



Řízení letového provozu České republiky

Rámcová dohoda

„Správa identit PAM III“

uzavřená podle § 1746 odst. 2 ve spojení s § 2586 a násl. a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

(dále jen „**rámcová dohoda**“)

1. Smluvní strany

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

se sídlem: Jeneč, Navigační 787, PSČ: 252 61

zastoupený: Ing. Janem Klasem, generálním ředitelem

IČO: 49710371

DIČ CZ699004742

bankovní spojení: KB, a.s, Praha 1, číslo účtu: 1162200106/0100

IBAN: CZ45 0100 0000 0011 6220 0106

SWIFT kód: KOMBCZPP

zapsaný v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. A 10771,

(dále jen „objednatel“)

a

ICZ a.s.

se sídlem: Na hřebenech II 1718/10, Nusle, 140 00 Praha 4

zastoupený: Mgr. Danem Rosendorfem, předsedou představenstva

IČO: 251 45 444

DIČ: CZ699000372

zapsaný v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 4840

(dále jen „**zhotovitel**“)

(objednatel a zhotovitel dále rovněž jako „**smluvní strany**“)

2. Preambule

Vzhledem k tomu, že:

- 2.1 objednatel má zájem na zajištění nástroje pro řízení a správu privilegovaných přístupů, tzv. "Privileged Access Management", který zajistí řízení přístupu k aktivům technologické infrastruktury objednatele (HW/SW) a monitorování operací prováděných privilegovanými osobami (osobami s účty s vyšším oprávněním než user/domain user), a dále má zájem o servisní podporu tohoto nástroje,
- 2.2 zhotovitel má zájem implementovat požadavky objednatele na výše uvedený nástroj a poskytnout k němu servisní podporu a disponuje vlastnostmi a schopnostmi umožňujícími mu uvedené poskytnout v nejvyšší dostupné kvalitě, je schopen a bude jednat se znalostí a pečlivostí, která je s předmětem jeho činnosti, resp. s jeho povoláním či stavem obvykle spojena, splňuje veškeré podmínky a požadavky v této rámcové dohodě stanovené a je oprávněn tuto rámcovou dohodu uzavřít a řádně plnit závazky v ní obsažené,

se smluvní strany dohodly na uzavření této rámcové dohody.

3. Předmět rámcové dohody

- 3.1 Zhotovitel se touto rámcovou dohodou zavazuje objednateli poskytnout a do prostředí objednatele implementovat nástroj pro řízení a správu privilegovaných přístupů, tzv. "Privileged Access Management" dle technické specifikace, která tvoří Přílohu č. 1 této rámcové dohody, která je její nedílnou součástí (dále jen „**Systém PAM**“). Uživatelské prostředí Systému PAM, včetně veškerých hlášení Systému PAM a nápovědy, bude v anglickém jazyce.
- 3.2 Plnění dle odst. 3.1 této rámcové dohody bude realizováno ve dvou následujících fázích:
 - 3.2.1. Fáze 1, jejíž obsah a rozsah je detailně specifikován v Příloze č. 2 této rámcové dohody – Cenová kalkulace, která je její nedílnou součástí a kterou se zhotovitel zavazuje realizovat v termínech uvedených v článku 7 této rámcové dohody a zahrnuje:
 - 3.2.1.1. zpracování analýzy v souladu s článkem 9 této rámcové dohody,
 - 3.2.1.2. poskytnutí licencí k software Systému PAM v souladu s článkem 19 této rámcové dohody a Přílohou č. 2 této rámcové dohody,
 - 3.2.1.3. provedení instalace Systému PAM v souladu s technickou specifikací, která tvoří Přílohu č. 1 této rámcové dohody,
 - 3.2.1.4. integraci a implementaci v souladu s odst. 11.2 této rámcové dohody,
 - 3.2.1.5. asistenci při zkušebním provozu Systému PAM,
 - 3.2.1.6. provedení testů, jak je dále uvedeno v článku 11 této rámcové dohody,
 - 3.2.1.7. provedení školení, jak je dále uvedeno v článku 12 této rámcové dohody,
 - 3.2.1.8. vypracování dokumentace, jak je dále uvedeno v článku 13 této rámcové dohody,(dále jen „**Dílo**“).
 - 3.2.2. Fáze 2, jejíž obsah a rozsah je detailně specifikován v Příloze č. 2 této rámcové dohody a která bude realizována na základě dílčích smluv, které budou uzavřeny na základě výzvy k plnění ze strany objednatele a její akceptace ze strany zhotovitele, ve kterých bude blíže specifikován předmět plnění, co do druhu a rozsahu, vždy však v rozsahu a charakteru stanoveném touto rámcovou dohodou (dále jen „**dílčí smlouva**“). Vzor dílčí smlouvy je uveden v příloze č. 3 této rámcové dohody.
- 3.3 Při provádění Díla je zhotovitel povinen postupovat v souladu s Plánem implementace Systému PAM, odsouhlaseným objednatelem dle článku 10.6 této rámcové dohody.
- 3.4 Smluvní strany výslovně sjednávají, že rámcová dohoda nezakládá závazek objednatele realizovat Fázi 2 (část 2) vymezenou položkou 10, popřípadě 20 Přílohy č. 2 této rámcové dohody, zároveň

