami, po dobu čtyř (4) let;

(Poskytnutí PIM řešení, Maintenance a Podpora dále společně jen „**Dílo**").

2.4. Zhotovitel se zavazuje a zaručuje, že veškeré činnosti a věcná plnění, které mají být provedeny na základě této Smlouvy, budou provedeny řádně a v dohodnutých termínech se znalostí a péčí, kterou je možné očekávat od odborníků, kteří mají požadované znalosti a relevantní zkušenosti s realizací činností obdobných jako je předmět této Smlouvy. Dílo nebude obsahovat žádné vady, které by bránily jeho použití k obvyklým účelům.

2.5. Zhotovitel se zavazuje v rámci plnění podle této Smlouvy nainstalovat nejnovější, výrobcem otestovanou a doporučenou verzi programových prostředků, která bude výrobcem v době plnění Smlouvy uvedena na trh.

2.6. Objednatel se zavazuje zajistit nezbytnou součinnost za podmínek stanovených v odst. 6.1 této Smlouvy a poskytnuté plnění za podmínek stanovených v této Smlouvě převzít a zaplatit za něj dohodnutou cenu v souladu s platebními podmínkami uvedenými v čl. 5. této Smlouvy.

2.7. Dodávka hardware je součástí předmětu Díla výhradně v případě, že tak stanoví příloha č. 1 Smlouvy.

3. TERMÍNY A MÍSTO PLNĚNÍ

3.1. Zhotovitel a Objednatel se dohodli na termínech plnění, které jsou uvedeny v harmonogramu plnění uvedeném v příloze č. 4 této Smlouvy (dále též „**Harmonogram plnění**").

3.2. Zhotovitel je oprávněn plnit i před sjednaným termínem plnění.

3.3. Zhotovitel se zavazuje dodat nejpozději do konce etapy B.4. Instalace definované v Harmonogramu plnění v příloze č. 4 této Smlouvy veškeré podklady potvrzující uhrazení ceny za licence a Maintenance na dobu jednoho (1) roku na PIM řešení za Objednatele a podklady potřebné k následnému obnovení Maintenance. Dále pak Zhotovitel Objednateli předá podklady pro zajištění přístupu k podpoře výrobce, aktualizacím PIM řešení a dalším zdrojům, ke kterým má Objednatel oprávněný přístup na základě platné Maintenance PIM řešení.

3.4. Místem plnění se sjednává sídlo Objednatele a Hostingová centra (dále též „**HC**") dle odst. 3.5 této Smlouvy. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Zhotovitel oprávněn poskytovat část svého plnění, resp. vést komunikaci s Objednatelem, telefonicky nebo prostřednictvím elektronické komunikace, případně též prostřednictvím vzdáleného přístupu.

3.5. Objednatel je oprávněn v průběhu trvání smluvního vztahu rozšířit nebo změnit poskytovatele a tedy i adresy HC v rámci České republiky. Aktuální adresy HC jsou:

3.5.1. Hostingové centrum Nagano

K Červenému dvoru 25/3156
130 00, Praha 3 – Strašnice

3.5.2. Hostingové centrum Chodov

V lomech 2339/1
149 00 Praha 4 – Chodov

4. PROVÁDĚNÍ, PŘEDÁNÍ A PŘEVZETÍ DÍLA

4.1. Způsob provedení části Díla spočívající v Poskytnutí PIM řešení bude blíže specifikován v rámci etapy analýza, blíže specifikované v příloze č. 1 této Smlouvy a TS (dále jen „Analýza").

4.2. Dílo provedené Zhotovitelem dle této Smlouvy bude Objednateli předáváno v souladu s postupem uvedeným v tomto čl. 4 Smlouvy. Částí Díla se rozumí: (i) Poskytnutí PIM řešení, (ii) Maintenance a (iii) Podpora.

4.3. Část Díla Poskytnutí PIM řešení bude Objednateli předána v místě plnění ve smyslu čl. 3 této Smlouvy v rámci akceptačního řízení, po odsouhlasení a následném potvrzení akceptačního protokolu pověřenými oprávněnými pracovníky Objednatele dle této Smlouvy. Řádné poskytování částí Díla Maintenance a Podpora bude potvrzováno prostřednictvím písemných dokumentů uvedených v odst. 4.6 až 4.9 této Smlouvy. Pro předání a převzetí částí Díla dále platí následující zásady:

4.3.1. proces akceptačního řízení je rozveden dále v tomto článku Smlouvy;

4.3.2. Objednatel není povinen část Díla převzít, dokud není předána v souladu s touto Smlouvou. Za takto nedokončenou část Díla není Objednatel povinen zaplatit cenu sjednanou ve Smlouvě.

4.4. Akceptační řízení části Díla spočívající v Poskytnutí PIM řešení probíhá následujícím způsobem:

4.4.1. Zhotovitel předá příslušnou část Díla Objednateli k akceptačnímu řízení spolu se Zhotovitelem podepsaným předávacím protokolem osvědčujícím předání části Díla k akceptačnímu řízení. Objednatel je povinen převzít část Díla k akceptačnímu řízení a odevzdat Zhotoviteli Objednatelem podepsaný předávací protokol bez zbytečného odkladu. Pro vyloučení pochybností se má za to, že akceptační řízení je zahájeno dnem podpisu předávacího protokolu Objednatelem.

4.4.2. Objednatel je povinen ve lhůtě dvanácti (12) pracovních dnů od zahájení akceptačního řízení uvést své výhrady a připomínky k části Díla vyjadřující případné vady části Díla, tj. rozpor vlastností části Díla oproti dohodnuté specifikaci uvedené v této Smlouvě a akceptované Analýze nebo určené v souladu s ní, a to formou písemného soupisu těchto výhrad a připomínek v akceptačním protokolu. V akceptačním protokolu Objednatel též specifikuje, zda část Díla v důsledku zjištěných vad neakceptuje, nebo ji akceptuje s výhradou odstranění zjištěných vad, přičemž Objednatel je rovněž oprávněn v případě akceptace části Díla s výhradou uvést v předmětném akceptačním protokolu část ceny v procentech z celkové ceny za část Díla, kterou bude možné dle odst. 5.8 této Smlouvy fakturovat, a to s ohledem na rozsah vad části Díla, které budou důvodem pro odmítnutí akceptace části Díla s výrokem „Akceptováno bez výhrad". Objednatel není povinen akceptovat část Díla s výhradou.

4.4.3. V případě, že Zhotovitel na části Díla neshledá žádné vady, část Díla akceptuje a vystaví o tom písemný akceptační protokol, ve kterém uvede, že část Díla je akceptována bez výhrad, a který bez zbytečného odkladu doručí Zhotoviteli.

4.4.4. Neakceptoval-li Objednatel část Díla bez výhrad, je Zhotovitel povinen se ve lhůtě 5 dnů od doručení akceptačního protokolu vyjádřit k Objednatelem zjištěným vadám, tyto bez zbytečného odkladu, nejpozději však do deseti (10) dnů od neúspěšné akceptace, odstranit a předat část Díla k opakovanému akceptačnímu řízení dle tohoto odst. 4.4 Smlouvy. Pokud z důvodu oprávněných výhrad Objednatele nebude dodržen termín pro akceptaci části Díla bez výhrad, je Zhotovitel v prodlení.

4.4.5. Část Díla bude považována za provedenou jako celek a předanou Objednateli dnem podpisu akceptačního protokolu Objednatelem s výrokem „Akceptováno bez výhrad".

4.4.6. Pro vyloučení pochybností se stanoví, že akceptační řízení ohledně akceptace Poskytnutí PIM řešení proběhne po úspěšném ukončení akceptačních testů, dodání dokumentace, poskytnutí školení a provedení veškerých dalších dílčích částí této části Díla, nedohodnou-li se smluvní strany jinak.

4.5. Pro akceptaci Analýzy ve smyslu odst. 4.1 této Smlouvy se přiměřeně použije akceptační procedura uvedená v odst. 4.4 této Smlouvy, nedohodnou-li se strany jinak. Ujednání o možnosti fakturovat část ceny se neaplikují.

4.6. Objednatel poté, co mu Zhotovitel předá

4.6.1. veškeré podklady potvrzující uhrazení ceny za Maintenance za období jednoho (1) roku plnění této Smlouvy,

4.6.2. podklady potřebné k následnému obnovení Maintenance,

4.6.3. podklady pro zajištění přístupu k podpoře výrobce, aktualizacím PIM řešení a dalším zdrojům, ke kterým má Objednatel oprávněný přístup na základě platné Maintenance PIM řešení,

potvrdí tuto skutečnost podpisem akceptačního protokolu.

4.7. Zhotovitel zašle Objednateli vždy do pěti (5) pracovních dnů ode dne uplynutí kalendářního měsíce, ve kterém byla poskytována Podpora, ke schválení záznam o poskytnutí služeb dle SKL dle katalogového listu PIM04 „Reparametrizace a optimalizace" s identifikací poskytnutých činností včetně jejich pracnosti (dále jen „**Záznam o poskytnutí služeb dle KL Reparametrizace a optimalizace**"). V Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace bude rozpad proveden dle nejmenší časové jednotky, hodina na jednoho člověka, pro dokladování pracnosti, a to nejméně v této míře detailu: konkrétní fyzická osoba provádějící činnost, popis činnosti, datum činnosti a doba trvání činnosti, přičemž evidovanou a účtovanou časovou jednotkou je každá započatá hodina činnosti. Plnění poskytované v rámci KL Reparametrizace a optimalizace bude vždy považováno za poskytnuté poté, co Objednatel potvrdí jeho řádné poskytnutí podpisem Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace.

4.8. Zhotovitel po uplynutí každého kalendářního měsíce poskytování Podpory vyhotoví kompletní výkazy, ze kterých bude jednoznačně zřejmé, zda byly služby Podpory a Maintenance poskytovány dle parametrů stanovených v příloze č. 2 této Smlouvy (dále jen „**Report podpory**"); pro vyloučení pochybností Report podpory zahrnuje údaje uváděné v Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace. Součástí Reportu podpory bude rovněž

vyhodnocení výše slevy z ceny, na kterou vzniklo Objednateli právo za vyhodnocovací období, za které byl Report podpory vyhotoven.

4.9. Zhotovitel zašle Objednateli vyhotovený Report podpory vždy do pěti (5) pracovních dnů ode dne uplynutí kalendářního měsíce, který je vyhodnocovacím / měřicím obdobím popsaným v předmětném Reportu podpory. Report podpory podléhá písemnému schválení Objednatelem. Pokud do desátého (10) dne ode dne předložení Reportu podpory nedojde k jeho schválení Objednatelem, zavazují se strany zahájit v dobré víře jednání za účelem dosažení shody o obsahu Reportu podpory.

4.10. Strany se dohodly, že použití ustanovení § 2605 odst. 2 občanského zákoníku je pro tuto Smlouvu vyloučeno.

5. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

5.1. Cena Díla byla stanovena dohodou v souladu s ustanoveními zákona č. 526/1990 Sb. o cenách, ve znění pozdějších předpisů následovně v (Kč):

Položka č.	Předmět plnění	Cena v Kč bez DPH	Sazba DPH v %	Výše DPH v Kč	Cena v Kč s DPH
1.	Poskytnutí PIM řešení	3 914 557,64	21	822 057,10	4 736 614,74
2.	Maintenance za období jednoho (1) roku	555 405,90	21	116 635,24	672 041,14
3.	Maintenance za období čtyř (4) let	2 221 623,60	21	466 540,96	2 688 164,56
4.	Podpora vyjma Reparametrizace a optimalizace – měsíční cena	17 550,00	21	3 685,50	21 235,50
5.	Podpora vyjma Reparametrizace a optimalizace – celková cena za čtyři (4) roky	842 400,00	21	176 904,00	1 019 304,00
6.	Reparametrizace a optimalizace – cena za jednu (1) člověkohodinu, (viz. SKL PIM04)	1 040,00	21	218,40	1 258,40
7.	Reparametrizace a optimalizace – cena za čtyři (4) roky (cena za 640 člověkohodin), (viz. SKL PIM04)	665 600,00	21	139 776,00	805 376,00
Celková nabídková cena (součet položek 1., 3., 5. a 7.)		7 641 181,24	21	1 605 278,05	9 246 459,30

5.2. Celková cena Díla dle této Smlouvy nepřekročí částku 7 644 181,24 Kč bez DPH, tedy při DPH ve výši 21%, která odpovídá 1 605 278,06 Kč, částku 9 249 459,30 Kč s DPH. Celková cena Díla bude určena jako součet cen za (i) Poskytnutí PIM řešení, (ii) Maintenance za období čtyř (4) let a (iii) Podporu dle doby jejího poskytování v souladu s Harmonogramem plnění, přičemž celková cena nepřekročí maximální cenu stanovenou v předchozí větě. Sjednaná celková cena pro celý rozsah Díla, určená v souladu s druhou větou tohoto odst. 5.2 této Smlouvy, je cenou nejvýše přípustnou, která je platná po celou dobu plnění této Smlouvy. Celkovou cenu Díla, určenou v souladu s druhou větou tohoto odst. 5.2 této Smlouvy, není možné z žádného důvodu navýšit s výjimkou navýšení sazby DPH při změně právních předpisů. Celková cena Díla, určená v souladu s druhou větou tohoto odst. 5.2 této Smlouvy, je stanovena za Dílo v rozsahu specifikace uvedené v této Smlouvě. Jakékoliv změny ceny Díla mohou být provedeny pouze dodatkem k této Smlouvě, který může být sjednán pouze v souladu s ustanoveními zákona č. 137/2006 Sb., o veřejných zakázkách ve znění pozdějších právních předpisů. Bude-li Podpora poskytována pouze po dobu části měsíce, bude hrazena poměrná část měsíční ceny. Zhotoviteli nevzniká právní nárok na poskytnutí plnění/ceny v plném rozsahu položky 7. tabulky v odst. 5.1 a tím ani poskytnutí plné ceny. V rámci KL Reparametrizace a optimalizace budou hrazeny pouze reálně čerpané člověkohodiny podle sjednané sazby za člověkohodinu, a to do maximálního objemu definovaného tímto katalogovým listem.

5.3. Cena zahrnuje ocenění všech prací a dodávek, které je nezbytné provést na základě vymezení dle této Smlouvy a jejích příloh, zejména přílohy č. 1, TS a SKL, není-li současně ve Smlouvě stanoveno, že jejich provedení má zajistit v rámci své součinnosti Objednatel.

5.4. Cena za část Díla Poskytnutí PIM řešení bude zaplacena Objednatelem na základě daňového dokladu (faktury), který Zhotovitel vystaví v souladu s touto Smlouvou po akceptaci části Díla Poskytnutí PIM řešení bez výhrad. V případě akceptace části Díla Poskytnutí PIM řešení s výhradou bude postupováno podle odst. 5.8 níže. Paušální měsíční cena za Podporu vyjma KL Reparametrizace a optimalizace bude hrazena za každý ukončený měsíc Podpory na základě daňového dokladu vystaveného Zhotovitelem po schválení Reportu podpory. Cena za Podporu bude zohledňovat případnou výši slevy z ceny dle SKL. Cena za poskytování plnění dle KL Reparametrizace a optimalizace bude hrazena za každý ukončený měsíc na základě schváleného Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace. Tato cena bude stanovena násobkem vynaložených a Objednatelem schválených člověkohodin a ceny za jednu člověkohodinu dle odst. 5.1 této Smlouvy. Objednatel není povinen čerpat ani uhradit maximální počet člověkohodin, resp. člověkodnů dle KL Reparametrizace a optimalizace. Cena za Maintenance bude hrazena ročně na základě faktury Zhotovitele. Zhotovitel je oprávněn vystavit fakturu poté, co Objednatel akceptačním protokolem podle odst. 4.6 této Smlouvy potvrdí splnění povinností Zhotovitele ohledně poskytování Maintenance za příslušné období.

5.5. Faktury Zhotovitele musí obsahovat všechny náležitosti řádného daňového a účetního dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, zejména dle jeho § 29, číslo této Smlouvy, číslo Smlouvy DMS, číslo projektu Objednatele, identifikaci plnění dle této Smlouvy, přičemž v případě faktury za Poskytnutí PIM řešení její nedílnou přílohou je závěrečný akceptační protokol o akceptaci části Díla Poskytnutí PIM řešení bez výhrad podepsaný Objednatelem, nejde-li o fakturu dle odst. 5.8 níže. V případě faktury za poskytování Podpory je nedílnou přílohou Objednatelem schválený Report podpory. V případě faktury za poskytování Maintenance je přílohou faktury Objednatelem potvrzený akceptační

protokol podle odst. 4.6 této Smlouvy vztahující se k příslušnému období. V případě faktury za poskytování služeb dle KL Reparametrizace a optimalizace je přílohou faktury Objednatelem schválený Záznam o poskytnutí služeb dle KL Reparametrizace a optimalizace obsahující údaj o množství reálně čerpaných člověkohodin.

5.6. Pokud faktura neobsahuje všechny zákonem a Smlouvou stanovené náležitosti a přílohy, je Objednatel oprávněn ji do data splatnosti vrátit s tím, že Zhotovitel je poté povinen vystavit novou fakturu s novým termínem splatnosti.

5.7. Splatnost faktur je dohodou smluvních stran stanovena na třicet dnů (30) ode dne jejího prokazatelného doručení Objednateli. Zaplacením se pro účely této Smlouvy rozumí odepsání příslušné částky z účtu Objednatele ve prospěch účtu Zhotovitele.

5.8. Objednatel neposkytuje zálohy. V případě, že Objednatel akceptuje Poskytnutí PIM řešení s výhradou, lze akceptační protokol prokazující takovouto akceptaci použít pro fakturaci do 60 % ceny Poskytnutí PIM řešení, stanoví-li tak písemně Objednatel. Zbývající část ceny Poskytnutí PIM řešení bude použita jako zádržné a bude vyplacena na základě daňového dokladu, jehož přílohou bude akceptační protokol prokazující akceptaci Poskytnutí PIM řešení bez výhrad.

6. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

6.1. Smluvní strany jsou povinny se vzájemně informovat o všech okolnostech důležitých pro řádné a včasné provedení Díla, přičemž Objednatel je povinen poskytnout Zhotoviteli součinnost v následujícím rozsahu:

6.1.1. zajistit potřebné přístupy do prostor MZe pro pracovníky Zhotovitele a spolupráci pracovníků MZe se Zhotovitelem v nezbytném rozsahu,

6.1.2. poskytnout Zhotoviteli všechny nezbytné součinnosti pro provedení Díla, které si Zhotovitel vyžádá a takovou nezbytnost součinnosti ze strany Objednatele náležitě odůvodní (zejména, fyzický přístup k hardware, přístupová práva nebo asistenci oprávněné osoby – administrátora IT),

6.1.3. vyjadřovat se k návrhům na další postup Zhotovitele, bude-li to nezbytné pro řádné zhotovení Díla,

6.1.4. zajistit účast svých pracovníků na školení v dohodnutém termínu,

6.1.5. zajistit připravenost hardware, který má Objednatel poskytnout dle TS.

6.2. Objednatel je povinen poskytovat součinnost pouze v nezbytném rozsahu, který je specifikován v odst. 6.1 této Smlouvy. Součinnost bude poskytnuta prostřednictvím kontaktní osoby.

6.3. V případě, že je nezbytná součinnost Objednatele pro řádné plnění této Smlouvy Zhotovitelem a Objednatel je v prodlení s jejím poskytnutím, zavazuje se Zhotovitel na toto prodlení Objednatele písemně upozornit v přiměřených intervalech, které nebudou delší než pět (5) dnů.

6.4. Zhotovitel je povinen Objednatele neprodleně informovat o jakýchkoliv okolnostech, které mohou ohrozit realizaci Díla nebo způsobit zpoždění realizace Díla.

6.5. Objednatel má právo přesvědčit se kdykoliv v průběhu plnění Díla o stavu prací na Díle. Pokud by se ukázalo, že Zhotovitel práce na Díle neprovádí nebo je prokazatelně a bezdůvodně provádí v rozporu se zadáním, má právo od Smlouvy odstoupit, a to za předpokladu, že na tento rozpor Zhotovitele písemně upozornil a Zhotovitel ve lhůtě deseti (10) pracovních dnů nesjednal nápravu tohoto stavu.

6.6. Zhotovitel je povinen provádět následující etapy Díla prostřednictvím osob, které uvedl v seznamu členů odborného týmu za účelem prokázání kvalifikace v rámci své nabídky na plnění Veřejné zakázky. Zhotovitel je povinen prostřednictvím těchto osob provádět etapy Analýza a Implementace části Díla Poskytnutí PIM řešení a dále část Díla Podpora. Zhotovitel je oprávněn nahradit tyto osoby jinými osobami s obdobnou (stejnou nebo vyšší) kvalifikací s předchozím písemným souhlasem Objednatele. Objednatel neodepře udělení souhlasu bez závažného důvodu.

6.7. Zhotovitel se při plnění zavazuje dodržovat zásady bezpečnosti informací v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti"), a vyhláškou č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti"). Bezpečností informací se v souladu se zákonem o kybernetické bezpečnosti rozumí zajištění důvěrnosti, integrity a dostupnosti informací, které budou uchovávány, vytvářeny nebo zpracovávány v PIM řešení nebo v systémech, které mají vazbu na PIM řešení a v souvislosti s kterými Objednateli vznikají právní povinnosti na základě zákona o kybernetické bezpečnosti (§ 3 tohoto zákona).

6.8. Zhotovitel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené zákonem o kybernetické bezpečnosti, vyhláškou o kybernetické bezpečnosti, vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Zejména se Zhotovitel zavazuje poskytnout Objednateli součinnost směřující k zavedení a provádění bezpečnostních opatření podle uvedených právních předpisů.

6.9. Jestliže vznikne v souvislosti se zavedením a prováděním bezpečnostních opatření podle právních předpisů uvedených v předchozím odstavci potřeba uzavřít dodatek k této smlouvě nebo zvláštní smlouvu, zavazuje se Zhotovitel poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy.