smluvní strany sjednávají, že Fázi 2 (část 1) vymezenou položkou 9, popřípadě 19 Přílohy č. 2 této rámcové dohody objednatel na základě dílčích smluv odebere v plném rozsahu.

- 3.5 Zhotovitel se touto rámcovou dohodou dále zavazuje objednateli poskytovat servisní podporu pro Systém PAM (dále jen „**Servisní podpora**“), a to v rozsahu dle článku 4 této rámcové dohody a za podmínek uvedených v článku 15 této rámcové dohody.
- 3.6 Zhotovitel se touto rámcovou dohodou dále zavazuje objednateli poskytovat konzultace za účelem změny konfigurace Systému PAM nebo změny v prostředí objednatele v rozsahu max. 1500 člověkohodin po dobu účinnosti této rámcové dohody. Konzultace budou poskytovány na základě objednávky akceptované zhotovitelem, ve které bude blíže specifikován předmět plnění, co do druhu a rozsahu, vždy však v rozsahu a charakteru stanoveném touto rámcovou dohodou. Objednávka bude zasílána prostřednictvím kontaktních osob dle odst. 16.1 této rámcové dohody elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS).
- 3.7 Zhotovitel se touto rámcovou dohodou dále zavazuje objednateli poskytovat maintenance, která zahrnuje poskytnutí aktualizací softwaru Systému PAM, které jsou nezbytné pro plnou funkčnost Systému PAM a poskytnutí nové verze takového softwaru, v případě, že je nová verze k dispozici.
- 3.8 Plnění této rámcové dohody je součástí projektu s názvem "Zvýšení kybernetické a fyzické bezpečnosti v ŘLP ČR, s.p.", reg. č. CZ.06.01.01/00/22_005/0002633, který je spolufinancován Evropskou unií z Evropského fondu pro regionální rozvoj, Integrovaného regionálního operačního programu 2021-2027, specifický cíl 1.1, průběžná výzva č. 5: KYBERNETICKÁ BEZPEČNOST."
- 3.9 Objednatel se zavazuje za podmínek stanovených touto rámcovou dohodou zaplatit za řádně a včas předané Dílo, za řádně a včas poskytnutou Servisní podporu a za řádně a včas poskytnuté konzultace ve výši a za podmínek stanovených v této rámcové dohodě a za řádně a včas poskytnuté plnění dle dílčí smlouvy.

4. Rozsah Servisní podpory a doba trvání Servisní podpory

4.1 Servisní podpora dle této smlouvy zahrnuje:

4.1.1. Servisní připravenost, která znamená:

- 4.1.1.1. připravenost kvalifikovaného personálu k provádění servisních zásahů na Systému PAM,
- 4.1.1.2. zřízení servisního kontaktu pro telefonické nebo emailové nahlášení požadavku ze strany objednatele, který bude dostupný 24 hodin denně, 7 dní v týdnu, 365 dní v roce,
- 4.1.1.3. poskytování služby Hotline, která znamená telefonickou podporu při řešení problémů souvisejících s provozem a funkčností Systému PAM na straně zhotovitele a dále řešení nejasností v otázkách funkčnosti Systému PAM na straně objednatele, dostupnost služby Hotline je v pracovní dny v rozsahu od 8:00 do 16:00 hodin a služba je poskytována v českém jazyce,
- 4.1.1.4. výkazy činnosti, tj. měsíční výkazy servisních zásahů v elektronické formě,
- 4.1.1.5. provádění lokalizace a identifikace závad a jejich příčin,
- 4.1.1.6. poskytování informací o stavu, postupu a způsobu odstraňování závad,
- 4.1.1.7. provádění obnovy nastavení (konfigurace) příslušné části Systému PAM, nebo Systému PAM jako celku dle uložené servisní zálohy,
- 4.1.1.8. provádění obnovy dat příslušné části Systému PAM k datu poslední servisní zálohy,
- 4.1.1.9. provádění servisních záloh nastavení a dat Systému PAM,
- 4.1.1.10. po oznámení závady zajištění funkčnosti Systému PAM.

4.1.2. Servisní zásahy, které zahrnují:

- 4.1.2.1. detekci závady,
- 4.1.2.2. analýzu problému,
- 4.1.2.3. odstranění závady v termínech dle odst. 15.5 této rámcové dohody,
- 4.1.2.4. dokumentaci servisního zásahu.

V případě, že si oprava závady vyžádá instalaci nové verze softwaru, je instalace této nové verze součástí paušální měsíční ceny za servisní zásahy a nebude pro objednatele znamenat další náklady.

4.1.3. Provádění údržby Systému PAM v rozsahu max. 30 člověkodní za dobu účinnosti této rámcové dohody, která zahrnuje:

- 4.1.3.1. kontrolu správnosti konfigurace a fungování Systému PAM jako celku,
- 4.1.3.2. kontrolu na případné bezpečnostní incidenty,
- 4.1.3.3. kontrolu systémové integrity,
- 4.1.3.4. kontrolu záloh a integrity dat,
- 4.1.3.5. správu a kontrolu programového vybavení zahrnující pravidelnou aktualizaci aplikací Systému PAM,
- 4.1.3.6. vypracování protokolu o údržbě s detailním popisem veškerých nalezených nedostatků a postupu pro jejich odstranění.

Zhotovitel je v rámci údržby oprávněn provést odstavení Systému PAM z provozu pouze v časovém období odsouhlaseném objednatelem (písemně nebo emailem).

4.1.4. Aktualizační školení v rozsahu max. 10 člověkodní za dobu účinnosti této rámcové dohody. Aktualizační školení se uskuteční v sídle objednatele, nedohodnou-li se smluvní strany jinak. Aktualizační školení může být provedeno i formou online školení.

4.1.5. Aktualizaci uživatelské a technické dokumentace k Systému PAM s ohledem na provedené změny Systému PAM v rozsahu max. 15 člověkodní za dobu účinnosti této rámcové dohody.

- 4.2 Servisní podporu se zhotovitel zavazuje poskytovat ode dne podepsání protokolu o řádném předání a převzetí Díla na základě odst. 14.1 této rámcové dohody.
- 4.3 Činnosti dle odst. 4.1.3, 4.1.4, a 4.1.5 této rámcové dohody budou prováděny na základě objednávky akceptované zhotovitelem, ve které bude blíže specifikován předmět plnění, co do druhu a rozsahu, vždy však v rozsahu a charakteru stanoveném touto rámcovou dohodou. Objednávka bude zasílána prostřednictvím kontaktních osob dle odst. 16.1 této rámcové dohody elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS).
- 4.4 Za účelem vyloučení pochybností smluvní strany uvádějí, že plnění poskytnuté na základě dílčí smlouvy nemá vliv na poskytování Servisní podpory dle tohoto odstavce a dle článku 15 této rámcové dohody a že Servisní podpora se vztahuje i na plnění poskytnuté na základě dílčí smlouvy.