6.10. Rozsah a povaha součinnosti Zhotovitele sjednané v odst. 6.8 až 6.9 Smlouvy budou vždy určeny zejména podle rozsahu a povahy vlivu PIM řešení na bezpečnost informací Objednatele a rovněž podle rozsahu a povahy vazeb PIM řešení na systémy, v souvislosti s kterými Objednateli vznikají právní povinnosti na základě zákona o kybernetické bezpečnosti (§ 3 tohoto zákona).

6.11. Zhotovitel je povinen zajistit dodržování pravidel a pokynů Objednatele týkajících se vstupu a pohybu osob v místech plnění uvedených v čl. 3. osobami jeho pracovníků a pracovníků jeho subdodavatelů.

6.12. V případě, že po skončení účinnosti této Smlouvy dojde k uzavření nové smlouvy týkající se služeb Podpory nebo jakékoli jejich části nebo podobného či souvisejícího plnění s novým poskytovatelem odlišným od Zhotovitele, zavazuje se Zhotovitel po skončení účinnosti této Smlouvy poskytovat Objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely plynulého a řádného poskytování služeb obdobných službám Podpory či jejich příslušné části novým poskytovatelem, pokud bude naplnění tohoto cíle záviset na znalostech Zhotovitele získaných na základě plnění této Smlouvy. Pro vyloučení pochybností se uvádí, že Zhotovitel je v rámci součinnosti dle tohoto odstavce Smlouvy povinen zabezpečit na výzvu Objednatele osobní účast příslušných členů realizačního týmu na jednáních s Objednatelem či jím určenými třetími stranami. Zhotovitel se zavazuje tuto součinnost poskytovat s odbornou péčí, bez zbytečného odkladu a zodpovědně, a to minimálně po dobu tří (3) měsíců ode dne, ve kterém tato Smlouva zanikla. Zhotovitel se zavazuje reagovat na požadavek Objednatele nebo jím určené třetí strany a zahájit poskytování součinnosti dle tohoto odstavce Smlouvy nejpozději do tří (3) pracovních dnů ode dne doručení takovéhoto požadavku. Smluvní strany se dohodly, že cena za plnění dle tohoto odstavce je součástí ceny za poskytování služeb Podpory bez nároku na další finanční plnění.

6.13. Použije-li Zhotovitel při plnění této smlouvy subdodavatele, odpovídá Objednateli, jako by plnil sám.

6.14. Zhotovitel je povinen v průběhu trvání této Smlouvy průběžně aktualizovat uživatelskou, provozní a technickou dokumentaci, kterou Objednateli předal v rámci provádění části Díla Poskytnutí PIM řešení a poskytnout aktualizovanou verzi Objednateli nejpozději do pěti (5) pracovních dnů po doručení žádosti Objednatele.

7. ZÁRUKA A ZÁRUČNÍ SERVIS

7.1. Zhotovitel se zavazuje po dobu čtyř (4) let poskytovat technickou podporu výrobce (Maintenance) za podmínek uvedených v SKL.

7.2. Zhotovitel poskytuje záruku za jakost spočívající v tom, že Zhotovitel se zavazuje v průběhu čtyř (4) let ode dne akceptace části Díla Poskytnutí PIM řešení bez výhrad („záruční doba") odstranit na své náklady veškeré vady části Díla Poskytnutí PIM řešení, kterými se rozumí zejména Zhotovitelem zaviněná nemožnost použití části Díla Poskytnutí PIM řešení v souladu s jeho účelem nebo rozpor jeho vlastností v s příslušnou dokumentací, a to do dvaceti (20) pracovních dnů (za podmínky, že Objednatel poskytne nezbytnou součinnost, zejména přístup na pracoviště, kde je části Díla Poskytnutí PIM řešení instalováno nebo využíváno, součinnost administrátora). Tato záruční doba se prodlužuje o dobu, po kterou nelze části Díla Poskytnutí PIM řešení využívat. Záruka dle tohoto článku se nevztahuje na vady způsobené zásahem Objednatele nebo jím pověřené třetí osoby do Díla provedeným bez vědomí Zhotovitele. Pro vyloučení pochybností se uvádí, že záruka za jakost uvedená v tomto odst. 7.2 se vztahuje i na PIM řešení ve verzi upravené v rámci poskytování Maintenance nebo Podpory. Závazkem dle odst. 7.2 této Smlouvy nejsou dotčeny závazky týkající se poskytování Maintenance nebo Podpory. Zhotovitel dále poskytuje záruku za jakost oprav nebo úprav provedených v průběhu záruční doby s tím, že záruční doba vztahující se k úpravám nebo opravám provedeným v průběhu záruční doby uplyne sto osmdesát (180) dnů po ukončení záruční doby vztahující se k části Díla Poskytnutí PIM řešení jako celku.

8. SMLUVNÍ POKUTY A NÁHRADA ŠKODY

8.1. Za každý den prodlení Zhotovitele s provedením části Díla Poskytnutí PIM řešení je Zhotovitel povinen zaplatit Objednateli smluvní pokutu a ve výši 0,2 % z maximální celkové ceny Díla bez DPH uvedené v odst. 5.2 této Smlouvy.

8.2. Za každý den prodlení Zhotovitele s odstraněním faktické vady části Díla Poskytnutí PIM řešení v intencích odst. 7.2. této Smlouvy je Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve výši 0,2% z maximální celkové ceny Díla bez DPH uvedené v odst. 5.2 této Smlouvy.

8.3. Za každý den prodlení Zhotovitele se splněním povinnosti poskytnout Objednateli:

8.3.1. podklady potvrzující uhrazení ceny za licence a Maintenance na dobu jednoho (1) roku na PIM řešení za Objednatele,

8.3.2. podklady potřebné k následnému obnovení Maintenance,

8.3.3. podklady pro zajištění přístupu k podpoře výrobce, aktualizacím PIM řešení a dalším zdrojům, ke kterým má Objednatel oprávněný přístup na základě platné Maintenance PIM řešení,

a to do konce etapy B.4. Instalace definované v Harmonogramu plnění v příloze č. 4 této Smlouvy, je Zhotovitel povinen zaplatit Objednateli smluvní pokutu ve 2.000,- Kč.

8.4. Zhotovitel je povinen uhradit Objednateli smluvní pokutu ve výši 500.000,- Kč za každé porušení povinnosti mlčenlivosti nebo jiné povinnosti specifikované v čl. 11. Smlouvy či jakékoli povinnosti specifikované v čl. 9. Smlouvy, a to za každý jednotlivý případ porušení povinnosti.

8.5. V případě, že Zhotovitel nevyužije pro plnění svých závazků v rozporu s odst. 6.6 osobu tam uvedenou, ale bude své závazky plnit prostřednictvím jiných osob, uhradí smluvní pokutu ve výši 50.000,- Kč, a to za každý jednotlivý případ takového porušení.

8.6. V případě porušení pravidel uvedených v čl. 6. odst. 6.11 této Smlouvy se Zhotovitel zavazuje uhradit Objednateli smluvní pokutu ve výši 150.000,- Kč, a to za každý jednotlivý případ takového porušení.

8.7. Objednatel má právo na slevu z ceny Podpory určenou v souladu s ustanoveními přílohy č. 2 této Smlouvy. Objednatel má dále právo na smluvní pokuty v souladu s ustanoveními přílohy č. 2 této Smlouvy.

8.8. Zhotovitel nese plnou odpovědnost za to, že Dílo nebude zatíženo právem třetí osoby. V případě, že jakákoliv třetí strana uplatní jakékoliv nároky vůči Objednateli z důvodu porušení obchodního tajemství, patentu, autorských či jiných práv duševního vlastnictví třetích stran souvisejících s provedením Díla, Objednatel bez zbytečného odkladu písemně oznámí Zhotoviteli tento uplatněný nárok či jakoukoli žalobu v této věci podanou proti Objednateli, nejpozději však ve lhůtě dvaceti (20) pracovních dnů ode dne, kdy třetí strana uplatnila nárok vůči Objednateli, resp. Objednateli byla doručena žaloba třetí strany. V případě soudního sporu nebo rozhodčího řízení se Zhotovitel zavazuje na výzvu Objednatele poskytnout veškerou potřebnou součinnost, a to především podat Objednateli veškeré informace, které jsou nezbytné k prokázání práv a Objednatele, resp. Zhotovitele, dále předat Objednateli včas listinné důkazy a navrhnout svědky,

kteří mohou být vyslechnuti před soudem. Zhotovitel se zavazuje odškodnit Objednatele v plné výši v případě, že třetí strana úspěšně a oprávněně proti Objednateli uplatní autorskoprávní či jiný nárok plynoucí z právní vady poskytovaného Díla.

8.9. Smluvní strany odpovídají za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Zhotovitel plně odpovídá též za škodu způsobenou v souvislosti s touto Smlouvou svým subdodavatelem. Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu § 2913 občanského zákoníku. Zhotovitel odpovídá za skutečně vzniklou škodu a ušlý zisk.

8.10. Objednatel je oprávněn požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta nebo sleva z ceny, přičemž smluvní strany výslovně uvádí, že uhrazení smluvní pokuty ani slevy z ceny nemá vliv na právo na náhradu škody.

8.11. Smluvní pokuty jsou splatné jednadvacátý (21.) den ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší. Zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.

8.12. Zhotovitel se zavazuje mít platné a účinné pojištění odpovědnosti za škodu způsobenou Zhotovitelem třetím osobám ve výši 15.000.000,- Kč a udržovat toto pojištění po celou dobu realizace Díla, zajišťování Podpory a trvání záruky k Dílu.

9. AUTORSKÁ PRÁVA, LICENČNÍ UJEDNÁNÍ A PŘECHOD VLASTNICTVÍ

9.1. Pro případ, že výsledkem činnosti Zhotovitele a/nebo jeho subdodavatele či osob jimi využitými k poskytování plnění dle této Smlouvy je dílo, které naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů (dále jen „**autorské dílo**"):

9.1.1. Zhotovitel prohlašuje, že bude nejpozději ke dni zahájení jakéhokoli užívání autorského díla Objednatelem oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorskému dílu a že má nebo bude mít nejpozději k uvedenému dni souhlas autorů k uzavření následujících licenčních ujednání; toto prohlášení zahrnuje i taková práva autorů, která by vytvořením autorského díla teprve vznikla. Pokud prohlášení dle předchozí věty nebude moci být dodrženo z důvodu, že část autorského díla byla provedena subdodavatelem Zhotovitele, je Zhotovitel povinen zajistit si od subdodavatele dostatečná práva k poskytnutí licence a souvisejících oprávnění Objednateli v souladu s ustanoveními této Smlouvy, a to nejpozději ke dni převzetí příslušné subdodávky;

9.1.2. Zhotovitel poskytuje Objednateli (nabyvateli licence) oprávnění ke všem v úvahu přicházejícím způsobům užití autorského díla a bez jakéhokoliv omezení, a to zejména pokud jde o územní, časový nebo množstevní rozsah užití;

9.1.3. smluvní strany se výslovně dohodly, že cena za poskytnutí této licence Zhotovitele je již zahrnuta v ceně za poskytnutí Díla;

9.1.4. Zhotovitel poskytuje tuto licenci Objednateli (nabyvateli licence) jako nevýhradní. Tímto ustanovením není dotčeno oprávnění Objednatele dle níže uvedených ustanovení udělit sublicence, resp. postoupit licenci dalším osobám;

9.1.5. Objednatel není povinen licenci využít;

9.1.6. Objednatel (nabyvatel licence) je oprávněn práva tvořící součást licence zcela nebo zčásti jako podlicenci poskytnout třetí osobě;

9.1.7. Objednatel (nabyvatel licence) je oprávněn bez dalšího upravit či jinak měnit autorské dílo, jeho název nebo označení autorů, stejně jako spojit autorské dílo s jiným dílem nebo zařadit autorské dílo do díla souborného nebo na jeho základě či při jeho využití vytvořit dílo nové, a to přímo nebo prostřednictvím třetích osob, přičemž tato oprávnění trvají i po ukončení účinnosti Smlouvy.

9.2. V případě, že součástí plnění Zhotovitele podle této Smlouvy jsou movité věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem jejich předání a převzetí Objednatelem.

9.3. Pokud v rámci plnění této Smlouvy vzniknou zdrojové kódy počítačových programů, je Zhotovitel povinen předat Objednateli tyto zdrojové kódy, které jsou spustitelné v prostředí Objednatele, zaručující možnost ověření, že zdrojový kód je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality, a to včetně podrobné dokumentace a komentáře zdrojového kódu (dokumentovaný a komentovaný zdrojový kód). Zhotovitel je povinen předat Objednateli zdrojové kódy bez prodlevy, nejpozději do tří (3) pracovních dnů, po jejich vyvinutí a doručení žádosti Objednatele o jejich poskytnutí, nejpozději však do pěti (5) pracovních dnů po skončení účinnosti Smlouvy, a to na základě předávacího protokolu.

9.4. Pokud kdykoliv po dobu trvání Smlouvy dojde k opravě zdrojového kódu v souvislosti s plněním této smlouvy, jeho změně, doplnění, upgrade či update, která bude vyvolána ze strany Zhotovitele, předá Zhotovitel tento nový dokumentovaný a komentovaný zdrojový kód. Objednateli neprodleně, nejpozději do tří (3) pracovních dnů, po doručení žádosti Objednatele o jeho poskytnutí, opět na základě předávacího protokolu.

9.5. Předchozí ustanovení tohoto článku se v plném rozsahu vztahují pouze na autorská díla, která byla vytvořena Zhotovitelem a/nebo jeho subdodavateli či osobami jimi využitými k poskytování plnění na základě této Smlouvy (dále jen „**Unikátní díla**"). Zhotovitel je povinen Objednateli poskytnout nebo pro Objednatele zajistit práva užít autorská díla, která nejsou Unikátními díly, ale představují standardní software třetích stran, tedy softwarové vybavení dodané v rámci Smlouvy, které nebylo vyvinuto Zhotovitelem a není aplikační softwarovou komponentou vyvinutou v rámci Smlouvy (dále jen „**Neunikátní díla**"), v rozsahu standardní licence umožňující minimálně užívání PIM řešení v souladu s jeho určením, přičemž teritoriální rozsah poskytnuté licence musí být sjednán alespoň pro území České republiky a licence musí být poskytnuta jako nevypověditelná minimálně na dobu trvání autorských práv majetkových. Pro vyloučení jakýchkoliv pochybností smluvní strany sjednávají, že jakákoliv autorská díla poskytnutá Objednateli v rámci plnění dle této Smlouvy jsou Unikátními díly, nejsou-li Zhotovitelem předem a výslovně označena za Neunikátní díla. Použití jakéhokoliv Neunikátního díla Zhotovitelem v rámci plnění dle této Smlouvy podléhá předchozímu písemnému schválení ze strany Objednatele. Ve vztahu k dokumentaci vztahující se k Neunikátním dílům je Zhotovitel povinen

poskytnout nebo pro Objednatele zajistit práva duševního vlastnictví přiměřeně dle odst. 9.5 a 9.6 Smlouvy.

9.6. Aniž jsou tím dotčena jiná oprávnění Objednatele dle této Smlouvy, platí, že veškerá autorská díla poskytnutá Objednateli jako součást plnění poskytovaného dle Smlouvy je Objednatel oprávněn, bez nutnosti opatřit si další souhlas Zhotovitele či jiné osoby, poskytnout k užití a případným úpravám či jiným změnám všem organizačním složkám státu a příspěvkovým organizacím v rezortu Objednatele, právnickým osobám založeným a/nebo řízeným Objednatelem a dalším osobám, kterým bude podle rozhodnutí Objednatele umožněno užití PIM řešení. Objednatel je dále oprávněn, bez nutnosti opatřit si další souhlas Zhotovitele či jiné osoby, poskytnout těmto subjektům podlicenci nebo na ně licenci postoupit, a to dle své volby. Možnost poskytnutí licence nebo sublicence dle předchozí věty se nepoužije pro Neunikátní díla, u nichž je předmětné nakládání s Neunikátním dílem vyloučeno standardními licenčními podmínkami vykonavatele majetkových práv autorských k předmětnému Neunikátnímu dílu. Zhotovitel je však při předání Neunikátního díla, jehož licenční podmínky omezují Objednatele v poskytnutí podlicence nebo postoupení licence, povinen předem písemně na tuto skutečnost Objednatele upozornit. Pokud Zhotovitel Objednatele na předmětnou skutečnost takto neupozorní, odpovídá za veškerou újmu, která může být Objednateli a/nebo všem organizačním složkám státu, příspěvkovým organizacím a právnickým založeným a/nebo řízeným Objednatelem způsobena. Bez ohledu na jiná ustanovení této Smlouvy platí, že licenční oprávnění poskytnutá Objednateli na základě této Smlouvy nesmí omezovat Objednatele v poskytnutí služeb PIM řešení k užití jiným osobám uvedeným v první větě tohoto odstavce, ani nesmí omezovat Objednatele v zajišťování provozu a rozvoje PIM řešení jiným dodavatelem než je Zhotovitel, to vše ani tehdy, budou-li součástí PIM řešení Neunikátní díla.

9.7. Zhotovitel tímto prohlašuje a Objednateli garantuje, že ani po ukončení účinnosti této Smlouvy nebo po ukončení plnění ze strany Zhotovitele nebude Zhotovitel uplatňovat žádné nároky v souvislosti s užíváním Unikátních i Neunikátních děl Objednatelem nebo třetími osobami ani úpravami či jinými změnami Díla prováděnými Objednatelem nebo třetími osobami. Zhotovitel dále prohlašuje a výslovně Objednatele ujišťuje, že na základě práv poskytnutých Zhotovitelem bude Objednatel oprávněn poptávat služby údržby, podpory a rozvoje PIM řešení nebo podobná či související plnění u jiných dodavatelů v budoucích zadávacích řízeních dle zákona č. 137/2006 Sb., o veřejných zakázkách ve znění pozdějších předpisů (dále jen „**ZVZ**"), resp. v zadávacích řízeních dle budoucích předpisů upravujících zadávání veřejných zakázek. V případě, že jakákoliv osoba namítne porušení svého práva duševního vlastnictví v souvislosti s postupem Objednatele dle předchozí věty, je Zhotovitel povinen na své náklady zajistit poskytnutí veškerých potřebných práv Objednateli.

9.8. V případě, že výsledkem plnění dle této Smlouvy budou jiné předměty duševního vlastnictví než autorská díla, poskytne Zhotovitel Objednateli licenci a další práva duševního vlastnictví s obdobnou specifikací jako v případě autorských děl.

9.9. Cena za poskytnutí všech práv duševního vlastnictví dle Smlouvy, zejména dle tohoto článku, je plně zahrnuta v ceně Díla dle čl. 5. Smlouvy.

9.10. Smluvní strany se dohodly, že ustanovení § 2364, § 2370 a § 2378 občanského zákoníku se nepoužijí.

9.11. Bude-li v souvislosti s plněním předmětu této Smlouvy Zhotovitelem vytvořena databáze, bude se za pořizovatele takové databáze vždy považovat Objednatel.

10. OZNÁMENÍ A KOMUNIKACE

10.1. Veškerá oznámení, tj. jakákoliv komunikace na základě této Smlouvy, bude probíhat v souladu s tímto článkem.

10.2. Kromě jiných způsobů komunikace dohodnutých mezi stranami se za účinné považují osobní doručování, doručování doporučenou poštou, faxem či elektronickou poštou, a to na následující adresy smluvních stran, nebo na takové adresy, které si strany vzájemně písemně oznámí.

10.2.1. Za Objednatele:

Kontakt	Oblast	Telefon	E-mail
David Šetina	Smluvní a obchodní podmínky, včetně podpisu předávacího a akceptačního protokolu	221 813092	david.setina@mze.cz
Ing. Karel Štefl	Technické záležitosti	221 812 659	karel.stefl@mze.cz

10.2.2. Za Zhotovitele:

Kontakt	Oblast	Telefon	E-mail
Michal Kopeček	Smluvní a obchodní podmínky, včetně podpisu předávacího a akceptačního protokolu	602 523 401	michal.kopecek@o2.cz
Martin Rubeš	Technické záležitosti	724 156 582	martin.rubes@o2.cz
Helpdesk	Záruční servis a Podpora	241 020 701	helpdesk@corpus.cz

10.3. Oznámení se považují za uskutečněná v případě osobního doručování anebo doručování doporučenou poštou okamžikem doručení, v případě posílání faxem či elektronickou poštou okamžikem obdržení potvrzení od protistrany při použití stejného komunikačního kanálu.

10.4. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny do tří (3) dnů ode dne změny oprávněné osoby na takovou změnu druhou smluvní stranu písemně upozornit. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.

11. OCHRANA INFORMACÍ

11.1. Zhotovitel se zavazuje během plnění i po ukončení této Smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví v souvislosti s plněním této Smlouvy (dále též **„důvěrné informace"**).

11.2. Ustanovení odst. 11.1. se nevztahuje na informace, které jsou veřejné nebo které měl Zhotovitel k dispozici nebo mu byly dostupné i před jejich zpřístupněním Objednatelem a na informace, které se staly veřejnými bez toho, aby to protiprávně způsobila přijímající strana, a dále na

informace, které Zhotovitel prokazatelně sám vyvinul nebo zjistil bez porušení závazků dle této Smlouvy.

11.3. Porušením ochrany informací není, pokud Zhotovitel zpřístupní důvěrné informace Objednatele:

11.3.1. neboť byl povinen učinit tak na základě zákona nebo vykonatelného rozhodnutí soudu či příslušného správního orgánu;

11.3.2. svým subdodavatelům, oprávněně se podílejícím na plnění této Smlouvy, jen v nezbytně nutném rozsahu potřebném k zajištění plnění jejich povinností subdodavatele, zavázal-li uvedené osoby smluvně k ochraně těchto informací;

11.3.3. svým účetním, daňovým, právním nebo jiným odborným poradcům, jsou-li tyto osoby smluvně nebo zákonem zavázány k ochraně těchto informací.

11.4. Zhotovitel se zavazuje v souvislosti s ochranou informací poučit všechny osoby, které se budou podílet na plnění předmětu Smlouvy, a to včetně subdodavatelů, o povinnosti mlčenlivosti.

11.5. Smluvní strany jsou povinny zachovávat ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a ZVZ.

11.6. Zhotovitel souhlasí se zveřejněním Smlouvy na internetových stránkách Ministerstva zemědělství ČR ve smyslu směrnice MZe č. 6/2015. Zhotovitel je srozuměn s tím, že Objednatel je oprávněn zveřejnit Smlouvu na svých webových stránkách a dále je povinen uveřejnit dle § 147a odst. 1 písm. a) ZVZ na svém profilu zadavatele (dále jen „Profil"), tuto Smlouvu včetně všech jejích změn a dodatků. Dále je Zhotovitel srozuměn s tím, že dle § 147a odst. 1 písm. b) ZVZ je Objednatel povinen uveřejnit na Profilu výši skutečné uhrazené ceny za plnění Veřejné zakázky a dle § 147a odst. 1 písm. c) ZVZ též seznam subdodavatelů Zhotovitele. Zhotovitel tímto uděluje Objednateli souhlas k uveřejnění všech podkladů, údajů a informací uvedených v tomto odstavci a těch, k jejichž uveřejnění vyplývá pro Objednatele povinnost dle právních předpisů.

11.7. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel oprávněn v souladu s § 147a ZVZ uveřejnit:

11.7.1. tuto Smlouvu včetně všech jejích změn a dodatků,

11.7.2. výši skutečně uhrazené ceny za plnění Veřejné zakázky a

11.7.3. seznam subdodavatelů dodavatele Veřejné zakázky.

12. PLATNOST A ÚČINNOST SMLOUVY, VÝPOVĚĎ A ODSTOUPENÍ OD SMLOUVY

12.1. Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami a je uzavřena na dobu určitou do konce doby poskytování Podpory.

12.2. Každá smluvní strana je oprávněna od Smlouvy odstoupit v případech stanovených zákonem a touto Smlouvou.

12.3. Objednatel je dále oprávněn od Smlouvy odstoupit v případě, že:

12.3.1. je Zhotovitel v prodlení s plněním jeho závazků po dobu delší než třicet (30) dnů;

12.3.2. Zhotovitel pozbude oprávnění vyžadované právními předpisy k činnostem, k jejichž provádění se Zhotovitel zavázal podle této Smlouvy;

12.3.3. Zhotovitel poruší povinnost ochrany důvěrných informací ve smyslu této Smlouvy;

12.3.4. vůči Zhotoviteli bylo zahájeno insolvenční řízení nebo byl insolvenční návrh zamítnut pro nedostatek majetku Zhotovitele, podle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů (dále jen „insolvenční zákon"), nebo pokud Zhotovitel vstoupí do likvidace či se ocitne v úpadku.

12.4. V případě odstoupení od Smlouvy tato Smlouva zaniká ke dni doručení odstoupení druhé smluvní straně. Smluvní strany si vrátí již poskytnuté plnění, není-li touto Smlouvou stanoveno jinak. Odstoupení od Smlouvy se nedotýká částí Díla, které byly ke dni účinnosti odstoupení od Smlouvy dokončeny a předány Objednateli, přičemž Poskytnutí PIM řešení se považuje za jednu část Díla. Objednatel má právo rozhodnout, zda si ponechá rozpracované plnění, tedy část Díla, která nebyla ke dni účinnosti odstoupení od Smlouvy dokončena a předána Objednateli. V případě, že si Objednatel rozpracované plnění ponechá, má Zhotovitel nárok na poměrnou část ceny odpovídající poměrné části zhotoveného Díla. V případě, že Objednatel nebude mít zájem ponechat si rozpracované plnění, má Zhotovitel, nebude-li se jednat o odstoupení od Smlouvy v rámci jejího odst. 12.3 této Smlouvy, nárok na náhradu účelně vynaložených nákladů na provedení daného plnění do doby doručení odstoupení od Smlouvy, výše náhrady těchto nákladů však nesmí být vyšší, než by byla 1/2 výše ceny předmětného plnění ponížené dle předchozí věty.

12.5. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněný nárok na zaplacení smluvních pokut.

12.6. Objednatel je oprávněn tuto Smlouvu částečně vypovědět v části týkající se poskytování Podpory, a to s dvouměsíční výpovědní dobou, která začíná běžet ode dne doručení výpovědi Zhotoviteli.

12.7. Objednatel je oprávněn tuto Smlouvu částečně vypovědět v části týkající se poskytování Maintenance, a to vždy ke konci ročního období trvání Maintenance, přičemž je povinen oznámit svou výpověď Zhotoviteli měsíc před ukončením příslušného ročního období.

12.8. Ukončením účinnosti této Smlouvy nejsou dotčeny nároky z odpovědnosti za vady, nároky z odpovědnosti za škodu a nároky ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy. Licence, ostatní práva dle čl. 9 a záruky poskytnuté po dobu účinnosti Smlouvy jsou zachovány v rozsahu, v jakém se týkají plnění, které si v souladu s touto Smlouvou Objednatel ponechá.

13. POSTOUPENÍ A ZMOCNĚNÍ

13.1. Žádná práva ani povinnosti z této Smlouvy nemohou být postoupena jednou smluvní stranou na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany, není-li v této Smlouvě výslovně uvedeno jinak.

13.2. Pokud Zhotovitel v souladu s touto Smlouvou pověří plněním některých svých povinností z této Smlouvy třetí osobu, zůstává Zhotovitel plně odpovědný za plnění třetí strany tak, jako by plnil sám.

13.3. Zhotovitel není na základě této Smlouvy oprávněn jednat jménem Objednatele bez písemné plné moci udělené pro konkrétní účel specifikovaný v takové plné moci Objednatelem.

14. ZÁVĚREČNÁ USTANOVENÍ

14.1. Zhotovitel tímto prohlašuje, že v době uzavření Smlouvy není vůči němu vedeno řízení dle insolvenčního zákona a zavazuje se Objednatele bezodkladně informovat o všech skutečnostech o jeho hrozícím úpadku, popř. o prohlášení jeho úpadku.

14.2. Zhotovitel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

14.3. Tato Smlouva (a její přílohy) představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze v souladu s ustanoveními ZVZ písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat jménem smluvních stran.

14.4. Vztahy vzniklé mezi smluvními stranami na základě této Smlouvy se řídí občanským zákoníkem a dalšími ustanoveními právních předpisů České republiky, zejména autorským zákonem. Smluvní strany se dohodly, že veškeré spory vzniklé na základě této Smlouvy budou řešeny prostřednictvím obecných soudů České republiky.

14.5. Nedílnou součástí této Smlouvy jsou tyto přílohy:

Příloha č. 1:	Návrh technického řešení
Příloha č. 2:	Specifikace katalogových listů
Příloha č. 3:	Technická specifikace
Příloha č. 4:	Harmonogram plnění
Příloha č. 5:	Vzor předávacího protokolu
Příloha č. 6:	Vzor akceptačního protokolu
Příloha č. 7:	Seznam subdodavatelů

14.6. V případě rozporu mezi čl. 1 až 14 této Smlouvy a přílohami mají přednost ustanovení čl. 1 až 14 této Smlouvy. Tím není dotčeno ustanovení odst. 2.2 článku 2. Smlouvy, přičemž garance tam uvedená má před jinými ustanoveními Smlouvy přednost.

14.7. Práva Objednatele vyplývající z této Smlouvy či jejího porušení se promlčují ve lhůtě patnácti (15) let ode dne, kdy právo mohlo být uplatněno poprvé.

14.8. Zhotovitel přebírá podle § 1765 odst. 2 občanského zákoníku nebezpečí změny okolností v souvislosti s plněním této Smlouvy, zejména v souvislosti s cenou za poskytnuté plnění a požadavky na poskytování Podpory.

14.9. Tato Smlouva je vyhotovena ve 4 vyhotoveních v českém jazyce s platností originálu, z nichž každá ze smluvních stran obdrží 2 vyhotovení.

14.10. Smluvní strany prohlašují, že si tuto Smlouvu přečetly, rozumí jejímu obsahu a s jejím obsahem souhlasí, což stvrzují svými podpisy.

Za Objednatele:

v Praze dne 26-04-2016

Nevěřejné

Česká republika –
Ministerstvo zemědělství
David Šetina
ředitel Odboru správy centrálních informačních systémů a kybernetické bezpečnosti

MINISTERSTVO ZEMĚDĚLSTVÍ
Těšnov 65/17
110 00 Praha 1 - Nové Město
-27-

Za Zhotovitele:

v Praze dne 22-04-2016

Nevěřejné

O2 IT Services s.r.o.
Ing. Václav Provazník
jednatel

O2 IT Services s.r.o.
Za Brumlovkou 266/2
140 00 Praha 4
DIČ: CZ02819678
10

Nevěřejné

O2 IT Services s.r.o.
Ing. Jan Bechyně
jednatel

PŘÍLOHA Č. 1

NÁVRH TECHNICKÉHO ŘEŠENÍ

Popis navrhovaného řešení

V rámci poptávaného řešení naše společnost nabízí řešení CyberArk Privileged Identity Management Suite (dále jen PIM) který je komplexní centrálně spravovaný nástroj a řešení pro vyloučení rizik a životní cyklus správy sdílených privilegovaných identit. Umožňuje organizacím zabezpečit, spravovat a monitorovat všechny činnosti spojené s různými typy privilegovaných identit jako například administrátorů Windows serverů, správců UNIX serverů, síťových prvků a v neposlední řadě hesel, které jsou součástí aplikací a skriptů. Veškeré přístupové údaje a informace se ukládají do centrálního úložiště Secure Digital Vault s vícevrstvým zabezpečením. Navrhované řešení ve všech bodech naplňuje požadavky zadávací dokumentace ohledně poptávaného řešení.

Přehled dodávaných licencí

Licence	Popis licence	Počet
PAS Enterprise Infrastructure (Software)	- 1 Licence bezpečnostního trezoru (Vault) - 1 Central Policy Manager – pro řízení přihlašovacích údajů/hesel - Softwarové appliance pro přístup k heslům - Licence pro řízení NEOMEZENÉHO počtu hesel	1x
Server Disaster Recovery module (Software)	Obsahuje plnou pasivní podporu pro všechny služby a komponenty nainstalovaného řešení	1x
Enterprise Password Vault (EPV)	Zabezpečuje, řídí a kontroluje využití privilegovaných účtů Licence na uživatele	260
Privileged Session Manager (PSM)	Monitoruje, izoluje a nahrává aktivity privilegovaných přístupů Licence na cílový systém	436
CyberArk PAS SDK	CyberArk PAS SDK (PACLI, NAPI, web-services)	1x
Application Identity Management (AIM)	Licence na instalovaného agenta v systému	2x
Application Identity Management for Application Servers (ASCP)	Licence na management	3x
Testing Environment License - Licence na trezor	Licence: Celá infrastruktura, až pro 50 uživatelských licencí EPV, 10 konkurentních session pro PSM, 50 SSH Key Manager systémových licencí a 20 Provider licencí pro AIM a OPM	1x

Enterprise Password Vault
Umožňuje organizacím zabezpečit, spravovat, automaticky měnit a zaznamenávat všechny činnosti spojené se všemi typy privilegovaných hesel a SSH klíčů. Jedná se o úložiště, na kterém je proveden hardening, enkryptované pomocí metody splňující standard FIPS 140-2 a odpovídající pouze zabezpečeného vault protokolu.

SSH Key Manager
Brání zneužití SSH klíčů, které jsou privilegovanými uživateli a aplikacemi Unix / Linux často používány k ověření privilegovaných účtů. SSSH Key Manager zabezpečuje a především rotuje privilegované SSH klíče na základě vaší bezpečnostní politiky. Řídí, monitoruje a chrání přístup k SSH klíčům. Toto řešení umožňuje organizacím získat kontrolu nad SSH klíči, které jsou často ponechány bez správy.

Privileged Session Manager
Umožňuje organizacím řídit a monitorovat privilegované přístupy k citlivým systémům a zařízením. PSM poskytuje záznam prováděné relace s možností jejího přehrávání a nahrávání textu, stejně jako bezpečný vzdálený přístup k citlivým systémům používající privilegované single sign-on přihlášení bez sdělení použitých pověření koncovým uživatelům.

Privileged Session Manager PSM SSH Proxy
Zachovává výhody PSM, jako jsou izolace, řízení a monitorování, přičemž umožňuje uživatelům připojit se transparentně k cílovým systémům na platformě UNIX z jejich vlastní pracovní stanice bez přerušení jejich nativních pracovních postupů. PSMP zaznamenává všechny aktivity, které se vyskytují v průběhu privilegovaných sezení v kompaktním formátu v trezoru serveru, kde mohou být přístupné autorizovaným auditorům. Podobně jako PSM poskytuje single sign-on přihlašování.

Application Identity Manager
Poskytuje privilegované přihlašovací údaje pro využití v aplikacích a skriptech formou Pull i Push přístupu. Eliminuje napevno uložená hesla v kódech a lokálně uložené SSH klíče a umožňuje skriptům a aplikacím obdržet přihlašovací údaje na vyžádání ze zabezpečeného úložiště.

Password Vault Web Access
Je centrálním webovým rozhraním pro správu PIM Suite.

Central Policy Manager
Umožňuje organizacím řídit a definovat politiku hesel. Může automatizovaně kontrolovat a měnit hesla na vzdálených systémech a ukládat je do EPV .

On-Demand Privileges Manager
Omezuje možnosti privilegovaného uživatele provádět vybrané aktivity. Eliminuje používání práv „root", nebo „Administrator" a umožňuje jejich personalizaci s konkrétním privilegovaným účtem.

Tabulka komponent a použité zkratky

Název komponenty	Zkratka
Privileged Identity Management	PIM
Enterprise Password Vault	EPV
Central Policy Manager	CPM
Password Vault Web Access	PVWA
Privileged Session Manager	PSM
On-Demand Privileges Manager	OPM
Application Identity Management	AIM
Disaster Recovery Vault	DR Vault
Event Notification Engine	ENE

Návrh technického řešení

Následující kapitola popisuje způsob naplnění funkčních a jiných požadavků vyplývajících z definice požadavků uvedených v Technické specifikaci.

Password Management
Řešení CyberArk poskytuje systém s centrálním vysoce zabezpečeným úložištěm privilegovaných účtů a příslušných hesel spolu s konektory na koncové systémy (dále jen EP) s řízenými účty a uživatelským rozhraním, nad kterým je postavena logická vrstva v podobě procesů a politik.

Uživatelé (zaměstnanci/externí dodavatelé) přistupující do systému pomocí uživatelského rozhraní na základě autentizace proti lokálnímu, nebo externímu adresáři (AD/LDAP) získává množinu privilegovaných účtů, kterými může disponovat.

Přístupy k takovým účtům je možné díky řešení CyberArk zabezpečit těmito způsoby:

1. Heslo je možné si nechat zobrazit na obrazovce a následně použít standardním způsobem pro přístup k chráněnému systému
2. Použít automatizované přihlášení (SSO) k systému pomocí privilegovaného účtu bez nutnosti prozrazení hesla. Přihlášení probíhá buďto přímo v prohlížeči prostřednictvím pluginu prohlížeče, který otevře okno s příslušnou klientskou aplikací, bez nutnosti její lokální instalace, nebo je využito lokální klientské aplikace na koncové stanici uživatele, které je heslo předáno pomocí skriptu. Tímto způsobem jsou podporovány běžné protokoly/aplikace:
    - SSH, Telnet;
    - RemoteDesktop;
    - HTTP(s)/Web aplikace;
    - Libovolná aplikace běžící v prostředí MS Windows;

Takový přístup výrazně zvyšuje uživatelský komfort, jelikož uživatelé nejsou nuceni s hesly privilegovaných účtů vůbec pracovat, veškerá akce probíhají automaticky na pozadí (tzv. privileged SSO). Uživatelé si tak např. nemusí pamatovat mnoho dalších hesel, ale využívají jen heslo svého účtu.

Řešení pro ochranu privilegovaných identit od společnosti CyberArk pro zobrazení/použití hesla uživatel spustí akci check-out, při které je za pomoci konektoru heslo změněno, stejně jako po ukončení práce s účtem, kdy je volána akce check-in. Při použití automatizovaného přihlášení dochází k akci check-out/in automaticky. Tímto je zaručena jasná evidence toho, kdo má k jakým účtům přístup a v jaké chvíli je využíval.

Kromě účtů, které má uživatel volně k dispozici, bude mít také přiřazeny účty, ke kterým získá přístup až po udání důvodu, nebo po schválení jiným uživatelem, nebo skupinou uživatelů. Takový přístup získá buď na omezenou dobu, nebo na stálo. Schvalovací workflow je možné libovolně strukturovat, nebo je možné využít napojení na externí service desk.

V případě nouzové situace, kdy je potřeba získat přístup k heslu privilegovaného účtu okamžitě, existuje proces, který takovou akci podporuje, za současného zalogování a odeslání notifikace na určenou kontaktní osobu.

Pro spravované účty jsou definovány politiky hesel, které jasně definují složitost hesla a jeho stáří – dle těchto politik jsou generována náhodná hesla, která jsou aktivně propisována do EP pomocí konektorů. V pravidelném intervalu je naplánována kontrola, zda nedošlo ke změně hesla privilegovaného účtu při externím zásahu mimo PIM systém. Detekovaný zásah je aktivně notifikován. Zároveň je plánováno pravidelné discovery účtů na EP – zde je vhodná interakce s IDM, aby bylo možné jednoznačně odlišit, zda se jedná o uživatelský účet patřící konkrétní identitě, nebo o sdílený privilegovaný účet. Takové účty jsou reportovány odpovědné osobě, která je na základě definovaného procesu zařadí příslušným uživatelům a nastaví odpovídající politiky hesel.

Kromě přístupu uživatelů k privilegovaným účtům, systém obsluhuje také přístup aplikací. Je poskytnut aplikační interface umožňující provést check-out hesla k účtu, čímž poskytuje možnost vyvarovat se použití otevřeného hesla přímo v kódu skriptu/aplikace. Standardně je v rámci řešení password managementu možné integrovat mechanizmus pro získávání hesla přímo do aplikačních serverů, které jej mohou používat k získání přístupu k různým datovým zdrojům (databáze). Tímto jednoduchým mechanizmem je možné zbavit se uložených přístupových údajů bez nutnosti spravovat aplikaci.

Session Recording

Součástí nabízeného řešení CyberArk je systém nahráváním uživatelských relací - snímáním obrazovky a logování uživatelského vstupu (key- logging). Každá akce (stisk klávesy, změna obrazovky apod.) privilegovaného účtu je nahrávána a je jednoznačně přiřazena konkrétní osobě. Nahrávky jsou zabezpečeným způsobem přenášeny do centrálního úložiště, kde jsou dlouhodobě uchovávány. Takové nahrávky jsou klíčovým důkazem, kterým je možné uživateli jednoznačně prokázat veškeré jeho aktivity. Zároveň však mohou obsahovat velice citlivé informace. Proto řešení poskytuje zabezpečení v souladu se základní bezpečnostní triádou CIA (confidentiality, integrity, availability):

- Confidentiality (důvěrnost) – nahrávky jsou po celou dobu uchovávány v zašifrované podobě - tedy od jejich zaznamenání, až po konečné uložení do centrálního repository a jejich archivace. Dále je zaručeno, že k těmto nahrávkám mohou přistupovat pouze autorizované osoby, aby nemohlo dojít k jejich zneužití. U vysoce citlivých/kritických systémů je možné aplikovat metodu čtyř očí, kdy je k zobrazení záznamu podmíněno schválením další osoby.
- Integrity (celistvost) – je nutné zabránit jakékoliv manipulaci s nahrávkami po celou dobu jejich existence, aby nemohlo dojít ke zpochybnění její prokazatelnosti. Toho je možné dosáhnout digitálním podpisem každé z nahrávek.
- Availability (dostupnost) – klíčovost těchto nahrávek implikuje nutnost zaručit jejich dostupnost. Nahrávky jsou pravidelně zálohovány, současně je zajištěno, že nemohou být jednoduše odstraněny.

Access Control

Tato oblast se zabývá řízením přístupu privilegovaných účtů, tedy kontrolu nad tím, jaké aktivity může jaký uživatel s privilegovaným účtem provádět. Můžeme chápat jako přidání další vrstvy oprávnění na koncovém systému, kde je účet využíván.

Tato funkcionalita není v rámci tohoto projektu vyžadována, přesto nabízené řešení tuto funkcionalitu podporuje, aby bylo možné celou problematiku pokrýt v rámci jednoho řešení pouze jeho rozšířením.

Access control je tedy určen sadou politik, které se skládají z následujících pravidel:

1. Výčet příkazů, které uživatel může/nemůže spouštět.
2. Výčet zdrojů, které uživatel může/nemůže využívat – např. soubory, adresáře.
3. Výčet kanálů, které uživatel může/nemůže využívat pro přístup k systému.
4. Časová okna definující, kdy je možné k systému přistupovat.

Omezení budou přímo vynucena, nebo pouze auditována, kdy vyhodnocení pravidla v případě porušení může spustit generování události do systému SIEM nebo notifikaci.

Politiky budou centrálně spravovány a bude zajištěna jejich distribuce a deployment na koncové systémy a to buď manuální (politiky jsou EP ručně přiřazeny), nebo automatická (na základě typu nebo kategorie EP).