5. Cena

5.1 Celková maximální cena za plnění vyplývající z této rámcové dohody činí:

23 000 000 Kč

(slovy: dvacet tři miliónů korun českých) bez DPH

a skládá se z následujících položek:

5.1.1. Cena za plnění ve Fázi 1 dle

odst. 3.2.1.1 až 3.2.1.8 této rámcové dohody, jejichž detailní rozpis je uveden v bodech 1, 3 až 8 a 17 Přílohy č. 2 této rámcové dohody,

5.1.2.Cena za plnění ve Fázi 2 dle odst. 3.2.2 této rámcové dohody, která je stanovena v souladu s jednotkovými cenami uvedenými v

bodech 19 a 20. Přílohy č. 2 této rámcové dohody.

5.1.3.Cena za Servisní podporu, která je stanovena v souladu s jednotkovými cenami uvedenými v bodech 11 až 14 Přílohy č. 2 této rámcové dohody.

5.1.5 Cena za maintenance dle odst. 3.7 této rámcové dohody je součástí ceny uvedené v bodech 17, 19 a 20 Přílohy č. 2 této rámcové dohody.

5.2 Výše uvedené ceny jsou konečné a zahrnují veškeré náklady, poplatky a odměny za poskytnuté licence dle článku 19 této rámcové dohody spojené s plněním dle této rámcové dohody/dílní smlouvy a zahrnují všechny další služby, dopravu a práva poskytnutá zhotovitelem. Změna ceny může být provedena výhradně písemnými vzestupně očíslovanými dodatky k této rámcové dohodě podepsanými oběma smluvními stranami, a to za dodržení podmínek stanovených zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“).

5.3 K výše uvedeným cenám bude účtována příslušná sazba daně z přidané hodnoty v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“).

5.4 Za účelem vyloučení pochybností smluvní strany uvádějí, že plnění poskytnuté na základě dílčí smlouvy nemá vliv na cenu dle odst. 5.1.3 této rámcové dohody.

6. Platební podmínky

6.1 Platby objednatel dle odst. 5.1.1 této rámcové dohody budou uskutečňeny na základě faktur – daňových dokladů vystavených zhotovitelem (dále jen „**faktura**“) následovně:

1. The **“*Journal of the American Academy of Child and Adolescent Psychiatry*”** is a peer-reviewed journal of child and adolescent psychiatry. It is published by the American Academy of Child and Adolescent Psychiatry (AACAP). The journal is one of the leading journals in the field of child and adolescent psychiatry.

[illegible]

6.1.3 Po implementaci do každého koncového systému objednatele určeného objednatelem dle odst. 10.1 této rámcové dohody vystaví zhotovitel fakturu v částce odpovídající jedné pětině ceny za položku 4 Přílohy č. 2 této rámcové dohody. K faktuře musí být přiložena kopie záznamu o implementaci dle odst. 11.3 této rámcové dohody.

§ 87(2)(b) [REDACTED]

(b) (7)(C), (b) (7)(D)

zprávy o provedeném školení. Cena za provedené školení musí být na faktuře vyčíslena zvlášť.