Řízení přístupu k EP

Řešení PIM tak bude umožňovat řídit a monitorovat přístup:

- externích dodavatelů přistupujících z Internetu k EP hostovaným v HC Nagano a HC Chodov;
- externích dodavatelů přistupujících z Internetu k EP hostovaným v lokalitě Těšnov;
- interních zaměstnanců MZe přistupujících z lokality Těšnov k EP hostovaným v HC Nagano, HC Chodov a v lokalitě Těšnov;

Integrace s prostředím klienta

Nabízené řešení CyberArk bude integrováno s ostatními systémy organizace dle následujícího popisu.

LDAP/AD

Adresářová služba LDAP nebo Active Directory bude využita jako primární zdroj autentizace a autorizace uživatelů pro všechny jejich aktivity v prostředí PIM. Autorizace opravňuje uživatele k těmto aktivitám:

1. Aktivity v rámci systému na řízení PIM, tedy příslušnost základních rolí:
    a. Administrátor – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek).
    b. Auditor – má přístup k auditním informacím a nahrávkám.
    c. Uživatel – je mu umožněn přístup k systému PIM a jeho běžné používání.
2. Aktivity spojené s privilegovanými účty:
    a. Vlastník – nastavuje, kdo má k účtu přístup, případně schvaluje přístup v rámci workflow, přiřazuje politiky hesel.
    b. Uživatel – může účet buď přímo používat, nebo je mu umožněno o přístup k účtu zažádat.

Struktura oprávnění je zpravidla ještě dále členěna, jedná se pouze o základní pohled. Konečný výčet rolí a jejich obsah vyplyne z analýzy během dodávky.

IDM

V rámci analýzy během dodávky bude za součinnosti zadavatele a správce IDM navržena kooperace systému IDM a PIM při discovery účtů na EP, kdy je potřeba zjistit, zda nově nalezený neřízený účet patří identitě (osobě), nebo se jedná o sdílený privilegovaný účet, na základě čehož je účet předán do správy buď IDM nebo PIM systému.

Logování a SIEM Systém

PIM loguje jak veškeré aktivity prováděné administrátory nad řešením, tak i veškeré operace uživatelů používajících PIM. Všechny tyto logované záznamy jsou v reálném čase přenášeny do systému pro bezpečnostní monitoring (SIEM) k jejich vyhodnocení a uložení na centrálním bezpečném místě pro případnou zpětnou analýzu.

Dodavatel bude se zadavatelem konzultovat návrh integrace logů ze systémů a aplikací na EP, aby bylo možné vyhodnotit dodržování pravidel pro přístup daných PIM řešením (např. že uživatelé přistupují k EP přes vyhrazené přístupové řešení a ne napřímo). Nasazení této funkcionality však provede zadavatel.

Service Desk

Schvalování uživatelských akcí bude řešeno přímo v systému PIM. Schvalování bude vynuceno v následujících případech:

1. Přiřazení privilegovaného účtu uživateli.

2. Použití privilegovaného účtu (např. při inicializaci relace).
3. Přístup k nahrávce uživatelské relace.

Nabízené řešení však obsahuje také rozhraní pro integraci s nástroji Service Desk.

Funkční požadavky

Součástí Technické specifikace je tabulka ve formátu Excel, která obsahuje seznam požadavků na funkcionalitu řešení PIM (dále jen „Tabulka požadavků") a způsoby jejich naplnění dodavatelem.

Rozsah

Řízené systémy/aplikace

V rámci projektu budou do Session Recordingu a Password Managementu postupně zahrnuty následující systémy a aplikace:

	Systém/Aplikace (typ EP)	Protokol/Rozhraní	Počet systémů/apl.
1.	Fyzické servery s operačním systémem • Unix/Linux – HP-UX, RedHat, CentOS • Windows (standalone, nebo zapojené do domény)	SSH – Unix/Linux RDP/WMI – Windows	100
2.	Virtuální servery s operačním systémem • Unix/Linux – RedHat, CentOS • Windows (standalone, nebo zapojené do domény)	SSH – Unix/Linux RDP/WMI – Windows VMWare	250
3.	Infrastrukturní a bezpečnostní prvky (routery, switche, firewall, WCF, IPS, IDS, WIFI atd.)	SSH/Telnet, HTTP(S) (webové rozhraní)	70
4.	VMware ESXi 5.1.0	Tlustý klient/web vSphere	Fyz. serverů: 16 CPU 12 core: 6 CPU 8 core: 24 CPU 6 core: 4 CPU 4 core: 6
5.	Citrix XenApp platforma, včetně session recordingu deployovaných aplikací.	Tlustý klient/web ICA	2
6.	LDAP (Oracle Internet Directory)	LDAP	2
7.	Microsoft Active Directory (přístup k doméně privilegovanými osobními účty nelze omezit, proto bude řešeno monitoringem SIEM systémem)	LDAP/RDP	3
8.	SAP • SAP Business Warehouse • SAP ERP (systémy R3, AF, EP)	Tlustý klient/web	1
9.	Databáze (Oracle, MS SQL)	SQL/Tlustý klient Oracle – SQL*Plus, SQL Developer MS SQL – SQL Server Management Studio	15 (instance)
10.	Aplikační servery s administračním web GUI (JBoss, WebLogic, GlassFish, Oracle AS, Tomcat)	Webové rozhraní	35
11.	Ostatní aplikace využívající webové rozhraní nebo tlustého klienta, např.: *SUR, AK, OIM, dohledové systémy, zálohovací systémy, SIEM, ServiceDesk*	Tlustý klient/web	30

Pokud nebude možné některé z aplikací/systémů uvedených v řádcích 3, 8, 10, 11 tabulky zařadit do plného Password Managementu z důvodu nemožnosti jednoduše měnit hesla k účtům, bude v takovém případě heslo alespoň evidováno a v pravidelném intervalu měněno správcem aplikace/systému manuálně.

Počty uživatelů

Počet uživatelů využívajících PIM pro přístup k systémům, pro něž je řešení navrženo, je následující:

- Celkový počet uživatelů: 260;

- Maximální počet současně přistupujících uživatelů: 70;
- Průměrný počet přistupujících uživatelů za den: 70;
- Průměrná délka uživatelské relace za den: 5 hodin;

Licence potřebné k pokrytí výše uvedených parametrů jsou součástí nabízeného řešení.

Archivace nahrávek

Nahrávky Session Recordingu bude možno uchovávat 5 let na bezpečném úložišti. Z tohoto úložiště nebudou nahrávky okamžitě dostupné, neboť bude nutné před jejich prohlížením nejprve nahrávky přenést na určené místo (vyvolat). Nabízené řešení CyberArk podporuje ukládání nahrávek v bezpečné formě na externí úložiště v prostředí zákazníka.

Nahrávky, které nejsou starší než 8 měsíců, budou dostupné bez nutnosti jejich vyvolávání.

Přístupové body

Řešení PIM bude v lokalitě MZe Těšnov obsahovat jeden přístupový bod, který bude zajišťovat nahrávání uživatelských relací a řízení přístupu k EP provozovaných jak v lokalitě Těšnov, tak i v HC Nagano a HC Chodov. Dále řešení PIM bude obsahovat jeden přístupový bod v HC Nagano/Chodov, který bude rovněž zajišťovat nahrávání uživatelských relací a řízení přístupu k EP provozovaných v HC Nagano a HC Chodov. Všechny přístupové body budou nasazeny v režimu vysoké dostupnosti. Řešení vysoké dostupnosti přístupového bodu bude ve všech případech obsahovat minimálně dva samostatné přístupové servery a v případě HC Nagano/Chodov musí být tyto přístupové servery geograficky odděleny do jednotlivých datových center. Každý ze serverů sám zajistí požadované výkonnostní parametry.

Prostředí

V rámci dodávky je dodávána instalace dvou prostředí PIM:

- Produkční
- Vývojové/Testovací

Vývojové/testovací prostředí bude sloužit k testování patchů a nových verzí systému dodaných výrobcem. Zároveň v něm bude probíhat vývoj a testování funkcionalit v rámci rozšiřování systému (konektory, skripty pro automatizované přihlašování, schvalovací WF, integrace, atp.).

Testovací/vývojové prostředí musí zajistit všechny požadované funkční parametry jako prostředí produkční a bude obsahovat minimálně po jedné z komponent použité v produkčním prostředí.

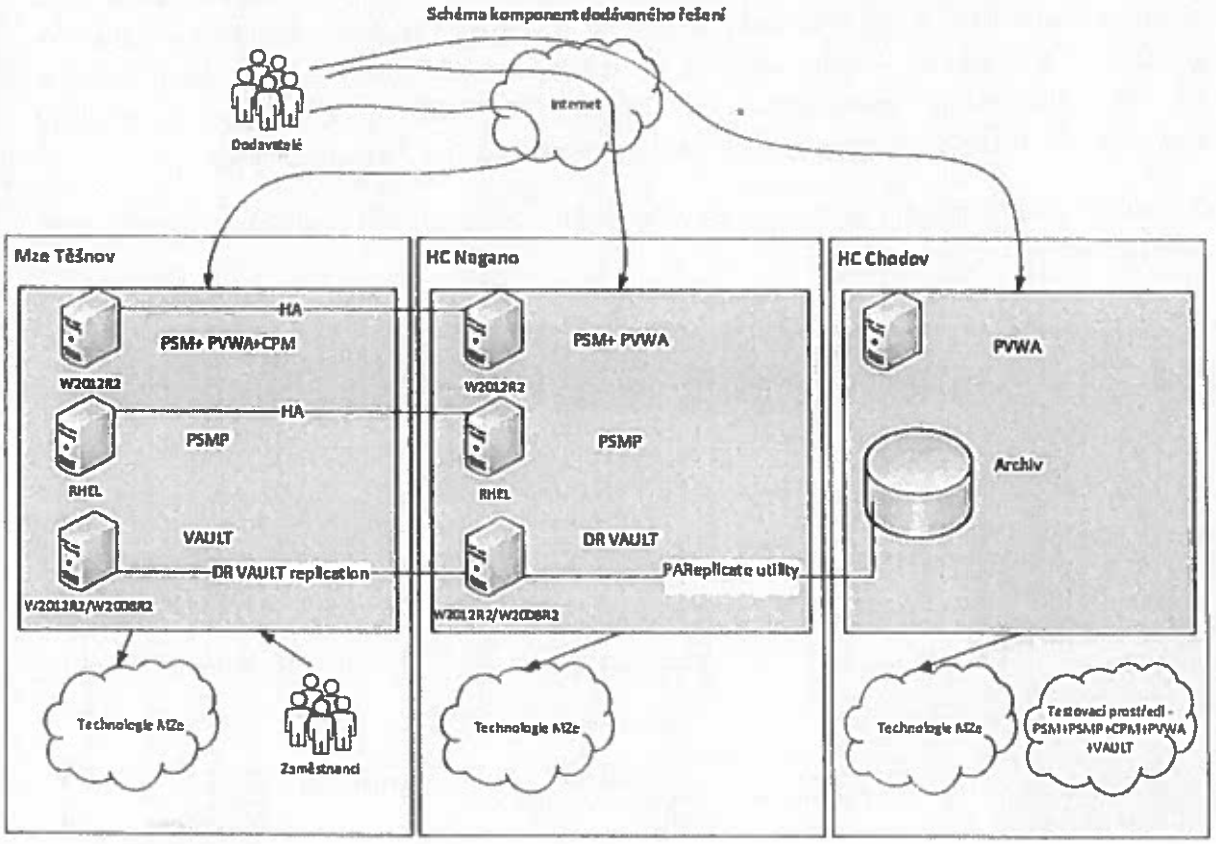
Všechny změny v rámci PIM řešení, zejména upgrade, bezpečnostní záplaty, nové funkcionality a další nové verze PIM řešení nebo jeho částí, se Dodavatel zavazuje řádně otestovat, ještě před nasazením do produkčního prostředí Objednatele.

Požadavky na kapacity virtualizačního prostředí, které vyplývají z níže uvedeného schématu dodávaného řešení:

- 2 × VAULT: 1 × Quad core processor (Intel compatible) 8GB RAM, 80GB diskového prostoru, síťový adapter 1GB

- 1 × PSM+PVWA+CPM: 2 × Quad core processor (Intel compatible) 16 GB RAM, 120 GB diskového prostoru, síťový adapter 1GB
- 2 × PSMP: 1 × Quad core processor (Intel compatible) 8GB RAM, 80GB diskového prostoru, síťový adapter 1GB
- 1 × PSM+PVWA: 1 × Quad core processor (Intel compatible) 8GB RAM, 80GB diskového prostoru, síťový adapter 1GB
- 1 × PVWA: 1 × Quad core processor (Intel compatible) 4GB RAM, 80GB diskového prostoru, síťový adapter 1GB

V rámci zajištění archivace dat, bude potřeba počítat s dodatečnou kapacitou 2TB zálohovacího prostoru.



Vysoká dostupnost

Všechny HA prostředky řešíme v rámci dodávky řešení. Nespoléháme tak v rámci dodávaného řešení na schopnosti virtuálního prostředí.

Fáze realizace dodávky

Analýza

Dodavatel v rámci dodávky provede nejprve analýzu nezbytnou pro instalaci a konfiguraci komponent PIM řešení, integraci všech požadovaných typů EP a připraví technický popis řešení, instalační postup, detailní časový harmonogram a definuje nároky na součinnost. Na základě požadavků na PIM řešení Dodavatel připraví návrh testovacích scénářů, pokrývajících testování všech funkčních rysů implementovaného řešení, včetně testování vybraných výkonových parametrů a výpadků jednotlivých komponent. Dále Dodavatel připraví návrh integrace PIM řešení do provozního a bezpečnostního (SIEM) monitoring systému Objednatele.

Všechny požadované výstupy z etapy Analýza budou Objednateli předloženy k odsouhlasení.

Instalace

Instalace řešení PIM bude provedena do vyhrazené bezpečnostní infrastruktury Objednatele, která je založena na virtuální platformě VMware a je distribuována přes obě datová centra (geocluster DC Nagano a DC Chodov) a lokalitu Těšnov. SW prostředky dodané v rámci řešení PIM budou instalovány v poslední verzi dostupné v době plnění. V rámci dodávky bude zajištěno nasazení a aktivace všech licencí a licenčních klíčů. Architektura instalovaného PIM řešení, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace.

V rámci instalace jsou definovány následující parametry komunikačních tras a síťových prostupů mezi jednotlivými komponentami řešení PIM.

Target / Source	Vault	DR	CPM	PVWA
Vault	x	TCP/1858 [1]	x	x
Disaster Recovery Vault (DR)	TCP/1858 [1]	x	x	x
Central Policy Manager (CPM)	TCP/1858 [1]	TCP/1858 [1]	x	x
Password Vault Web Access (PVWA)	TCP/1858 [1]	TCP/1858 [1]	x	x
Privileged Session Manager (PSM)	TCP/1858 [1]	TCP/1858 [1]	x	x
Application Identity Manager (AIM)	TCP/1858 [1]	TCP/1858 [1]	x	x
On-Demand Privileges Manager (OPM)	TCP/1858 [1]	TCP/1858 [1]	x	x
User (Administrator)	TCP/1858 [1], opt Remote Administration [2]	TCP/1858 [1], opt. Remote Administration [2]	TCP/3389	TCP/80 TCP/443 TCP/3389

Target / Source	PSM	AIM	OPM	SMTP Server (for Event Notification)	Manage Target Devices, e.g. Server, Router, ...
Vault	x	x	x	TCP/25	x
Disaster Recovery Vault (DR)	x	x	x	TCP/25	x
Central Policy Manager (CPM)	x	x	x	x	See footnotes below [3]
Password Vault Web Access (PVWA)	x	x	x	x	x
Privileged Session Manager (PSM)	x	x	x	x	TCP/3389 or TCP/22
Application Identity Manager (AIM)	x	x	x	x	x
On-Demand Privileges Manager (OPM)	x	x	x	x	x
User (Administrator)	TCP/443 TCP/3389	x	x	x	TCP/22, TCP/3389, etc [4]

[1] Výchozí port, lze jej změnit na jiný (444 atd.)

[2] Vzdálená správa HW pomocí HP iLO, IBM RSA, Dell DRAC atd.

[3] Standardní porty služeb, aplikací a operačních systémů

[4] V závislosti na zařízeních spravovaných prostřednictvím přímého přístupu

Implementace

V rámci fáze implementace bude Dodavatelem zajištěna konfigurace PIM řešení tak, aby řešení vyhovovalo požadavkům uvedeným v Technické specifikaci.

Jako součást dodávky bude provedeno:

- Konfigurace komponent PIM řešení;
- Navržení a nasazení mechanizmu vynucování a kontroly přístupu k EP výhradně přes nahrávaný kanál;

- Integrace následujících EP:

	Název systému	Počet	Přístup/Aplikace
1.	Red Hat Enterprise Linux 6 (64-bit)	1	SSH
2.	HP-UX 11i v3	1	SSH
3.	Microsoft Windows Server 2012 (64-bit)	1	WMI/RDP
4.	Microsoft Windows Server 2008 R2 (64-bit)	1	WMI/RDP
5.	Firewall Fortinet FortiGate	1	SSH/Web
6.	Switch HP 7500 (SSH)	1	SSH
7.	Switch Cisco Catalyst 4500 (Telnet)	1	Telnet
8.	Oracle RAC database 11g (11.2.0.3)	1	SQL
9.	Microsoft SQL Server 2008 R2 SP1	1	SQL
10.	Microsoft ActiveDirectory	1	RDP/LDAP(s)
11.	LDAP (Oracle Internet Directory)	1	LDAP(s)
12.	VMWare ESXi 5.1.0	1	vSphere
13.	Webová aplikace – vyplyne z analýzy	2	Web
14.	SAP – vyplyne z analýzy	1	Web/SAP klient
15.	Aplikace/systémy podporované PIM řešením, které vyplynou z analýzy	2	

- Vytvoření politik v souladu s bezpečnostní politikou Objednatele;
- Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup;
- Vytvoření procesu pro nouzový přístup k EP v případě celkového nebo částečného výpadku PIM řešení;
- Integraci PIM řešení do provozního a bezpečnostního monitoringu provede Objednatel za součinnosti Dodavatele;
- Nastavení zálohování konfigurace a dat PIM řešení;

Akceptační testy

V rámci analytické fáze budou Dodavatelem navrhnuty testovací scénáře, které budou pokrývat požadované oblasti a parametry řešení dle Technické specifikace.

Dokumentace

Dokumentace dodaná v rámci řešení bude obsahovat jak originální dokumentaci dodávanou výrobcem PIM řešení, tak i dokumenty popisující nasazení PIM řešení v prostředí Objednatele.

Oficiální dokumentace výrobce produktu k PIM řešení bude předána v elektronické podobě (formát PDF nebo MS Word) a bude provedena anglickém jazyce. Dokumentace od výrobce bude pokrývat následující oblasti:

- popis architektury;
- instalace řešení;
- administrace řešení;

- uživatelská příručka;

Dokumentace popisující nasazení PIM řešení v prostředí Objednatele bude předána v elektronické podobě ve formátu MS Word a bude provedena v českém jazyce a bude respektovat požadavky na rozsah a obsah dodávané dokumentace dle Technické specifikace.

Školení

Dodavatel zajistí proškolení 3 osob Objednatele na úrovni administrace řešení v rozsahu umožňujícím provádět:

- Běžný rutinní provoz a údržbu dodávaného PIM řešení, včetně provedení příslušných konfiguračních změn;
- Řešení obvyklých problémů;
- Správu uživatelských oprávnění;
- Integraci EP;
- Analýzu zaznamenaných uživatelských relací;
- Monitoring stavu zařízení;
- Zálohování a obnovu konfigurace a dat;
- Tvorbu pohledů a reportů;

TOTO JE ELEKTRONICKÁ VERZE NÁVRHU SMLOUVY VE FORMÁTU WORD.

V KOMPLETNÍ NABÍDCE VE FORMÁTU PDF, BUDU NA TOMTO MÍSTĚ VLOŽENY:

- EXCELOVSKÁ TABULKA – PŘEHLED FUNKČNÍCH POŽADAVKŮ – dokument je přiložen k nabídce jako příloha pdf souboru
- PROHLÁŠENÍ VÝROBCE, ŽE NABÍZENÉ ŘEŠENÍ JE URČENO PRO ČESKÝ TRH – tento dokument je jen součástí nabídky, není samostatně přiložen

CYBERARK

Za společnost CyberArk potvrzuji, že nabízené produkty v rámci výběrového řízení pro Ministerstvo zemědělství s názvem „Správa a monitoring privilegovaných účtů - PIM" jsou určeny pro český trh.

Dále potvrzujeme, že společnost Corpus Solutions a.s. je oprávněna tento produkt dodávat pro Ministerstvo zemědělství.