- 6.2 Platby objednatele dle odst. 5.1.2 této rámcové dohody budou uskutečněny na základě faktur vystavených zhotovitelem v souladu s dílčí smlouvou.
- 6.3 Měsíční platby za servisní připravenost a servisní zásahy se budou hradit na základě faktury – daňového dokladu vystavené zhotovitelem vždy k poslednímu dni příslušného měsíce.
- 6.4 Platby za údržbu, aktualizací školení a aktualizaci dokumentace se budou hradit na základě faktury – daňového dokladu vystavené zhotovitelem na základě skutečně odpracovaných člověkohodin vždy k poslednímu dni příslušného měsíce, ve kterém byly služby poskytnuty. K faktuře musí být přiložen výkaz poskytnutých služeb za příslušný měsíc odsouhlasený oběma smluvními stranami
- 6.5 Platba za konzultace dle odst. 5.1.4 této rámcové dohody bude fakturována a kalkulována dle skutečně odpracovaných člověkohodin vždy k poslednímu dni příslušného měsíce, ve kterém byly konzultace poskytnuty. K faktuře musí být přiložen výkaz poskytnutých konzultací za příslušný měsíc odsouhlasený oběma smluvními stranami.
- 6.6 Platby dle odstavce 5.1.5 této rámcové dohody budou zahrnuty v platbě dle odst. 6.1.2 nebo 6.2 této rámcové dohody.
- 6.7 Ceny uvedené v odst. 5.1.1 až 5.1.5 této rámcové dohody nebudou po dobu tří let od podpisu rámcové dohody upravovány o inflaci. Po uplynutí tří (3) let od podpisu rámcové dohody budou ceny dle odst. 5.1.2 až 5.1.5 této rámcové dohody upravovány jednou ročně na základě průměrné roční míry inflace za předchozí kalendářní rok, jak je oficiálně zveřejňována Českým statistickým úřadem.
- 6.8 V případě, že má zhotovitel sídlo mimo území České republiky, ceny uvedené v odst. 5.1.2 až 5.1.5 této rámcové dohody se po uplynutí tří (3) let od data podpisu rámcové dohody upraví ročně na základě harmonizovaného indexu spotřebitelských cen předcházejícího kalendářního roku, tak jak byl zveřejněn EUROSTAT pro stát sídla zhotovitele.
- 6.9 Úpravu ceny dle inflace lze vyjádřit následujícím vzorcem:

$$P_2 = P_1 \left(\frac{100 + RI}{100} \right)$$

- 6.10 Kde P2 je nová cena, P1 je stará cena a RI je průměrná roční míra inflace za předchozí kalendářní rok, jak je oficiálně zveřejňována Českým statistickým úřadem, v případě, že má zhotovitel sídlo mimo území České republiky, RI znamená HICP - roční míra změny vykázaná za předchozí kalendářní rok – zdroj – HICP – všechny položky – roční data (průměrný index a míra změny) (https://ec.europa.eu/eurostat/databrowser/view/PRC_HICP_AIND/default/table?lang=en) pro stát sídla zhotovitele.
- 6.11 Jestliže je průměrná roční míra inflace za předchozí kalendářní rok, jak je oficiálně zveřejňována Českým statistickým úřadem nebo v případě zhotovitele se sídlem mimo území České republiky harmonizovaný index spotřebitelských cen předcházejícího kalendářního roku, tak jak byl zveřejněn EUROSTAT pro stát sídla zhotovitele, nižší nebo rovno 0,5 %, ustanovení odst. 6.7 a 6.8 této rámcové dohody o úpravě ceny o inflaci se neaplikuje. Maximální možné meziroční zvýšení ceny nemůže být vyšší než 10 %.
- 6.12 Zhotovitel je povinen objednateli písemně oznámit změnu ceny dle odst. 6.7 nebo 6.8 této rámcové dohody, a to nejpozději se zasláním faktury, která zohledňuje tuto změnu, jinak se změna ceny na základě inflace neaplikuje. Takové oznámení zhotovitel zašle na adresu pro zasílání faktur dle odst. 6.15 této rámcové dohody.
- 6.13 Splatnost faktur je stanovena v délce třicet (30) kalendářních dnů ode dne jejich obdržení objednatelem.
- 6.14 Faktury musí splňovat všechny náležitosti daňového dokladu dle zákona o DPH, jinak budou vráceny zhotoviteli. V případě oprávněného vrácení faktury přestává běžet lhůta její splatnosti v den jejího odeslání objednatelem a nová lhůta počíná běžet ode dne nového doručení opravené či doplněné faktury objednateli. Oprava faktury musí být provedena nejpozději do 10 dnů od jejího obdržení zhotovitelem. Cena za školení musí být na faktuře uvedena samostatně.

- 6.15 Každá faktura s odvoláním na číslo této rámcové dohody/dílčí smlouvy objednatele uvedené v záhlaví této rámcové dohody/dílčí smlouvy jako evidenční číslo ŘLP ČR, s.p., a registrační číslo projektu CZ.06.01.01/00/22_005/0002633, včetně všech příloh dle ustanovení 6.1, 6.2, 6.4 a 6.5 této rámcové dohody, musí být zaslána v listinné podobě na adresu sídla objednatele uvedenou v článku 1 této rámcové dohody/dílčí smlouvy nebo elektronickou poštou z e-mailové adresy zhotovitele ■■■■■■■■■■ na e-mailovou adresu objednatele: fakturace@ans.cz.
- 6.16 Celková maximální cena za plnění vyplývající z této rámcové dohody nesmí za dobu trvání této rámcové dohody přesáhnout částku uvedenou v odst. 5.1 této rámcové dohody.

7 Termín plnění

- 7.1 Zhotovitel se zavazuje předat Dílo v následujících termínech:
- 7.1.1 předložení analýzy dle odst. 9.1 této rámcové dohody: T0 + max. 6 měsíců,
 - 7.1.2 předložení návrhu Plánu implementace Systému PAM dle odst. 10.2 této rámcové dohody: T0 + max. 8 měsíců,
 - 7.1.3 instalace SW (položky 2 a 3 Přílohy č. 2 rámcové dohody): do 2 měsíců od dodání HW ze strany objednatele,
 - 7.1.4 integrace SW do prostředí objednatele a implementace dle odst. 11.2 rámcové dohody, školení dle odst. 12.1.1 rámcové dohody: do 12 měsíců od dodání HW ze strany objednatele,
 - 7.1.5 ukončení zkušebního provozu dle odst. 11.5 rámcové dohody: do 15 měsíců od dodání HW ze strany objednatele,
 - 7.1.6 kompletace a odevzdání dokumentace dle odst. 13.1 rámcové dohody, školení dle odst. 12.1.2 rámcové dohody, podpis protokolu dle odst. 11.9 rámcové dohody: do 18 měsíců od dodání HW ze strany objednatele.
- 7.2 „Měsíc“ znamená období třiceti (30) po sobě jdoucích dní a „T0“ je den zveřejnění této rámcové dohody v registru smluv.
- 7.3 Zhotovitel se zavazuje předat plnění ve Fázi 2 Díla v termínu stanoveném v dílčí smlouvě.,

8 Místo plnění

- 8.1 Místem plnění je sídlo objednatele uvedené v čl. 1 této rámcové dohody.