Daniel Hetényi

Daniel Hetényi

Regionálny obchodný manažér
Cyber-Ark Software Ltd. (skrátene CyberArk),
Daniel.Hetenyi@cyberark.com
+421 911 037 137

MINISTERSTVO ZEMĚDĚLSTVÍ

Specifikace katalogových listů

Správa a monitoring privilegovaných účtů – PIM

OBSAH

1. PŘEHLED ZÁKLADNÍCH POJMŮ

Termín	Význam
Celková měsíční cena	Součet paušálních měsíčních cen za katalogové listy, u kterých je placena paušální měsíční cena
Člověkoden	Představuje 8 hodin práce jednoho pracovníka
Helpdesk	Specializované oddělení zajišťující komplexně uživatelskou podporu
Check-out/check-in hesla	funkce umožňující získání (check-out) hesla ke spravovanému privilegovanému účtu na základě oprávnění uživatele (a následné oznámení o konci jeho využití – check-in)
ITSM	IT service management – řízení úrovně poskytovaných Služeb především, nikoliv však výhradně, v rozsahu doporučeném ITIL
KL	katalogový list
KPI	výkonnostní parametr, hodnotící parametr Služby
Maintenance	Služby a aktivity, poskytované výrobcem Systému nebo jeho komponent, potřebné pro udržení Systému v provozuschopném stavu v souladu s dohodnutými parametry a zajišťující kompatibilitu Systému s komponentami ICT Objednatele.
MZe	Česká republika - Ministerstvo zemědělství
Objednatel, Zadavatel	osoba, která je jako Objednatel definovaná v záhlaví Smlouvy
Obnovení služby (fix time)	Je časová lhůta, ve které je Zhotovitel povinen realizovat požadovanou činnost nebo obnovit parametry Služby, resp. Systému, na sjednanou úroveň s tím, že doba obnovení parametrů Služby, resp. Systému, je počítána od vzniku původního požadavku bez ohledu na změnu priority požadavku
Odezva (response time)	Je časová lhůta, ve které je Zhotovitel povinen odpovědět na požadavek předaný prostřednictvím Service Desku Objednatele, a to buď odmítnutím, nebo přijetím požadavku
PIM	Privileged Identity Management - správa privilegovaných identit/účtů
Pracovní den	každý den mimo sobot, neděl a státních svátků a ostatních svátků dle zákona č. 245/2000 Sb., o státních svátcích, o významných dnech a o dnech pracovního klidu, ve znění pozdějších právních předpisů
Pracovní doba nebo Kalendář	doba, kdy je Služba poskytována – od-do, které dny v týdnu, počet minut pro potřeby výpočtu dostupnosti: 10x5 – Pracovní dny od 8:00 do 18:00 hodin 24x7 – nepřetržitě
Provozní deník	dokumentace obsahující náležitosti uvedené v kapitole 2.2.1 této přílohy č. 2 Smlouvy
Rozhraní Systému	integrační a komunikační rozhraní Systému prezentované vnějším rozhraním hraničního (posledního) aktivního síťového prvku pod správou Zhotovitele, tvořícího rozhraní mezi sítí Zhotovitele a vnější komunikační infrastrukturou
Service Desk (SD)	Nástroj pro podporu řízení služeb
Servisní okno	časový interval definovaný Objednatelem a zakotvený v dokumentaci MZe
SLA	sjednaná úroveň poskytované Služby
Služba	služba Podpory definovaná v jednotlivých KL

Smlouva	Smlouva o poskytnutí řešení „Správa a monitoring privilegovaných účtů – PIM" uzavřená mezi Objednatelem a Zhotovitelem
SSO (Single-Sign-On)	systém jednotného přihlášení umožňující autentizaci do dalších systémů na základě jednoho přihlášení bez nutnosti dalšího zadávání přístupových údajů
SW	software, aplikace – program, programové vybavení nebo jeho komponenta
Standardní SW (SSW)	softwarové vybavení třetích stran dodané v rámci Smlouvy, na základě kterého byl zhotoven Systém, které nebylo vyvinuto Zhotovitelem a není aplikační SW komponentou Systému vyvinutou v rámci Smlouvy
Systém	řešení PIM, předmět dodávky
Zhotovitel	osoba, která je jako Zhotovitel definovaná v záhlaví Smlouvy

2. PODMÍNKY POSKYTOVÁNÍ SLUŽEB SYSTÉMU

2.1. Obecné podmínky

Zhotovitel je povinen bezplatně poskytnout součinnost pro MZe související s odbornými, zákonnými a jinými kontrolami a audity, které mohou být uplatňovány vůči MZe v souvislosti s dodávkou služeb a Systémem jako takovým.

Veškeré výkazy, podklady a dokumenty musí být ve formě, umožňující přezkoumatelnost a auditovatelnost ze strany kontrolních organizací, kterými se rozumí veškeré subjekty oprávněné provádět kontrolu jakkoliv týkající se plnění této Smlouvy na základě právního předpisu. Pokud je dokument, výkaz nebo jiný podklad, související s tímto dokumentem zpochybněn kontrolní organizací, je Zhotovitel povinen poskytnout podklady, které budou kontrolním orgánem akceptovány. V případě, že Zhotovitel nebude schopen tyto podklady dodat a/nebo tyto nebudou kontrolním orgánem akceptovány a pokud absence těchto dokumentů bude důvodem k udělení sankce vůči MZe, Zhotovitel poskytne náhradu ve výši sankce, uplatněné vůči MZe, a to i po uplynutí účinnosti této Smlouvy, pokud se sankce bude týkat období trvání Smlouvy.

Zhotovitel je před zahájením dodávky Služby Objednateli povinen dodat písemný seznam komponent Systému, které kategorizuje jako standardní software, krabicový software případně software třetích stran a takto označit i odpovídající položky konfigurační databáze Objednatele.

Všechny úpravy, funkcionality, programové kódy, konfigurace apod., které Zhotovitel neoznačí jako standardní software a/nebo které vznikly v průběhu platnosti Smlouvy, jsou považovány za vlastnost Systému, kterou může Objednatel kdykoliv na základě vlastního uvážení využít v jiných informačních systémech a libovolně upravovat bez jakýchkoliv licenčních závazků vůči Zhotoviteli nebo třetím stranám. Tím nejsou dotčena práva Objednatele ani povinnosti Zhotovitele dle Smlouvy.

Pokud je zjištěno podávání nepravdivých dat a výkazů Zhotovitelem, je celé měřicí období, ve kterém bylo toto zjištěno, považováno za nesplněné ve všech parametrech, u kterých bylo toto pochybení zjištěno. Vyplývající slevy jsou aplikovány na každý parametr zvlášť v maximálním rozsahu stanoveném touto Smlouvou.

Zhotovitel je povinen se řídit zákonnými, technickými a jinými požadavky, pravidly a doporučeními, souvisejícími se zajišťovanými službami, spravovanou nebo využívanou infrastrukturou a využívanými nebo poskytovanými službami, které nejsou předmětem tohoto dokumentu.

Ústní jednání v souvislosti s předmětem dodávky / plnění definovaným Smlouvou nemá povahu jakéhokoliv závazku.

2.2. Dokumentace

Veškerá infrastruktura, která je předmětem dodávky Služeb, bude dokumentována. Zhotovitel zajistí aktualizaci při každé změně, provedené Zhotovitelem. Pokud dokumentace neexistuje, Zhotovitel ji v potřebném rozsahu vytvoří. Dokumenty dokumentace mají v úvodní sekci seznam změn, ve kterém jsou stručně shrnuty změny provedené od předchozího vydání dokumentace. Dokumentace zahrnuje zejména, nikoliv však výhradně následující položky:

- hlavní komponenty PIM řešení na úrovni celků, na které lze aplikovat změnu ve smyslu doporučení ITIL;
- veškeré licence včetně volně šiřitelných a neplacených licencí;
- vazby mezi komponentami PIM řešení na úrovni fyzické, logické, datové, dodávky služeb;
- uživatelskou dokumentaci;
- bezpečnostní dokumentaci;
- administrátorskou dokumentaci;
- zálohovací plány a postupy;
- opatření a dokumentace k zajištění kontinuity provozu (vč. plánů obnovy PIM řešení);
- postupy pro obnovení dat včetně konfigurací do původního provozního stavu;
- konfigurace aplikací a případně jejich komponent;
- seznamy použitých softwarových komponent a standardního SW včetně jejich verzí;
- všechny programové kódy, vzniklé jako předmět dodávky, kromě Standardního SW;
- všechny programové kódy, vzniklé nebo změněné v průběhu platnosti Smlouvy;
- konfigurace a artefakty, nezbytné pro sestavení programových komponent z programových kódů;
- Provozní deník;

2.2.1. Provozní deník

Zhotovitel je povinen při poskytování Služeb dle této Smlouvy vést Provozní deník. Provozní deník bude veden jeden pro celý Systém.

Zhotovitel je povinen do Provozního deníku prostřednictvím záznamu zaznamenat minimálně následující události a to nejdéle do 4 hodin od provedení změny:

- Provedení úkonů předepsaných v KL včetně identifikace příslušného KL;
- Havarijní stavy, opravy, výměny komponent;
- Anomálie a nestandardní stavy systémů, které mají dopad na plnění SLA;
- Zprovoznění nového nebo dočasně odstaveného systému a/nebo odstavení systému;
- Spuštění, vypnutí a restart systému;
- Obnovení ze zálohy.

Každý záznam bude obsahovat minimálně následující informace:

- Datum a čas pořízení záznamu;
- Identifikace osoby pořizující záznam;
- V případě událostí trvajících více než 1 hodinu také čas začátku a konce události;
- Popis události.
- Provedené úkony k události s uvedenými časy provedení
- Zdůvodnění, na základě jakého požadavku byla činnost vykonána (např. ID záznamu v Service Desku Objednatele, číslo Smlouvy a příslušný KL).

Pro vyloučení pochybností se uvádí, že Provozní deník není systémovou dokumentací. Při realizaci změny se do Provozního deníku zapisuje, že byla provedena změna a její stručný popis. Popis změny, resp. nově vzniklý stav a konfigurace systému jsou detailně popisovány v systémové dokumentaci. Pro vyloučení pochybností se uvádí, že změnou se myslí jakákoliv změna ve smyslu „Change management" podle ITIL.

Způsob vedení Provozního deníku není předepsán. Zhotovitel je oprávněn vést Provozní deník v elektronické podobě, avšak tak, aby byl pro Objednatele a jeho pracovníky kdykoliv přístupný a bylo možno z něj provádět kopie, přehledy a exporty dat.

Objednatel připouští vedení jednotného Provozního deníku pro všechny KL. V takovém případě každý záznam obsahuje také identifikaci KL, ke kterému se vztahuje.

2.3. Změny v Systému provedené Objednatelem

Objednatel je oprávněn provádět změny (administrovat) v Systému pomocí standardního rozhraní Systému (např. přidávat/odebírat uživatele, přidávat/odebírat koncové systémy na kterých je Systémem řízen přístup, zálohovat Systém, apod.) do míry, na kterou je Systém Zhotovitelem nadimenzován na základě informací uvedených v Technické specifikaci. Tyto změny nijak neovlivní povinnosti Zhotovitele dané katalogovými listy.

V případě jiných změn (např. instalace SW na přístupový bod) realizovaných za účinnosti Smlouvy je Objednatel povinen nechat si takovouto změnu schválit Zhotovitelem, který tak vyhodnotí dopady na funkčnost Systému. V případě neakceptace změny Zhotovitelem, musí zhotovitel navrhnout jiné řešení, které bude mít na Systém stejný účinek. Provedení změn Objednavatelem podle postupu schváleného Zadavatelem nezbavuje Zhotovitele povinností ze zajištění parametrů služeb definovaných v KL.

3. SLEVA Z CENY A SMLUVNÍ POKUTY

Slevy z ceny za nedodržení celkové dostupnosti a za nedodržení Obnovy služby vzniklé v souvislosti se stejným incidentem lze kumulovat.

Zhotovitel není v prodlení s plněním povinnosti, na jejíž porušení se sleva z ceny nebo smluvní pokuta vztahuje, a to po dobu, pro kterou prokáže, že za porušení povinnosti Zhotovitel neodpovídá (např. prokázána příčina ležící mimo Systém).

Uplatnění slevy z ceny nebo smluvní pokuty nemá vliv na povinnost poskytování Služeb ve sjednaných úrovních. Nárok na slevu z ceny Služeb nebo smluvní pokutu se nedotýká závazku Zhotovitele splnit povinnost, se kterou je v prodlení (pokud je to vzhledem k povaze předmětné Služby objektivně možné).

Objednatel má právo v případě porušení parametrů definovaných katalogovými listy na slevy z ceny nebo na smluvní pokuty ve výši stanovené v jednotlivých katalogových listech.

3.1. Uplatnění slevy z ceny služeb a možnost odstoupení od Smlouvy

Součet všech poskytnutých slev z ceny Služeb v daném měsíci se odečte od Celkové měsíční ceny všech poskytnutých Služeb za daný měsíc. Objednatel má za daný měsíc nárok na zaplacení ceny za poskytnuté Služby pouze ve výši takto vypočteného rozdílu.

V případě, že součet všech poskytnutých slev z ceny poskytnutých Služeb v daném měsíci je vyšší než Celková měsíční cena poskytnutých Služeb za daný měsíc, bude neuplatněný nárok na slevu z ceny Služeb uplatněn v dalším měsíci.

V případě, že výše neuplatněné slevy z ceny Služeb převýší součet cen Služeb za následující měsíce až do konce trvání Smlouvy, je Objednatel oprávněn od Smlouvy odstoupit. Objednatel je současně oprávněn před odstoupením od Smlouvy vyúčtovat Zhotoviteli částku odpovídající výši neuplatněné slevy z ceny Služeb jako smluvní pokutu.

Odstoupení od smlouvy nemá vliv na výši uplatněné slevy ani smluvní pokutu.

4. VYHODNOCOVÁNÍ KVALITY POSKYTOVANÝCH SLUŽEB

4.1. Měření Služeb

Objednatel bude provádět dostupnými prostředky kontrolu provádění činností dle katalogového listu. Pokud Objednatel identifikuje, že dotčená činnost nebyla vykonána nebo byla vykonána v rozporu

Priorita	Definice priority požadavku	Parametry řešení požadavku
Priorita 1 Kritická	Některé nebo všechny části PIM řešení selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost PIM řešení.	Odezva: 1 hodiny Obnovení služby: 4 hodin
Priorita 2 Vysoká	PIM řešení je funkční pouze částečně, PIM řešení je ovlivněno selháním nebo omezením některé z komponent nebo funkcí podporujících důležité činnosti PIM řešení.	Odezva: 2 hodin Obnovení služby: 10 hodin
Priorita 3 Střední	PIM řešení je funkční, závada nemá vliv na činnost PIM řešení. Vyskytují se nedostatky nepodstatné povahy, které způsobují například nekomfortnost obsluhy nebo zvyšující pracnost činností než v běžném provozu.	Odezva: 12 hodin Obnovení služby: 2 dny
Priorita 4 Nízká	Bezpečnostní hrozba, která má dopad na PIM řešení	Odezva: 24 hodin Obnovení služby: 3 dny
Priorita 5 Ostatní	Požadavkem je žádost o podání informace (dotaz, vysvětlení) nebo existence aktualizace či záplaty Systému. Priorita požadavku zároveň zahrnuje situace, kdy některé funkce prokazatelně selhaly, ale nejsou v daný moment využívány nebo nemají žádný vliv na řádný chod Systému, za předpokladu, že řešení požadavku závisí na součinnosti třetí strany mimo vliv Zhotovitele.	Odezva: 3 dny Obnovení služby: 15 dnů

5. SEZNAM KATALOGOVÝCH LISTŮ

5.1. PIM01 Odezva

Katalogový list služby	
Identifikace (ID)	PIM01
Název Služby	Odezva
Popis Služby	Zajištění odezvy služeb, funkcí a dat řešení PIM.
Parametry	
Název	KPI01 Odezva
Definice	Zajištění dostupnosti Služby • Obnovení funkcí PIM řešení či některé z jeho komponent podle priorit definovaných v 4.3.1 Priority pro provozní prostředí;
Parametry KPI	
Kalendář služby	24x7
Odezva	Viz 4.3.1 Priority pro provozní prostředí
Obnovení služby	Viz 4.3.1 Priority pro provozní prostředí
Definice parametrů	Odezva Systému je definována následovně: 1. Je možné se úspěšně přihlásit do všech komponent Systému a na přístupové body. • Funkce přihlášení se do Systému se považuje za dostupnou, pokud se uživateli zobrazí kompletní uživatelské rozhraní Systému (dále jen „Odezva systému na přihlášení") do 5 vteřin od potvrzení přihlašovacích údajů, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem; • Pokud je Odezva Systému na přihlášení v intervalu od 5 do 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován jako závada Priority 3; • Pokud je Odezva Systému na přihlášení delší než 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, nebo pokud se není možné do Systému přihlásit, je tento stav považován jako závada Priority 1; 2. Po přihlášení do Systému jsou uživateli k dispozici všechny jemu přiřazené funkce/zdroje/role/účty/nástroje; • Pokud má uživatel po úspěšném přihlášení k dispozici pouze některé nikoliv všechny jemu přiřazené funkce/zdroje/role/účty/nástroje, jedná se o závadu Priority 2; • Pokud uživatel nemá po úspěšném přihlášení k dispozici žádné jemu přiřazené funkce/zdroje/role/účty, jedná se o závadu Priority 1; 3. Funkce „check-out/check-in" hesel poskytuje funkční heslo k řízenému účtu; • Funkce „check-out/check-in" hesel se považuje za dostupnou, pokud Systém poskytne funkční heslo k řízenému účtu do 5 vteřin od potvrzení operace typu „check-out" nebo „check-in" (dále jen „Odezva na „check-out/check-in"), kde tato doba zahrnuje pouze zpoždění

	zapříčiněné Systémem; • Pokud je Odezva na check-out/check-in Systému v intervalu od 5 do 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován za závadu Priority 3; • Pokud je Odezva na check-out/check-in Systému delší než 10 vteřin, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, nebo pokud Systém neposkytuje funkční heslo k řízenému účtu, je tento stav považován jako závadu Priority 1; 4. Přihlášení prostřednictvím SSO na cílový Systém je funkční pro všechny typy dostupných podporovaných zařízení/rozhraní; • Pokud dojde k úspěšnému přihlášení pomocí SSO realizovaného Systémem od okamžiku požadavku na přihlášení do doby o maximálně 3 vteřiny delší, než je doba trvání úspěšného přihlášení realizované mimo Systém, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován za dostupnost funkce přihlášení pomocí SSO; • Pokud dojde k úspěšnému přihlášení pomocí SSO realizovaného Systémem od požadavku na přihlášení do doby delší o více než 3 vteřiny, ale zároveň kratší než 10 vteřin, než je doba trvání úspěšného přihlášení realizované mimo Systém, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován za závadu Priority 3; • Pokud dojde k úspěšnému přihlášení pomocí SSO realizovaného Systémem od doby požadavku na přihlášení do doby delší než 10 vteřin, oproti době trvání úspěšného přihlášení realizované mimo Systém, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem, je tento stav považován za závadu Priority 1; • Pokud nedojde k úspěšnému přihlášení pomocí SSO, je tento stav považován za závadu Priority 1; 5. Systém nemá zaznamenatelný vliv na odezvy činností realizovaných v rámci probíhající uživatelské relace; • Pokud je vliv Systému na odezvu činnosti realizované v rámci probíhající uživatelské relace zaznamenatelný (pomalé překreslování oken, zpoždění uživatelských vstupů, apod.), jedná se o závadu Priority 2; 6. Systém zaznamenává/nahrává uživatelské relace na koncových systémech a zaznamenává/ukládá metadata těchto relací; • Funkce zaznamenávání/nahrávání uživatelských relací se považuje za dostupnou, pokud jsou veškeré relace uživatelů kompletně zaznamenány/nahrány, a to od okamžiku přihlášení uživatele na koncový systém, až do jeho odhlášení z koncového systému, a zároveň jsou zaznamenány/nahrány veškeré činnosti, které uživatel během relace provedl; • V opačném případě se jedná o závadu Priority 1;

	7. Zaznamenané/nahrané uživatelské relace je možné přehrát; • Funkce přehrání uživatelské relace se považuje za dostupnou, pokud jsou všechny zaznamenané/nahrané uživatelské relace dostupné pouze na základě přiděleného oprávnění, je možné spustit jejich přehrání, během kterého je možné identifikovat všechny činnosti, které uživatel během relace provedl; • V opačném případě se jedná o závadu Priority 3; 8. U zaznamenaných/nahraných uživatelských relací je zachována integrita; • Jakákoliv změna zaznamenané/nahrané relace je detekovatelná; • V opačném případě se jedná o závadu Priority 3; 9. Systém audituje jak veškeré operace uživatelů, administrátorů v rámci Systému, tak i interní operace Systému samotného; • Funkce auditování operací se považuje za dostupnou, pokud je auditní záznam o operaci v Systému zaznamenán a zároveň dostupný ke kontrole do 5 vteřin po provedení příslušné činnosti, kde tato doba zahrnuje pouze zpoždění zapříčiněné Systémem; • V opačném případě se jedná o závadu Priority 3; 10. Systém generuje reporty; • Funkce generování reportů se považuje za dostupnou, pokud reporty zobrazují kompletní data Systému a výstup reportu je k dispozici za adekvátní dobu s ohledem na složitost reportu; • V opačném případě se jedná o závadu Priority 3;
Způsob výpočtu a měření	Jako směrodatné a závazné pro Zhotovitele se pro měření uvedených parametrů odezvy Systému berou hodnoty naměřené dohledovým systémem Objednatele. V případné zjištění nedostupnosti, nefunkčnosti či omezení funkce Systému je tento stav zaznamenán do Service Desku Objednatele. Pracovníci Helpdesku Objednatele následně kontaktují kanálem, definovaným Smlouvou (email, telefon, Service Desk Objednatele), technickou podporu Zhotovitele a o tomto kontaktování provedou záznam do tiketu v Service Desku Objednatele jako počátek nedostupnosti Služby.
Měřicí bod	Service Desk Objednatele.
Způsob dokladování	Měsíční report o plnění KPI.
Sleva z ceny	Jednorázová sleva z ceny ve výši 10.000,- Kč v případě porušení dohodnuté doby pro Obnovení služby viz tabulka Priorit v kapitole viz 4.3.1 Priority pro provozní prostředí a zároveň další sleva z ceny ve výši 2500 Kč za každou započatou hodinu nad dohodnutou dobu pro Obnovení služby viz tabulka Priorit v kapitole 4.3.1 Priority pro provozní prostředí.
Doplňující informace	
Poznámka	-
Platební podmínky	Paušální měsíční cena podle Smlouvy.