9 Analýza

- 9.1 Zhotovitel zpracuje v termínu dle odst. 7.1.1 této rámcové dohody analýzu a návrh celkové koncepce používání, správy a řízení privilegovaných účtů, které jsou nebo mohou být v budoucnu do řešení PAM připojeny. V rámci této aktivity je předpokládána realizace workshopů s objednatelem, kdy dojde k vysvětlení aktuálních procesů nakládání s privilegovanými účty ze strany objednatele a vysvětlení technologického zázemí objednatele. Objednatel předpokládá využití know-how a zkušeností zhotovitele, který v rámci analýzy navrhne nejvhodnější způsob, jak odhalené typy účtů vhodně řídit a spravovat a toto řešení udržovat efektivní v čase. Tuto analýzu zhotovitel vytvoří v souladu s její bližší specifikací, která tvoří Přílohu č. 4 této rámcové dohody, která je její nedílnou součástí (dále jen „Analýza“).
- 9.2 Objednatel Analýzu do 15 (patnácti) pracovních dní od jejího předložení zhotovitelem, v případě, že splňuje požadavky dle této rámcové dohody, akceptuje. V případě, že Analýza požadavky dle této rámcové dohody nesplňuje, objednatel se do 15 (patnácti) pracovních dnů od jejího předložení zhotovitelem písemně vyjádří spolu s uvedením případných výhrad, připomínek a požadavků na její úpravu v souladu s touto rámcovou dohodou.
- 9.3 Do 15 (patnácti) pracovních dnů po doručení vyjádření dle předchozího odstavce zhotovitel Analýzu upraví dle požadavků objednatele a zohlední v ní případné připomínky a výhrady objednatele. Takto upravenou Analýzu zhotovitel předloží objednateli k opětovné akceptaci. Zhotovitel zároveň podrobně

seznámí zástupce objednatele se způsobem zpracování připomínek a požadavků objednatele a se změnami v Analýze. V případě, že Analýza nadále nesplňuje požadavky dle této rámcové dohody, postupuje se opakovaně dle odst. 9.2 a 9.3 této rámcové dohody až do akceptace Analýzy objednatelem. Uvedený postup nemá vliv na termíny stanovené v článku 7 této rámcové dohody.

9.4 O akceptaci Analýzy smluvní strany podepíše protokol o akceptaci.

10 Plán implementace

10.1 Pokud si smluvní strany nedohodnou jinak, v sídle objednatele se po akceptaci Analýzy dle odst. 9.4 této rámcové dohody uskuteční jednání o Plánu implementace Systému PAM (dále jen „**Plán implementace**“) do pěti (5) koncových systémů objednatele určených objednatelem na základě následujících kritérií:

10.1.1 alespoň jeden systém musí být z prostředí řízení letového provozu (ATM systém),

10.1.2 alespoň jeden systém musí být založen na OS Linux,

10.1.3 alespoň jeden systém musí být založen na OS Windows,

10.1.4 alespoň jeden systém musí být plně řízen – včetně automatizované politiky řízení hesel,

10.1.5 alespoň jeden systém musí být v kontrolovaném režimu – bez automatizované změny hesel,

10.1.6 alespoň jeden systém musí být v evidenčním režimu – pouze pro manuální vyzvedávání hesel,

10.1.7 alespoň u jednoho ze systémů musí být přístupy explicitně povolované na základě workflow,

10.1.8 alespoň u jednoho ze systémů musí být pro připojení koncové relace použit tlustý klient jiný než secure shell nebo remote desktop,

10.1.9 celkový počet uživatelů nesmí být větší než 50.

10.2 Na základě výše uvedeného jednání zhotovitel v termínu dle odst. 7.1.2 této rámcové dohody předloží objednateli návrh Plánu implementace.

10.3 Návrh Plánu implementace musí obsahovat detailní popis provádění Fáze 1 této rámcové dohody tak, aby splňoval požadavky Přílohy č. 1 této rámcové dohody a byl v souladu s Analýzou, a dále musí obsahovat časový harmonogram tak, aby zhotovitel splnil termíny stanovené v odst. 7.1 této rámcové dohody, plán školení, testovací plány a seznam předávané dokumentace. Zhotovitel je oprávněn vyžádat si na objednateli součinnost při tvorbě Plánu implementace, zejména v souvislosti s podáním informací ohledně interních procesů objednatele, objednatel je povinen zhotoviteli takovou součinnost v rozumné míře poskytnout.

10.4 Objednatel se k návrhu Plánu implementace do deseti (10) pracovních dnů od jeho předložení písemně vyjádří spolu s uvedením případných výhrad, připomínek a požadavků na jeho úpravu.