5.2. PIM02 Maintenance

Katalogový list služby

Identifikace (ID)	PIM02
Název Služby	Maintenance
Popis Služby	Technická podpora produktu
Parametry	
Název	KPI02 Maintenance
Definice	Zajištění technické podpory směrem k výrobci dané nárokem platné Maintenance na komponenty PIM řešení.
Parametrizační	
Kalendář služby	10x5
Odezva	Podle Priority 3
Obnovení služby	Podle Priority 3
Definice parametrů	Přímý přístup Objednatele a Zhotovitelem zprostředkovaný přístup ke službám, souvisejících s Maintenance, všech výrobců všech komponent Systému. Jedná se zejména, nikoli však výhradně, o tyto služby: • přístup a možnost využití kontaktního místa podpory výrobce • možnost zadávat požadavky, související se zajištěním provozuschopnosti a aktualizacemi Systému • možnost získávání všech typů aktualizací a opravených verzí • přístup do znalostní báze daného výrobce • užívání všech výhod a služeb, které výrobce v rámci Zhotovitelem poskytnutého typu Maintenance poskytuje • zajištění všech informací a součinností, vyžadovaných výrobcem v souvislosti s poskytováním Maintenance a podpory Tyto služby jsou hrazeny tímto KL a Objednateli nevznikne uplatněním požadavku u výrobce v rámci KL PIM02 žádný dodatečný náklad. Veškeré podklady související se zajištěním Maintenance (licence, přístupové údaje na portály výrobců, kontaktní údaje na kontaktní místa výrobce – email, telefon, apod.) budou předány Objednateli a Zhotovitel bude zajišťovat jejich aktuálnost směrem k Objednateli po celou dobu účinnosti Smlouvy.
Způsob výpočtu a měření	Kontrola dostupnosti služeb výrobců, souvisejících s KL PIM02. Počátkem nedostupnosti je čas záznamu v Service Desku Objednatele, kterým oznamuje Zhotoviteli nedostupnost služeb pro každou Maintenance pro každou komponentu Systému. Doklady, prokazující platnost Maintenance a podpory na vyžádání a/nebo při změně (vč. obnovení) smluv s výrobcem. Nesmí dojít k nezajištění Maintenance a podpory.
Měřicí bod	Service Desk Objednatele.
Způsob dokladování	Záznam v Service Desku Objednatele.
Smluvní pokuta	Objednatel má právo na uhrazení smluvní pokuty ve výši 10.000,- Kč za každý případ porušení povinnosti Zhotovitele zajistit Maintenance v souladu s tímto katalogovým listem v daném měsíci (tzn. Maintenance nebude zajištěna vůbec nebo bude zajištěna v rozporu se sjednanými parametry). Objednatel má dále právo na smluvní pokutu 10.000,- Kč za každý případ porušení parametru Obnovení služby pro kteroukoliv

	z činností definovaných výše v rámci Definice parametrů.
Doplňující informace	
Poznámka	Doba poskytování služby Maintenance je určena ve Smlouvě.
Platební podmínky	Paušální roční platba za Maintenance produktu/produktů PIM řešení.

5.3. PIM03 Správa PIM

Katalogový list služby	
Identifikace (ID)	PIM03
Název Služby	Správa PIM řešení.
Popis Služby	Zajištění správy všech komponent dodaného PIM řešení.
Parametry	
Název	KPI03 Správa PIM
Definice	Správa PIM řešení zahrnuje především, nikoliv však výhradně, následující činnosti: • Provoz a správa všech komponent PIM řešení (SW, OS) • Profylaktické činnosti • Kontrola výkonnosti PIM řešení a návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře IS MZe • Identifikace aktualizací relevantních k prostředí Objednatele, ověření jejich dopadů v prostředí Objednatele a jejich aplikace na Systém Objednatele; • Aplikace schválených aktualizací na Systém • Posouzení dopadu nových aplikací požadovaných k instalaci na přístupové servery pro zajištění správy technologií v prostředí MZe
Parametry KPI	
Kalendář Služby	10x5
Odezva	Viz 4.3.1 Priority pro provozní prostředí
Obnovení služby	Viz 4.3.1 Priority pro provozní prostředí
Definice parametrů	• Sledování, identifikace, posouzení dopadů, poskytnutí stanoviska k nasazení a aplikace bezpečnostních aktualizací na Systému. Bezpečnostní aktualizace je aktualizace uvolněná výrobcem řešení pro produkční nasazení, která řeší bezpečnostní slabinu či zranitelnost řešení, zde se jedná o požadavek Priority 4; • Sledování, identifikace, posouzení dopadů, poskytnutí stanoviska k nasazení a aplikace aktualizací či záplat Systému. Zde se jedná o požadavek Priority 5. • Posouzení dopadu nových aplikací požadovaných k instalaci na přístupové servery pro zajištění správy technologií v prostředí MZe dle Priority 4 (viz 2.3 Změny v Systému provedené Objednatelem)
Způsob výpočtu a měření	V případné vydání nové aktualizace/opravného balíku/nové verze SW výrobcem založí Zhotovitel požadavek do Service Desku Objednatele informující o této skutečnosti. Zhotovitel je povinen požadavek založit nejdéle do doby dané jako Odezva pro příslušnou prioritu požadavku, od vydání aktualizace výrobcem (např. zveřejnění na portálu výrobce, informační email výrobce, apod.). Požadavek může rovněž založit Objednatel, pokud tuto skutečnost zjistí dříve, kdy následně Helpdesk Objednatele

	informuje o této skutečnosti domluveným kanálem (email, telefon, Sevice Desk Zhotovitele) technickou podporu Zhotovitele. Do doby pro Obnovení služby dané prioritou požadavku počítané od okamžiku zveřejnění informace výrobcem musí Zhotovitel poskytnout stanovisko pro vhodnost nasazení v prostředí Objednatele s identifikací možných dopadů, definovat způsob nasazení a provést aplikaci aktualizace či záplaty.
Měřící bod	Service Desk Objednatele, informační kanál výrobce (portál, informační email, apod.)
Způsob dokladování	Měsíční report o plnění KPI.
Sleva z ceny	1000 Kč za každou započatou hodinu nad dobu pro Obnovení Služby stanovenou prioritou požadavku.
Doplňující informace	
Poznámka	-
Platební podmínky	Paušální měsíční cena podle Smlouvy.

5.4. PIM04 Reparametrizace a optimalizace

Katalogový list Služby	
Identifikace (ID)	PIM04
Název Služby	Reparametrizace, optimalizace a adaptace Systému pro jeho efektivnější využívání
Popis Služby	On-site asistence, optimalizace a provádění úprav Systému za účelem jeho efektivnějšího, bezpečnějšího a komplexnějšího využívání. Službou je zabezpečeno řešení požadavků na Systém, jejichž příčinou není incident (nefunkčnost).
Parametry	
Název	KPI04 Reparametrizace
Definice	V rámci této Služby jsou vykonávány zejména, nikoliv však výhradně, následující činnosti: • realizace rekonfigurací a drobných úprav vedoucích k efektivnějšímu, bezpečnějšímu a komplexnějšímu využívání Systému; • integrace nových koncových zařízení; • řádné zadokumentování provedených změn Služba bude poskytována podle požadavků Objednatele.
Parametry KPI	
Kalendář Služby	10x5
Definice parametrů	Odmítnutí nebo přijetí požadavku s definováním termínu jeho zapracování do 3 Pracovních dní. Dodržení stanoveného termínu ukončení realizace požadavku. Dodání měsíčního záznamu o poskytnutí Služby (viz níže v tomto KL).
Měřící bod	Service Desk MZe.
Způsob dokladování	Měsíční záznam o poskytnutí Služby s identifikací poskytnutých činností a služeb, rozpadu pracnosti, včetně elektronické verze záznamu ve standardním čitelném formátu. Minimální jednotkou pro dokladování pracnosti je hodina na jednoho člověka.

Smluvní pokuty	V případě porušení byť i jednoho parametru KPI04 má Objednatel právo na smluvní pokutu ve výši 10.000,- Kč za každé porušení povinnosti. Za porušení parametru KPI04 Zhotovitelem se považuje: 1. nedoručení přijetí nebo odmítnutí požadavku Objednatele do 3 Pracovních dnů; 2. v případě přijetí požadavku Objednatele a termínu jeho zapracování, nedodržení této doby zapracování požadavku včetně řádného zadokumentování provedených změn; 3. nedodání měsíčního záznamu o poskytnutí Služby se všemi požadovanými parametry (viz Způsob dokladování)
Doplňující informace	
Objem poskytované Služby	Objem, který je Objednatel oprávněn čerpat, činí 20 člověkodní za období jednoho roku po dobu trvání Podpory definované Smlouvou. Nevyčerpaný objem je převeden do následujícího ročního období. Čerpání bude probíhat podle aktuálních potřeb Objednatele.
Platební podmínky	V rámci tohoto katalogového listu budou hrazeny pouze reálně čerpané člověkohodiny podle sjednané sazby za člověkohodinu, a to do maximálního objemu definovaného tímto katalogovým listem. Úhrada bude provedena na základě odsouhlasené pracnosti (počet člověkohodin) a záznamu o poskytnutí Služby (Záznamu o poskytnutí služeb dle KL Reparametrizace a optimalizace). Minimální jednotkou pro dokladování pracnosti je hodina na jednoho člověka.

PŘÍLOHA Č. 3

TECHNICKÁ SPECIFIKACE

	Popis požadavku	Povinné	Váha	Splňuje
A.1.	Všechny komponenty systému (PIM řešení) jsou dostupné v českém nebo anglickém jazyce.	ANO	-	ANO
A.2.	PIM řešení je určené pro český trh (potvrzeno prohlášením výrobce). Poskytující zajistí v souvislosti s poskytováním záručního servisu registraci objednatele v příslušné databázi výrobce řešení tak, aby byl objednatel oprávněn k technické podpoře v České republice přímo ze strany tohoto výrobce či jeho servisních partnerů.	ANO	-	ANO
A.3.	Uživatelské rozhraní poskytující základní funkce je přístupné přes webové rozhraní s podporou prohlížeče • Internet Explorer ve verzi 10 a vyšší.	ANO	-	ANO
A.4.	Produkční prostředí je instalováno v režimu vysoké dostupnosti. Každá z komponent tedy musí obsahovat minimálně dvě samostatné instance provozované v HA módu active/active, nebo active/pasive. Řešení vysoké dostupnosti musí být plně automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro přepnutí mezi instancemi v případě vzniku chybového stavu, nejsou přípustná. Vysoká dostupnost musí být plně zajištěna na úrovni dodávaného PIM řešení, tedy buď na úrovni samotné aplikace a/nebo operačního systému. Pokud se nejedná o instalaci OS na fyzickém HW (tj. v případě použití virtualizace), dodávané řešení nesmí spoléhat na zajištění vysoké dostupnosti nástroji a prostředky virtualizační technologie.	ANO	-	ANO

A.5.	Autentizace uživatelského přístupu ke všem komponentám je řízena adresářem LDAP, nebo Active Directory.	ANO	-	ANO
A.6.	Autorizace uživatelského přístupu ke všem komponentám je řízena adresářem LDAP, nebo Active Directory (členství uživatelů ve skupinách).	NE	4	ANO
A.7.	K autentizaci je využit stávající SSO provider (Forgerock OpenAM), nebo automatické přihlášení na základě přihlášení k AD doméně (Integrated Windows Authentication).	NE	3	ANO
A.8.	PIM řešení loguje auditní záznamy o všech administrátorských a uživatelských aktivitách. Minimálně se logují následující typy událostí vykonaných v PIM: • úspěšné a neúspěšné (pokus o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo udělal jakou konfigurační změnu) • check-in/check-out hesla • přístup k nahrané session	ANO	-	ANO

A.9.	Řešení PIM je integrované se SIEM řešením HP ArcSight, které je provozováno v prostředí MZe. Auditní záznamy jsou logovány a dostupné bez prodlení od vzniku události alespoň jednou z následujících metod: • Syslog • SNMP TRAP • Textový soubor • JDBC • Microsoft Event Log	ANO	-	ANO
A.10.	Řešení PIM poskytuje reporty ve formátech PDF nebo MS Excel (XLS/XLSX). Minimálně následující reporty jsou v rámci dodaného řešení k dispozici: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty – check out/in, přidělení účtu, atp.	ANO	-	ANO
A.11.	Řešení PIM umožňuje naplánovat reporty k pravidelnému odesílání na email, nebo k ukládání do složky.	NE	3	ANO
A.12.	Součástí dodaného řešení PIM je uživatelský nástroj na vytváření nových reportů a jejich editaci.	NE	3	ANO
A.13.	Řešení PIM umožňuje definovat emailové notifikace na základě vybraných událostí.	NE	2	ANO

A.14.	Dodané PIM řešení zatěžuje sdílené prostředky v minimální míře. Pokud je tedy stejné funkcionality možné dosáhnout s významně nižším zatížením používaných prostředků, je aplikován právě tento přístup. Znamená to, že využívání sdílených prostředků musí být optimalizováno, pokud je to možné (např. nahrávky musí být při přenosu a ukládání komprimovány). Týká se tedy vytížení: • Integrovaných systémů/aplikací (přístupové body, řízené EP, LDAP/AD) • Systémových zdrojů (CPU, RAM, IOPS, apod.) • Síťové infrastruktury (např. při přenosu nahrávek)	ANO	-	ANO
A.15.	Řešení PIM podporuje správu EP přes přenosové cesty se sníženou propustností a spolehlivostí.	ANO	-	ANO
A.16.	Všechny komponenty dodaného řešení PIM jsou dostatečně zabezpečeny. Toho je dosaženo minimálně následujícími opatřeními: • je proveden hardening, • citlivá komunikace mezi komponentami, s externími systémy, nebo s uživateli je zabezpečena kryptografickými metodami, v rámci kterých jsou použity kryptografické algoritmy, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb. (Zákon o kybernetické bezpečnosti), nebo mezinárodně uznávaným standardem FIPS 140-2, • přístup k citlivým údajům a funkcím systému (jako jsou například hesla, nebo funkce změn heslo), je dostatečně chráněn pomocí kryptografických metod, v rámci kterých jsou použity kryptografické algoritmy, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb. (Zákon o kybernetické bezpečnosti), nebo mezinárodně uznávaným standardem FIPS 140-2, • v případě použití kryptografických metod, které nejsou v souladu s předchozími body, je možné implementovat dodatečná opatření, která jsou v souladu s předchozími body a zajistí dostatečnou ochranu ve smyslu předchozích bodů (např. slabě šifrovaná komunikace je posílána v IPSec tunelu, který je dodán jako součást řešení PIM)	ANO	-	ANO

A.17.	Systém podporuje rozšíření o modul na řízení přístupu (**Access Control**), tedy omezení oprávnění privilegovaných účtů dle definovaných politik na operačních systémech Unix/Linux a Windows (např. náhrada za sudo). Zmiňované rozšíření není požadováno jako součást dodávky.	**ANO**	-	**ANO**
A.18.	V rámci PIM řešení jsou definovány alespoň tyto následující uživatelské role: a. **Administrátor** – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek). b. **Auditor** – má přístup k auditním informacím a nahrávkám. c. **Uživatel** – je mu umožněn přístup k systému PIM a jeho běžné používání.	**ANO**	-	**ANO**
B.1.	Systém zaznamenává videonahrávky s aktivitou účtu, uskutečněnou prostřednictvím řešení PIM, s jednoznačnou vazbou na osobu, která aktivitu vykonává.	**ANO**	-	**ANO**
B.2.	V rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku.	**ANO**	-	**ANO**
B.3.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Stisknuté klávesy • Názvy oken spuštěných aplikací V obsahu metadat je možné vyhledávat dle zadaného řetězce.	**ANO**	-	**ANO**
B.4.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Výstupy na obrazovku V obsahu metadat je možné vyhledávat dle zadaného řetězce.	**NE**	**3**	**ANO**

B.5.	Nahrávky jsou zabezpečeně přenášeny do centrálního repository. Po celou dobu jejich existence je zaručen pouze autorizovaný přístup.	ANO	-	ANO
B.6.	Přístup k nahrávkám je řízen členstvím uživatele ve skupině/roli.	NE	3	ANO
B.7.	Uživatelé jsou upozorněni na skutečnost, že jejich aktivita je nahrávána.	ANO	-	ANO
B.8.	Nahrávky je možné exportovat do samostatného souboru, který lze přehrát bez nutnosti připojení (offline).	ANO	-	ANO
B.9.	Pro přístup k nahrávkám je možné vynutit metodu čtyř očí, tedy nutnost autorizace přístupu k nahrávce další osobou.	NE	1	ANO
B.10.	Řešení PIM obsahuje rozhraní pro integraci s nástroji typu service desk. • **Přístup k nahrávce** je povolen až na základě existence schváleného servisního ticketu.	NE	1	ANO
B.11.	Řešení PIM obsahuje rozhraní pro integraci s nástroji typu service desk. • Před samotnou **inicializací** nahrávaného **spojení** je vynuceno zadání čísla schváleného servisního ticketu (jehož existence a stav je aktivně ověřena). Číslo servisního ticketu je dostupné v rámci metadat uložených k nahrávce	NE	4	ANO
B.12.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volné textové pole	NE	4	ANO

B.13.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volba položky číselníku	NE	4	ANO
B.14.	Systém zaručuje, že není možné nahrávky jednoduše odstranit ani upravit, aby nemohla být zpochybněna jejich průkaznost.	ANO	-	ANO
B.15.	Repository s nahrávkami je pravidelně zálohováno tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).	ANO	-	ANO
B.16.	Nahrávky jsou efektivním způsobem zaznamenávány a přenášeny (komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke výraznému zatěžování prostředků (úložiště, síť). Maximální tolerovaná průměrná velikost nahrávky při běžném používání je 400kB/minutu.	ANO	-	ANO
B.17.	Relace je možné sledovat v živém režimu, pokud právě probíhají. Relaci je možné během sledování kdykoliv přerušit.	NE	4	ANO
B.18.	Je podporováno nahrávání SSH a RDP relace.	ANO	-	ANO
B.19.	Je podporováno nahrávání Citrix session (protokol ICA).	NE	5	ANO

B.20.	Je podporováno nahrávání následujících protokolů/relací: • Telnet • VNC • HTTP • HTTPS • Xserver • VMware hypervizor • MSSQL DB • Oracle DB	NE	5	ANO
B.21.	Řešení PIM nemá zaznamenatelný vliv na odezvy činností realizovaných v rámci probíhající uživatelské relace. Odezva systému při běžné práci se nesmí navýšit o více než 18% oproti přímému přístupu (mimo PIM řešení).	ANO	-	ANO
C.1.	Repository privilegovaných uživatelů s hesly je pravidelně zálohováno tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).	ANO	-	ANO
C.2.	Je implementován proces zajišťující bezpečný přístup k heslům uložených v systému i v případě jeho částečné nebo úplné nedostupnosti.	ANO	-	ANO
C.3.	Systém umožňuje vzdáleně měnit hesla k účtům na řízeném EP. Změna hesla je poskytnuta v rámci následujících akcí na řízeném účtu: • Reset hesla • „Check-out" hesla (změna hesla a následné poskytnutí hesla uživateli spolu s označením účtu jako používaného daným uživatelem) • „Check-in" hesla (změna hesla a odznačení účtu)	ANO	-	ANO

C.4.	Systém podporuje funkci vzdálené změny hesla na následujících typech EP: • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Red Hat Enterprise Linux 6 (64-bit) • HP-UX 11i v3 • Oracle RAC database 11g • Microsoft SQL Server 2008 R2 SP1 • Microsoft ActiveDirectory	ANO	-	ANO
C.5.	Systém umožňuje evidovat hesla k účtům neřízených EP. Změna hesel u těchto účtů je prováděna manuálně.	ANO	-	ANO
C.6.	Systém umožňuje označit řízené účty jako exkluzivní. Takové účty může v jednu chvíli používat (prostřednictvím funkce check-out/in a SSO) maximálně jeden uživatel.	ANO	-	ANO
C.7.	Řešení PIM je schopné spravovat EP přes přenosové cesty se sníženou propustností (WAN, DSL, apod.).	ANO	-	ANO
C.8.	Systém umožňuje definovat různé politiky hesel definující: • Složitost hesla (délka, sady znaků) • Stáří hesla • Opakovatelnost hesla Politiky je možné přiřazovat účtům jednotlivě nebo skupinově. Politiky jsou vynucovány během generování nových hesel, nebo při ručních změnách hesel z PIM systému.	ANO	-	ANO
C.9.	Systém automaticky provede změnu hesla na EP, pokud vypršela jeho platnost dle stáří, které je definované v přiřazené politice.	NE	2	ANO
C.10.	Systém v pravidelném intervalu kontroluje, zda heslo na EP odpovídá tomu evidovanému v PIM systému. V případě rozdílu je odeslána notifikace.	NE	4	ANO
C.11.	Přístup k účtům a jejich heslům je definován buď na úrovni účtu, nebo skupiny účtů.	ANO	-	ANO

C.12.	Uživatel má k dispozici účty buď na přímé použití, nebo je má k dispozici na podání žádosti. Žádost o přístup k účtu musí schválit jiný uživatel nebo skupina uživatelů. Schvalovatel je jasně definován v kontextu konkrétního účtu nebo skupiny účtů.	ANO	-	ANO
C.13.	Přiřazení privilegovaného účtu uživateli se řídí schvalovacím workflow, které je možné uživatelsky modifikovat. Workflow podporuje minimálně následující funkce: • Víceúrovňové kaskádovité schvalování, • Schvalování skupinou v režimu 1 z N (alespoň jedno schválení z N schvalovatelů)	NE	5	ANO
C.14.	Uživateli je umožněno požádat o přístup k účtu jen na omezenou dobu (interval od-do).	ANO	-	ANO
C.15.	Je navržen a implementován proces pro nouzový přístup k účtu bez potřebného schválení. Při spuštění takového procesu je současně vytvořen záznam o této události a je odeslána notifikace na určenou kontaktní osobu/osoby.	NE	5	ANO
C.16.	Systém poskytuje, prostřednictvím API, bezpečný přístup k heslům privilegovaných účtů pro aplikace/skripty na základě nastavených oprávnění (pro eliminaci otevřených hesel v kódech a konfiguračních souborech). S API je možné komunikovat z následujících programovacích jazyků: • Java • .NET • Unix/Linux shell script • Windows batch	ANO	-	ANO
C.17.	Řešení PIM musí podporovat použití spravovaného hesla účtu pro plánovanou úlohu (Scheduled Task) v OS Windows.	ANO	-	ANO

C.18.	Je navržen a implementován proces pro automatické discovery neřízených účtu na EP. Takové účty jsou v rámci navrženého procesu zařazeny do systému řízení PIM, nebo označeny jako výjimky, na které není již dále upozorňováno. Výsledek discovery je zaznamenán a je dostupný v podobě reportu, který může být naplánován k automatickému odesílání emailem.	NE	5	ANO
C.19.	Systém podporuje SSO pro privilegované účty (ve smyslu zmíněném v odstavci 5.1), tedy možnost se automaticky přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporovány jsou minimálně následující aplikace/protokoly: • Windows RDP • SSH (např. PuTTY)	ANO	-	ANO
C.20.	Další podporované aplikace/protokoly pro SSO jsou: • HTTP(s)/Web aplikace • Libovolná aplikace běžící v prostředí MS Windows	NE	5	ANO
C.21.	Během SSO je heslo automaticky zadáno na pozadí bez možnosti jeho odhalení, tedy heslo není aplikaci předáno v prostředí uživatele (např. není v paměti jeho stanice).	NE	5	ANO

Popis naplnění požadavku	Doplňující odkaz na externí zdroj
Všechny komponenty řešení PIM jsou dostupné v anglickém jazyce	
Pro obsluhu uživatelského rozhraní slouží komponenta Password Vault Web Access běžící na IIS 7.5 a vyšším. Podporuje Internet Explorer 8.0, 9.0, 10.0 a 11.0. Dále jsou podporovány prohlížeče Firefox a Chrome vydané během posledních šesti měsíců. Podmínkou je mít nainstalovaný Java plugin.	Privileged Account Security System Requirements
Jednotlivé komponenty produkčního prostředí podporuji režim vysoké dostupnosti: - Enterprise Password Vault, který slouží jako vysoce zabezpečené repozitory pro ukládání identit, lze clusterovat na úrovni operačního systému. Každý vault má svojí vlastní databázi, mezi kterými probíhají instantní aktualizace. Password Vault Web Access - webové rozhraní pro správu PIM. Jedná se o další kritickou komponentu, její dostupnost je řešená pomocí webové farmy. PSM - lze clusterovat na úrovni operačního systému	Privileged Account Security Implementation Guide

Řešení podporuje LDAP v3, testované a certifikované je pro tyto výrobce: MS Active-Directory – Windows 2003 with Service Pack 2, Windows 2008, Windows 2012 (native/mixed mode) Sun One v5.2 IBM Tivoli Directory Server v6.0 Novell eDirectory v8.7.1 Oracle Internet Directory v10.1.4	Privileged Account Security System Requirements s.6, Privileged Account Security Reference Guide s.98
Řešeno pomocí Transparent user management	"Priviledged Account Security Implementation Guide" : Transparent User Management (str. 86)
Navrhované řešení umožňuje SSO přes Windows authentizaci, lze následně doimplementovat další poskytovatele. Podrobněji je tato možnost popsána v kapitole "Privileged Single Sign-On" v Privileged Account Security Implementation Guide na str. 256	Privileged Single Sign-On v Privileged Account Security Implementation Guide na str. 256
Řešení splňuje všechny tyto požadavky. Seznam všech možných událostí je dostupný v dokumentaci.	Privileged Account Security Reference Guide str. 120 - "Activity references"

Posílání auditních logů lze nastavit pomocí Syslog protokolu do SIEM aplikací, včetně HP ArcSight.	Privileged Account Security Implementation Guide - "Integrating with SIEM Applications" str. 820
Standardně podporováno za pomoci tzv. "Activity report"	
Konfiguraci reportu jde uložit do standardní a konzistentní zprávy. Tyto zprávy lze naplánovat pro automatické generování na týdenní nebo měsíční bázi. Tato konfigurace zahrnuje typ zprávy, jeho obsah, uživatele, kteří budou mít přístup, a zda tito uživatelé obdrží automatické upozornění pokaždé, když je report generován.	Privileged Account Security Implementation Guide - The Privileged Account Security Solution Reports str. 327
Řešení poskytuje širokou škálu šablon reportů, dále je možno ho integrovat s Crystal reports a dělat nové šablony.	
V rámci řešení tuto roli plní "Event Notification Engine" (ENE). Seznam událostí, které je možno posílat lze dohledat v doplňujícím odkazu na externí zdroj	Sekce "Implementing Dynamic References" v Privileged Account Security Implementation Guide na str. 762

Veškeré auditní záznamy včetně videonahrávek jsou komprimovány. Pro přehráni videonahrávek ve vysoké kompresi, je potřeba na klienta kde budou přehrávány doinstalovat PSM kodek . Přenos množství dat za 1m se pohybuje v rozmezí 100-250 kb.	
Velmi malá zátěž linky v řádově jednotkách MB, pouze při odesílání záznamu do Vault.	
Řešení je instalováno na operační systémy, na kterých se během instalačního procesu provede hardening všech nepotřebných procesů. Takto zabezpečené servery zpracovávají pouze požadavky protokolu CyberArk. Šifrování dat je plně v souladu s FIPS 140-2.	

Řešení plně podporuje daný požadavek v komponentách OPM a AIM. Vše je cenrálně řízené, omezení jsou na úrovni uživatele.	Privileged Account Security Implementation Guide, Application Identity Management Implementation Guide
V rámci PSM jsou definovány následující role: IT administrators -uživatelé, kterým je povoleno vykonávat úkony na vzdálených systémech a zařízeních Auditors and security officers - uživatelé s přístupem k auditním informacím privileged session záznamům Administrators - správci PSM, přístup k auditním informacím a nahrávkám je povolen pouze požadovaným osobám.	
PSM nahrává automaticky všechny aktivity účtů s jejich jednoznačnou identifikací ve výchozím nastavení.	Privileged Account Security Implementation Guide - Configuring Recordings and Audits str. 573
V konfiguraci nastavení nahrávání záznamů lze zapnout volbu "Universal keystrokes text recorder". Jsou zaznamenány veškeré vstupy. Výstupy jsou zaznamenány pomocí nahrávání videa a textu. Pro úplný rozsah požadavku je potřeba mít implementované PSMP.	
Řešení zcela splňuje požadavek, metadata jsou indexována. Lze navíc auditovat jednotlivé příkazy psané do uživatelského vstupu.	
Řešení splňuje požadavek v plném rozsahu ve výchozím nastavení. Metadata obsahují uživatelské vstupy i systémové výstupy, obojí je indexováno pro snadné vyhledávání.	

Komunikace v rámci celého Privileged Account Security probíhá zabezpečeně za pomocí patentovaného protokolu CyberArk	
Přístup k nahrávkám mají uživatelé s rolí Auditors and security officers, oprávnění lze nastavit i individuálně.	
Uživatelům se při nahrávání zobrazí logo v pravém dolním rohu s danou informací.	
Nahrávka se dá exportovat do externího úložiště, přičemž zůstává její originál v původním úložiště. Nahrávky lze i porovnávat a ověřovat jejich autenticitu.	
Standardně podporovaná metoda, je součástí řešení.	Privileged Account Security Implementation Guide - Dual Control str.240
Uživatelé mohou vytvářet přímé odkazy URL na tzv PSM session recordings z logů logovacích nástrojů třetích stran jako je například SIEM, přidáním ID záznamu relace, která se objeví v protokolu auditu do dynamického odkazu, který spojuje autorizovaného uživatele na konkrétní událost v PSM. K těmto nahrávkám lze přistupovat přímo prostřednictvím oprávněných uživatelů a není tedy nutné hledat konkrétní session recording event.	
Navrhované řešení tuto možnost umožňuje viz doplňující údaje na externí zdroj	Privileged Account Security Implementation Guide - Configuring Dual Control together with Ticketing Integration str.504
Lze nastavit pravidlem v Master Policy	Privileged Account Security Implementation Guide - Specifying a Reason for Accessing Passwords str.233

Lze nastavit pravidlem v Master Policy	Privileged Account Security Implementation Guide - Specifying a Reason for Accessing Passwords str.233
Nanhrávku není možné smazat ani rolí auditor, při smazání bude označena pouze ke smazání, udělá se notifikace a o celé události je vedený auditní záznam. Délku po kterou bude nahrávka označena ke smazání lze nastavit individuálně.	
Repozitory se replikuje do vzdáleného úložiště pomocí zabezpečeného CyberArk Vault protokolu . Zálohy jsou šifrovány.	
Systém zaznamenává pouze aktivní relace, nahrávky jsou komprimovány.	
Kdykoliv se lze připojit na live session a terminovat ji.	
Zajištěno komponenatmi "Privileged Session Manager SSH Proxy" a "Privileged Session Manager"	Privileged Account Security Implementation Guide - Accessing PSM Live Sessions Users can generate direct URL links to live str.558
PSM podporuje nahrávávání Citrix Session	

PSM podporuje nahrávávání všech vyjmenovaných protokolů a relací	
Řešení PIM od CyberArk je tzv "agent less", zátěž na cílových systémech je minimální.	
Repozitory se replikuje do vzdáleného úložiště pomocí zabezpečeného CyberArk Vault protokolu . Zálohy jsou šifrovány.	
Požadavek je řešen pomocí účtu, který je vyjmut z administrace, uložený v trezoru a definován proces, při kterém ho lze použít.	
Master Policy umožňuje organizacím povolit uživatelům nastavit heslo na jedno použití a uzamknout přísttup tak, že ho ostatní uživatelé nemohou ve stejnou dobu použít. Po tom, co uživatel heslo použije ho systém vrátí zpět do trezoru. Tímto způsobem se zajišťuje výhradní použití privilegované účtu a umožňuje plnou kontrolu a sledování využití hesla. V případě, že je politikou organizace určeno jednorázové použití hesla, lze pomocí Master policy také nakonfigurovat změnu hesla před tím než ho odemkneme a umožníme používání dalšími uživateli.	Privileged Account Security Implementation Guide - Accounts Check-out and Check-in str.235

Řešení splňuje všechny uvedené požadavky na změnu hesla vyjmenovaných vzdálených systémů.	Privileged Account Security System Requirements - Automatic Password Management str.15
Požadavek je řešen pomocí účtu, který je vyjmut z administrace, uložený v trezoru a definován proces, při kterém ho lze použít.	
Obdobně jako C3 viz doplňující odkaz	Privileged Account Security Implementation Guide - Aecounts Check-out and Check-in str.235
Řešení je schopné spravovat EP přes přenosové cesty se sníženou propustností	
Řešení toto nastavení umožňuje	Privileged Account Security Implementation Guide - Managing Password Change Processes str.364
Řešení toto nastavení umožňuje, lze i nastavit schvalování této události	Privileged Account Security Implementation Guide - Managing Password Change Processes str.364
Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Managing Password Change Processes str.366
Řešení tento požadavek splňuje	

Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Dual Control str.240
Řešení tento požadavek splňuje	
Lze nastavit takzvaný "Request timeframe" , případně počet použití daného účtu	
Řešení umožňuje havarijní přístup, dá se konfigurovat pomocí "Master Policy". Systém generuje o celé události notifikaci a zapíše auditní záznam.	
K heslům je možné přistupovat pomocí CyberArk Credential Manageru z vlastních aplikací nebo skriptů. Podporovány jsou Java, .NET, Unix a Windows Shell skripty, C/C++.	
Provádí se aktivace přes tzv. "Platform management" a následně se vybírá platforma pro servisní účty, kde je Windows scheduled tasks jednou z možností.	Privileged Account Security Implementation Guide - Service Account Platforms str.114

Dodávané řešení nabízí novou generaci workflow na discovery a provisioning účtů, které je v souladu s podnikovými procesy s cílem zjednodušit a urychlit nasazení a řízení privilegovaného zabezpečení účtu. Proces zařazení do PIM jerozdělen do následujících třech kroků: **Discover** - automatizované vyhledávání privilegovaných účtů nastavené pro rychlé vyhledávané kritických účtů a pověření **Analyze** - Poskytuje snadný přehled o všech zjištěných účtech, které vám umožní analyzovat a určit, které účty již nejsou potřeba a mohou být odstraněny, a posoudit riziko každého účtu. **Provision** - jednoduchou a intultivní cestou umožňuje uložení účtů do bezpečného úložiště	Privileged Account Security Implementation Guide - Accounts Feed str.163
Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Privileged Single Sign-On str. 257
Za pomocí "Universal connector", který mapuje se rozhraní aplikace.	Privileged Account Security Implementation Guide - Configuring a PSM Universal Connector Connection Component str.640
Při transparentním připojení se provede impersonalizace a injekce přímo do session bez možnosti jeho odhalení.	Privileged Account Security Implementation Guide - Configuring Transparent Connections str.508

	Popis požadavku	Povinné	Váha	Splňuje	Popis naplnění požadavku	Doplňující odkaz na externí zdroj
A.1.	Všechny komponenty systému (PIM řešení) jsou dostupné v českém nebo anglickém jazyce.	ANO	-	ANO	Všechny komponenty řešení PIM jsou dostupné v anglickém jazyce	
A.2.	PIM řešení je určené pro český trh (potvrzeno prohlášením výrobce). Poskytující zajistí v souvislosti s poskytováním záručního servisu registraci objednatele v příslušné databázi výrobce řešení tak, aby byl objednatel oprávněn k technické podpoře v České republice přímo ze strany tohoto výrobce či jeho servisních partnerů.	ANO	-	ANO		
A.3.	Uživatelské rozhraní poskytující základní funkce je přístupné přes webove rozhraní s podporou prohlížeče • Internet Explorer ve verzi 10 a vyšší.	ANO	-	ANO	Pro obsluhu uživatelského rozhraní slouží komponenta Password Vault Web Access běžící na IIS 7.5 a vyšším. Podporuje Internet Explorer 8.0, 9.0, 10.0 a 11.0. Dále jsou podporovány prohlížeče Firefox a Chrome vydané během posledních šesti měsíců. Podmínkou je mít nainstalovaný Java plugin.	Privileged Account Security System Requirements
A.4.	Produkční prostředí je instalováno v režimu vysoké dostupnosti. Každá z komponent tedy musí obsahovat minimálně dvě samostatné instance provozované v HA módu active/active, nebo active/pasive. Řešení vysoké dostupnosti musí být plně automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro přepnutí mezi instancemi v případě vzniku chybového stavu, nejsou přípustná. Vysoká dostupnost musí být plně zajištěna na úrovni dodávaného PIM řešení, tedy buď na úrovni samotné aplikace a/nebo operačního systému. Pokud se nejedná o instalaci OS na fyzickém HW (tj. v případě použití virtualizace), dodávané řešení nesmí spoléhat na zajištění vysoké dostupnosti nástroji a prostředky virtualizační technologie.	ANO *	-	ANO	Jednotlivé komponenty produkčního prostředí podporují režim vysoké dostupnosti: - Enterprise Password Vault, který slouží jako vysoce zabezpečené repozitory pro ukládání identit, lze clusterovat na úrovni operačního systému. Každý vault má svoji vlastní databázi, mezi kterými probíhají instantní aktualizace. Password Vault Web Access - webové rozhraní pro správu PIM. Jedná se o další kritickou komponentu, její dostupnost je řešená pomocí webové farmy. PSM - lze clusterovat na úrovni operačního systému	Privileged Account Security Implementation Guide
A.5.	Autentizace uživatelskeho přístupu ke všem komponentám je řízena adresářem LDAP, nebo Active Directory.	ANO	-	ANO	Řešení podporuje LDAP V3, testované a certifikované je pro tyto výrobce: MS Active Directory – Windows 2003 with Service Pack 2, Windows 2008, Windows 2012 (native/mixed mode) Sun One v5.2 IBM Tivoli Directory Server v6.0 Novell eDirectory v8.7.1 Oracle Internet Directory v10.1.4	Privileged Account Security System Requirements s.6, Privileged Account Security Reference Guide s.98
A.6.	Autorizace uživatelského přístupu ke všem komponentám je řízena adresářem LDAP, nebo Active Directory (členství uživatelů ve skupinách).	NE	4	ANO	Řešeno pomocí Transparent user management	"Privileged Account Security Implementation Guide" - Transparent User Management (str. 86)
A.7.	K autentizaci je využit stávající SSO provider (Forgerock OpenAM), nebo automatické přihlášení na základě přihlášení k AD doméně (Integrated Windows Authentication).	NE	3	ANO	Navrhované řešení umožňuje SSO přes Windows authentizaci, lze následně doimplementovat další poskytovatele. Podrobnější je tato možnost popsána v kapitole "Privileged Single Sign-On" v Privileged Account Security Implementation Guide na str. 256	Privileged Single Sign-On v Privileged Account Security Implementation Guide na str. 256
A.8.	PIM řešení loguje auditní záznamy o všech administrátorských a uživatelských aktivitách. Minimálně se logují následující typy událostí vykonaných v PIM: • úspěšné a neúspěšné (pokus o) přihlášení a odhlášení • konfigurační změny (musí být zřejmé, kdo udělal jakou konfigurační změnu) • check-in/check-out hesla • přístup k nahrané session	ANO	-	ANO	Řešení splňuje všechny tyto požadavky. Seznam všech možných událostí je dostupný v dokumentaci.	Privileged Account Security Reference Guide str. 120 - "Activity references"

A.9.	Řešení PIM je integrované se SIEM řešením HP ArcSight, které je provozováno v prostředí MZe. Auditní záznamy jsou logovány a dostupné bez prodlení od vzniku události alespoň jednou z následujících metod: • Syslog • SNMP TRAP • Textový soubor • JDBC • Microsoft Event Log	ANO	-	ANO	Posílání auditních logů lze nastavit pomocí Syslog protokolu do SIEM aplikací, včetně HP ArcSight.	Privileged Account Security Implementation Guide - "Integrating with SIEM Applications" str. 820
A.10.	Řešení PIM poskytuje reporty ve formátech PDF nebo MS Excel (XLS/XLSX) Minimálně následující reporty jsou v rámci dodaného řešení k dispozici: • Seznam uživatelů a jejich oprávnění, včetně výpisu účtů, které mají k dispozici • Seznam všech spravovaných účtů, včetně přiřazených politik hesel a výčtu uživatelů, kteří mají k danému účtu přístup • Seznam aktivit nad účty – check out/in, přidělení účtu, atp.	ANO	-	ANO	Standardně podporováno za pomocí tzv. "Activity report"	
A.11.	Řešení PIM umožňuje naplánovat reporty k pravidelnému odesílání na email, nebo k ukládání do složky.	NE	3	ANO	Konfiguraci reportu jde uložit do standardní a konzistentní zprávy. Tyto zprávy lze naplánovat pro automatické generování na týdenní nebo měsíční bázi. Tato konfigurace zahrnuje typ zprávy, jeho obsah, uživatele, kteří budou mít přístup, a zda tito uživatelé obdrží automatická upozornění pokaždé, když je report generován.	Privileged Account Security Implementation Guide - The Privileged Account Security Solution Reports str. 327
A.12.	Součástí dodaného řešení PIM je uživatelský nástroj na vytváření nových reportů a jejich editaci.	NE	3	ANO	Řešení poskytuje širokou škálu šablon reportů, dále je možno ho integrovat s Crystal reports a dělat nové šablony.	
A.13.	Řešení PIM umožňuje definovat emailové notifikace na základě vybraných událostí.	NE	2	ANO	V rámci řešení tuto roli plní "Event Notification Engine" (ENE). Seznam událostí, které je možno posílat lze dohledat v doplňujícím odkazu na externí zdroj	Sekce "Implementing Dynamic References" v Privileged Account Security Implementation Guide na str. 762
A.14.	Dodané PIM řešení zatěžuje sdílené prostředky v minimální míře. Pokud je tedy stejné funkcionality možné dosáhnout s významně nižším zatížením používaných prostředků, je aplikován právě tento přístup. Znamená to, že využívání sdílených prostředků musí být optimalizováno, pokud je to možné (např. nahrávky musí být při přenosu a ukládání komprimovány). Týká se tedy vytížení: • Integrovaných systémů/aplikací (přístupové body, řízené EP, LDAP/AD) • Systémových zdrojů (CPU, RAM, IOPS, apod.) • Síťové infrastruktury (např. při přenosu nahrávek)	ANO	-	ANO	Veškeré auditní záznamy včetně videonahrávek jsou komprimovány. Pro přehrání videonahravek ve vysoké kompresi, je potřeba na klienta kde budou přehrávány doinstalovat PSM kodek . Přenos množství dat za 1m se pohybuje v rozmezí 100-250 kb.	
A.15.	Řešení PIM podporuje správu EP přes přenosové cesty se sníženou propustností a spolehlivostí.	ANO	-	ANO	Velmi malá zátěž linky v řádově jednotkách MB, pouze při odesílání záznamu do Vault.	

A.16.	Všechny komponenty dodaného řešení PIM jsou dostatečně zabezpečeny. Toho je dosaženo minimálně následujícími opatřeními: • je proveden hardening, • citlivá komunikace mezi komponentami, s externími systémy, nebo s uživateli je zabezpečena kryptografickými metodami, v rámci kterých jsou použity kryptografické algoritmy, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb. (Zákon o kybernetické bezpečnosti), nebo mezinárodně uznávaným standardem FIPS 140-2, • přístup k citlivým údajům a funkcím systému (jako jsou například hesla, nebo funkce změn hesla), je dostatečně chráněn pomocí kryptografických metod, v rámci kterých jsou použity kryptografické algoritmy, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb. (Zákon o kybernetické bezpečnosti), nebo mezinárodně uznávaným standardem FIPS 140-2, • v případě použití kryptografických metod, které nejsou v souladu s předchozími body, je možné implementovat dodatečná opatření, která jsou v souladu s předchozími body a zajistí dostatečnou ochranu ve smyslu předchozích bodů (např. slabě šifrovaná komunikace je posílána v IPSec tuneku, který je dodán jako součást řešení PIM)	ANO	-	ANO	Řešení je instalováno na operační systemy, na kterych se během instalačního procesu provede hardening všech nepotřebných procesů. Takto zabezpečané servery zpracovávají pouze požadavky protokolu CyberArk. Šifrování dat je plně v souladu s FIPS 140-2.	
A.17.	Systém podporuje rozšíření o modul na řízení přístupu (Access Control), tedy omezení oprávnění privilegovaných účtů dle definovaných politik na operačních systémech Unix/Linux a Windows (např. náhrada za sudo). Zmiňované rozšíření není požadováno jako součást dodávky.	ANO	-	ANO	Řešení plně podporuje daný požadavek v komponentách CPM a AIM. Vše je centrálně řízené, omezení jsou na úrovni uživatele.	Privileged Account Security Implementation Guide, Application Identity Management Implementation Guide
A.18.	V rámci PIM řešení jsou definovány alespoň tyto následující uživatelské role: a. Administrátor – konfiguruje systém nebo jeho část, může vytvářet/upravovat/odstraňovat objekty systému (kromě odstraňování auditních informací a nahrávek). b. Auditor – má přístup k auditním informacím a nahrávkám. c. Uživatel – je mu umožněn přístup k systému PIM a jeho běžné používání.	ANO	-	ANO	V rámci PSM jsou definovány následující role: T administrators -uživatelé, kterým je povoleno vykonávat úkony na vzdálených systémech a zařízeních Auditors and security officers - uživatelé s přístupem k auditním informacím privileged session záznamům Administrators - správci PSM, přístup k auditním informacím a nahrávkám je povolen pouze požadovaným osobám.	
B.1.	Systém zaznamenává videonahrávky s aktivitou účtu, uskutečněnou prostřednictvím řešení PIM, s jednoznačnou vazbou na osobu, která aktivitu vykonává.	ANO	-	ANO	PSM nahrává automaticky všechny aktivity účtů s jejich jednoznačnou identifikací ve výchozím nastavení.	Privileged Account Security Implementation Guide - Configuring Recordings and Audits str. 573
B.2.	V rámci nahrávky jsou zaznamenávány uživatelské vstupy (key-logging) a výstupy na obrazovku.	ANO	-	ANO	V konfiguraci nastavení nahrávání záznamů lze zapnout volbu "Universal keystrokes text recorder". Jsou zaznamenány veškeré vstupy. Výstupy jsou zaznamenány pomocí nahrávání videa a textu. Pro úplný rozsah požadavku je potřeba mít implementované PSMP.	
B.3.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Stisknuté klávesy • Názvy oken spuštěných aplikací V obsahu metadat je možné vyhledávat dle zadaného řetězce.	ANO	-	ANO	Řešení zcela splňuje požadavek, metadata jsou indexována. Lze navíc auditovat jednotlivé příkazy psané do uživatelského vstupu.	
B.4.	V rámci nahrávky jsou ukládány následující strukturovaná metadata: • Výstupy na obrazovku V obsahu metadat je možné vyhledávat dle zadaného řetězce.	NE	B	ANO	Řešení splňuje požadavek v plném rozsahu ve výchozím nastavení. Metadata obsahují uživatelské vstupy i systémové výstupy, obojí je indexováno pro snadné vyhledávání.	

B.5.	Nahrávky jsou zabezpečeně přenášeny do centrálního repository. Po celou dobu jejich existence je zaručen pouze autorizovaný přístup.	ANO	-	ANO	Komunikace v rámci celého Privileged Account Security probíhá zabezpečeně za pomocí patentovaného protokolu CyberArk	
B.6.	Přístup k nahrávkám je řízen členstvím uživatele ve skupině/roli.	NE	3	ANO	Přístup k nahrávkám mají uživatelé s rolí Auditors and security officers, oprávnění lze nastavit i individuálně.	
B.7.	Uživatelé jsou upozorněm na skutečnost, že jejich aktivita je nahrávána.	ANO	-	ANO	Uživatelům se při nahrávání zobrazí logo v pravém dolním rohu s danou informací.	
B.8.	Nahrávky je možné exportovat do samostatného souboru, který lze přehrát bez nutnosti připojení (offline).	ANO	-	ANO	Nahrávka se dá exportovat do externího úložiště, přičemž zůstává její originál v původním úložišti. Nahrávky lze i porovnávat a ověřovat jejich autenticitu.	
B.9.	Pro přístup k nahrávkám je možné vynutit metodu čtyř očí, tedy nutnost autorizace přístupu k nahrávce další osobou.	NE	1	ANO	Standardně podporovaná metoda, je součástí řešení.	Privileged Account Security Implementation Guide - Dual Control str.240
B.10.	Řešení PIM obsahuje rozhraní pro integraci s nástroji typu service desk. • Přístup k nahrávce je povolen až na základě existence schváleného servisního ticketu.	NE	1	ANO	Uživatelé mohou vytvářet přímé odkazy URL na tzv PSM session recordings z logů logovacích nástrojů třetích stran jako je například SIEM, přidáním ID záznamu relace, která se objeví v protokolu auditu do dynamického odkazu, který spojuje autorizovaného uživatele na konkrétní událost v PSM. K těmto nahrávkám lze přistupovat přímo prostřednictvím oprávněných uživatelů a není tedy nutné hledat konkrétní session recording event.	
B.11.	Řešení PIM obsahuje rozhraní pro integraci s nástroji typu service desk. • Před samotnou inicializací nahrávaného spojení je vynuceno zadání čísla schváleného servisního ticketu (jehož existence a stav je aktivně ověřena). Číslo servisního ticketu je dostupné v rámci metadat uložených k nahrávce	NE	4	ANO	Navrhované řešení tuto možnost umožňuje viz doplňující údaje na externí zdroj	Privileged Account Security Implementation Guide - Configuring Dual Control together with Ticketing integration str.504
B.12.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volné textové pole	NE	4	ANO	Lze nastavit pravidlem v Master Policy	Privileged Account Security Implementation Guide - Specifying a Reason for Accessing Passwords str.233
B.13.	Systém umožňuje vynutit udání důvodu přístupu k EP před zahájením nahrávaného spojení. Text důvodu je dostupný v rámci metadat uložených k nahrávce. Forma zadání důvodu je: • Volba položky číselníku	NE	4	ANO	Lze nastavit pravidlem v Master Policy	Privileged Account Security Implementation Guide - Specifying a Reason for Accessing Passwords str.233
B.14.	Systém zaručuje, že není možné nahrávky jednoduše odstranit ani upravit, aby nemohla být zpochybněna jejich průkaznost.	ANO	-	ANO	Nahrávku není možné smazat ani roli auditor, při smazání bude označena pouze ke smazání, uděší se notifikace a o celé události je veden auditní záznam. Délku po kterou bude nahrávka označena ke smazání lze nastavit individuálně.	
B.15.	Repository s nahrávkami je pravidelně zálohováno tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).	ANO	-	ANO	Repozitory se replikuje do vzdáleného úložiště pomocí zabezpečeného CyberArk Vault protokolu . Zálohy jsou šifrovány.	
B.16.	Nahrávky jsou efektivním způsobem zaznamenávány a přenášeny (komprimace, zaznamenávání pouze aktivní relace), aby nedocházelo ke výraznému zatěžování prostředků (úložiště, síť). Maximální tolerovaná průměrná velikost nahrávky při běžném používání je 400kB/minutu.	ANO	-	ANO	Systém zaznamenává pouze aktivní relace, nahrávky jsou komprimovány	
B.17.	Relace je možné sledovat v živém režimu, pokud právě probíhají. Relaci je možné během sledování kdykoliv přerušit.	NE	4	ANO	Kdykoliv se lze připojit na live session a terminovat ji.	

B.18	Je podporováno nahrávání SSH a RDP relace.	ANO	-	ANO	Zajištěno komponentami "Privileged Session Manager SSH Proxy" a "Privileged Session Manager"	Privileged Account Security Implementation Guide - Accessing PSM Live Sessions Users can generate direct URL links to live str.558
B.19	Je podporováno nahrávání Citrix session (protokol ICA).	NE	5	ANO	PSM podporuje nahrávávání Citrix Session	
B.20	Je podporováno nahrávání následujících protokolů/relací: • Telnet • VNC • HTTP • HTTPS • Xserver • VMware hypervizor • MSSQL DB • Oracle DB	NE	5	ANO	PSM podporuje nahrávávání všech vyjmenovaných protokolů a relací	
B.21	Řešení PIM nemá zaznamenatelný vliv na odezvy činností realizovaných v rámci probíhající uživatelské relace. Odezva systému při běžné práci se nesmí navýšit o více než 18% oproti přímému přístupu (mimo PIM řešení).	ANO	-	ANO	Řešení PIM od CyberArk je tzv "agent less", zátěž na cílových systémech je minimální.	
C.1.	Repository privilegovaných uživatelů s hesly je pravidelně zálohováno tak, aby byla zaručena jeho dostupnost. Zálohy jsou dostatečně zabezpečeny proti neoprávněnému přístupu (např. jsou zašifrovány).	ANO	-	ANO	Repozitory se replikuje do vzdáleného úložiště pomocí zabezpečeného CyberArk Vault protokolu . Zálohy jsou šifrovány.	
C.2.	Je implementován proces zajišťující bezpečný přístup k heslům uložených v systému i v případě jeho částečné nebo úplné nedostupnosti.	ANO	-	ANO	Požadavek je řešen pomocí účtu, který je vyjmut z administrace, uložený v trezoru a definován proces, při kterém ho lze použít.	
C.3.	Systém umožňuje vzdáleně měnit hesla k účtům na řízeném EP. Změna hesla je poskytnuta v rámci následujících akcí na řízeném účtu: • Reset hesla • „Check-out" hesla (změna hesla a následné poskytnutí hesla uživateli spolu s označením účtu jako používaného daným uživatelem) • „Check-in" hesla (změna hesla a odznačení účtu)	ANO	-	ANO	Master Policy umožňuje organizacím povolit uživatelům nastavit heslo na jedno použití a uzamknout přístup tak, že ho ostatní uživatelé nemohou ve stejnou dobu použít. Po tom, co uživatel heslo použije ho systém vrátí zpět do trezoru. Tímto způsobem se zajišťuje výhradní použití privilegované účtu a umožňuje plnou kontrolu a sledování využití hesla. V případě, že je politikou organizace určeno jednorázové použití hesla, lze pomocí Master policy také nakonfigurovat změnu hesla před tím než ho odemkneme a umožníme používání dalšími uživateli.	Privileged Account Security Implementation Guide - Accounts Check-out and Check-in str 235
C.4.	Systém podporuje funkci vzdálené změny hesla na následujících typech EP: • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Red Hat Enterprise Linux 6 (64-bit) • HP-UX 11i v3 • Oracle RAC database 11g • Microsoft SQL Server 2008 R2 SP1 • Microsoft ActiveDirectory	ANO	-	ANO	Řešení splňuje všechny uvedené požadavky na změnu hesla vyjmenovaných vzdálených systémů.	Privileged Account Security System Requirements - Automatic Password Management str. 15
C.5.	Systém umožňuje evidovat hesla k účtům neřízených EP. Změna hesel u těchto účtů je prováděna manuálně.	ANO	-	ANO	Požadavek je řešen pomocí účtu, který je vyjmut z administrace, uložený v trezoru a definován proces, při kterém ho lze použít.	

C.6.	Systém umožňuje označit řízené účty jako exkluzivní. Takové účty může v jednu chvíli používat (prostřednictvím funkce check-out/in a SSO) maximálně jeden uživatel.	ANO	-	ANO	Obdobně jako C3 viz doplňující odkaz	Privileged Account Security Implementation Guide - Accounts Check-out and Check-in str.235
C.7.	Řešení PIM je schopné spravovat EP přes přenosové cesty se sníženou propustností (WAN, DSL, apod.).	ANO	-	ANO	Řešení je schopné spravovat EP přes přenosové cesty se sníženou propustností	
C.8.	Systém umožňuje definovat různé politiky hesel definující: • Složitost hesla (délka, sady znaků) • Stáří hesla • Opakovatelnost hesla Politiky je možné přiřazovat účtům jednotlivě nebo skupinově. Politiky jsou vynucovány během generování nových hesel, nebo při ručních změnách hesel z PIM systému.	ANO	-	ANO	Řešení toto nastavení umožňuje	Privileged Account Security Implementation Guide - Managing Password Change Processes str.364
C.9.	System automaticky provede změnu hesla na EP, pokud vypršela jeho platnost dle stáří, které je definované v přiřazené politice.	NE	2	ANO	Řešení toto nastavení umožňuje, lze i nastavit schvalování této události	Privileged Account Security Implementation Guide - Managing Password Change Processes str.364
C.10.	Systém v pravidelném intervalu kontroluje, zda heslo na EP odpovídá tomu evidovanému v PIM systému. V případě rozdílu je odeslána notifikace.	NE	4	ANO	Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Managing Password Change Processes str.366
C.11.	Přístup k účtům a jejich heslům je definován buď na úrovni účtu, nebo skupiny účtů.	ANO	-	ANO	Řešení tento požadavek splňuje	
C.12.	Uživatel má k dispozici účty buď na přímé použití, nebo je má k dispozici na podání žádostí. Žádost o přístup k účtu musí schválit jiný uživatel nebo skupina uživatelů. Schvalovatel je jasně definován v kontextu konkrétního účtu nebo skupiny účtů.	ANO	-	ANO	Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Dual Control str.240
C.13.	Přiřazení privilegovaného účtu uživateli se řídí schvalovacím workflow, které je možné uživatelsky modifikovat. Workflow podporuje minimálně následující funkce: • Víceúrovňové kaskádovité schvalování, • Schvalování skupinou v režimu 1 z N (alespoň jedno schválení z N schvalovatelů)	NE	5	ANO	Řešení tento požadavek splňuje	
C.14.	Uživatel je umožněno požádat o přístup k účtu jen na omezenou dobu (interval od-do).	ANO	-	ANO	Lze nastavit takzvaný "Request timeframe", případně počet použití daného účtu	
C.15.	Je navržen a implementován proces pro nouzový přístup k účtu bez potřebného schválení. Při spuštění takového procesu je současně vytvořen záznam o této události a je odeslána notifikace na určenou kontaktní osobu/osoby.	NE	5	ANO	Řešení umožňuje havarijní přístup, dá se konfigurovat pomocí "Master Policy". Systém generuje o celé události notifikaci a zapíše auditní záznam.	
C.16.	System poskytuje, prostřednictvím API, bezpečný přístup k heslům privilegovaných účtů pro aplikace/skripty na základě nastavených oprávnění (pro eliminaci otevřených hesel v kódech a konfiguračních souborech). S API je možné komunikovat z následujících programovacích jazyků: • Java • .NET • Unix/Linux shell script • Windows batch	ANO	-	ANO	K heslům je možné přistupovat pomocí CyberArk Credential Manageru z vlastních aplikací nebo skriptů. Podporovány jsou Java, .NET, Unix a Windows Shell skripty, C/C++.	
C.17.	Řešení PIM musí podporovat použití spravovaného hesla účtu pro plánovanou úlohu (Scheduled Task) v OS Windows.	ANO	-	ANO	Provádí se aktivace přes tzv. "Platform management" a následně se vybírá platforma pro servisní účty, kde je Windows scheduled tasks jednou z možností.	Privileged Account Security Implementation Guide - Service Account Platforms str 114

C.18.	Je navržen a implementován proces pro automatické discovery neřízených účtu na EP. Takové účty jsou v rámci navrženého procesu zařazeny do systému řízení PIM, nebo označeny jako výjimky, na které není již dále upozorňováno. Výsledek discovery je zaznamenán a je dostupný v podobě reportu, který může být naplánován k automatickému odesílání emailem.	NE	5	ANO	Dodávané řešení nabízí novou generaci workflow na discovery a provisioning účtů, které je v souladu s podnikovými procesy s cílem zjednodušit a urychlit nasazení a řízení privilegovaného zabezpečení účtu. Proces zařazení do PIM je rozdělen do následujících třech kroků: Discover - automatizované vyhledávání privilegovaných účtů nastavené pro rychlé vyhledávané kritických účtů a pověření Analyze - Poskytuje snadný přehled o všech zjištěných účtech, které vám umožní analyzovat a určit, které účty již nejsou potřeba a mohou být odstraněny, a posoudit riziko každého účtu. Provision - jednoduchou a intuitivní cestou umožňuje uložení účtů do bezpečného úložiště	Privileged Account Security Implementation Guide - Accounts Feed str.163
C.19.	Systém podporuje SSO pro privilegované účty (ve smyslu zmíněném v odstavci 5.1), tedy možnost se automaticky přihlásit ke koncovému systému prostřednictvím privilegovaného účtu bez nutnosti zadávání hesla. Podporovány jsou minimálně následující aplikace/protokoly: • Windows RDP • SSH (např. PuTTY)	ANO	-	ANO	Řešení tento požadavek splňuje	Privileged Account Security Implementation Guide - Privileged Single Sign-On str. 257
C.20.	Další podporované aplikace/protokoly pro SSO jsou: • HTTP(s)/Web aplikace • Libovolná aplikace běžící v prostředí MS Windows	• NE	5	ANO	Za pomocí "Universal connector", který mapuje se rozhraní aplikace.	Privileged Account Security Implementation Guide - Configuring a PSM Universal Connector Connection Component str.640
C.21.	Během SSO je heslo automaticky zadáno na pozadí bez možnosti jeho odhalení, tedy heslo není aplikaci předáno v prostředí uživatele (např. není v paměti jeho stanice).	NE	5	ANO	Při transparentním připojení se provede impersonalizace a injekce přímo do session bez možnosti jeho odhalení.	Privileged Account Security Implementation Guide - Configuring Transparent Connections str.508

PŘÍLOHA Č. 4

HARMONOGRAM PLNĚNÍ

Plnění bude realizováno v následujících etapách, které jsou detailněji popsány v Technické Specifikaci:

Etapa		Čas (týdny)
B.1.	Podpis smlouvy	T
B.2.	Analýza	T + 3
B.3.	Akceptace Analýzy	T + 4
B.4.	Instalace	T + 6
B.5.	Implementace	T + 11
B.6.	Akceptační testy	T + 12
B.7.	Dokumentace	T + 14
B.8.	Školení	T + 16
B.9.	Akceptace dodávky (platební milník)	T + 16

T = den nabytí účinnosti Smlouvy.

Milník	Termín OD	Termín DO
Maintenance	Ukončení etapy B.4 Instalace	4 roky ode dne „Termín OD"

Milník	Termín OD	Termín DO
Podpora	Akceptace PIM řešení	4 roky ode dne „Termín OD"

PŘÍLOHA Č. 5

VZOR PŘEDÁVACÍHO PROTOKOLU

MINISTERSTVO ZEMĚDĚLSTVÍ

PŘEDÁVACÍ PROTOKOL Č. XXX

P_0128_2015

Projekt

Správa a monitoring privilegovaných účtů – PIM

Předmět:			
Smlouva č.:	S2015-0009, 987-2014-13310		
Zhotovitel:			
Vypracoval:		Datum:	

Strany předání	
Předávající:	Přebírající:
	Česká republika – Ministerstvo zemědělství Těšnov 65/17 110 00 Praha, Česká republika IČ: 00020478

Předmět předání

Seznam příloh předání	
Číslo:	Název přílohy
1	
2	
3	

Schvalovací doložka			
Datum převzetí:			
Předal:		Převzal:	
Jméno a příjmení		Jméno a příjmení	
Organizace		Organizace	Ministerstvo zemědělství ČR
Podpis		Podpis	

PŘÍLOHA Č. 6

VZOR AKEPTAČNÍHO PROTOKOLU

MINISTERSTVO ZEMĚDĚLSTVÍ

AKCEPTAČNÍ PROTOKOL Č. XXX P_0128_2015

Projekt

SPRÁVA A MONITORING PRIVILEGOVANÝCH ÚČTŮ – PIM

Předmět:			
Smlouva č.:	S2015-0009, 987-2014-13310		
Dodavatel:			
Vypracoval:		Datum:	
	Ministerstvo zemědělství	O2 IT Services s.r.o.	
Osoba zodpovědná za akceptaci:			

Předmět akceptace

Závěry akceptace	
Závěr (akceptováno nebo neakceptováno):	
Způsob akceptace (s výhradami nebo bez výhrad):	

Seznam výhrad akceptace			
Číslo:	Popis výhrady	Termín odstranění	Zodpovědná osoba
1			

Seznam příloh akceptace	
Číslo:	Název přílohy
1	
2	
3	

Schvalovací doložka			
Jméno a příjmení	Organizace	Podpis	Datum
	Ministerstvo zemědělství		
	O2 IT Services		

PŘÍLOHA Č. 7

SEZNAM SUBDODAVATELŮ

1/

Název:	Corpus Solutions, a.s.
Sídlo:	Na Vítězné plání 1719/4, Nusle, Praha 4
Právní forma:	Akciová společnost
Identifikační číslo:	25764616
Rozsah plnění Smlouvy:	Analýza, implementace a dodávka centrální správy privilegovaných účtů se abezpečeným úložištěm hesel a správou přístupů k těmto účtům. Maintenance, podpora a zajištění reparametrizace a optimalizace dodaného řešení.

2/

Název:	Risk Analysis Consultants, s.r.o.
Sídlo:	Táborská 979/5, Nusle, Praha 4
Právní forma:	Společnost s ručením omezeným
Identifikační číslo:	63672774
Rozsah plnění Smlouvy:	Podpora a zajištění reparametrizace a optimalizace dodaného řešení.

MINISTERSTVO
ZEMĚDĚLSTVÍ
Těšnov 65/17
110 00 Praha 1- Nové Město
-110-

MINISTERSTVO
ZEMĚDĚLSTVÍ
Těšnov 65/17
110 00 Praha 1- Nové Město
-110-