10.5 Do deseti (10) pracovních dnů po doručení vyjádření dle předchozího odstavce zhotovitel návrh Plánu implementace upraví dle požadavků objednatele a zohlední v něm případné připomínky a výhrady objednatele. Plán implementace zhotovitel předloží objednateli k akceptaci, a to v elektronické formě v běžně používaném formátu. Zhotovitel zároveň podrobně seznámí zástupce objednatele se způsobem zpracování připomínek a požadavků objednatele a se změnami oproti prvnímu návrhu Plánu implementace, a zodpoví případné dotazy.

10.6 Objednatel do deseti (10) pracovních dnů od předložení návrhu Plánu implementace k akceptaci dle odst. 10.5 této rámcové dohody ověří, zda byly v návrhu Plánu implementace zhotovitelem řádně vypořádány veškeré požadavky, připomínky a výhrady objednatele vznesené dle odst. 10.4 této rámcové dohody. Pokud byly veškeré požadavky, připomínky a výhrady objednatele řádně vypořádány, objednatel ve výše uvedené lhůtě Plán implementace akceptuje a podepíše o tom akceptační protokol. V opačném případě objednatel v téže lhůtě vrátí návrh Plánu implementace zhotoviteli k přepracování spolu s odůvodněním. Následně budou smluvní strany postupovat obdobně dle odst. 10.5 a 10.6 této rámcové dohody (a to i opakovaně), až do akceptace Plánu implementace. Uvedený postup nemá vliv na termíny stanovené v článku 7 této rámcové dohody.

11 Nasazení a akceptace

- 11.1 Zhotovitel se zavazuje zhotovit Dílo v souladu s technickou specifikací, která tvoří Přílohu č. 1 této rámcové dohody a s akceptovaným Plánem implementace.
- 11.2 Zhotovitel se zavazuje propojit Systém PAM s ostatními systémy objednatele, provést potřebnou konfiguraci a nastavení Systému PAM a všech nezbytných komponent a implementaci do koncových systémů objednatele určených objednatelem v souladu s ustanovením odst. 10.1 rámcové dohody (dále jen „**implementace**“). Implementace zahrnuje:
- 11.2.1 nastavení politik pro Systém PAM,
 - 11.2.2 nastavení a zabezpečení úložiště hesel a nahrávek privilegovaných uživatelů,
 - 11.2.3 nastavení nahrávání privilegovaných relací s retencí tři měsíce,
 - 11.2.4 integraci koncových zařízení, včetně zachování neovlivněného hesla nejvyšší úrovně oprávnění,
 - 11.2.5 minimálně pro systémy uvedené v položce 1.21 Přílohy č. 1 Technická specifikace - bude provedena integrace řízení hesel privilegovaných účtů včetně bezheslového přihlášení na integrované zařízení/systém (SSO), pokud to vybraná technologie bude přímo podporovat nebo pokud bude nutné v rámci implementace provést proprietární napojení,
 - 11.2.6 integraci na SIEM,
 - 11.2.7 součinnost při konfiguraci sítě a bezpečnostního monitoringu.
- 11.3 O implementaci do každého z koncových systémů objednatele určených objednatelem dle odst. 10.1 této rámcové dohody provede zhotovitel písemný záznam. Objednatel je oprávněn implementaci odmítnout v případě, že nesplňuje požadavky stanovené Analýzou. V případě odmítnutí objednatel do 10 dnů vyhotoví zprávu o odmítnutí implementace s uvedením nedostatků, které vedly k jejímu odmítnutí a zhotovitel je povinen tyto nedostatky bezodkladně a s náležitou péčí odstranit. Tento postup se opakuje až do akceptace implementace objednatelem. Ustanovení odst. 7.1.4 této rámcové dohody zůstávají nedotčena.
- 11.4 Zhotovitel se zavazuje při provádění této rámcové dohody respektovat provozní a bezpečnostní pravidla systémů objednatele a zachovávat mlčenlivost o důvěrných informacích objednatele, se kterými se přitom seznámí.
- 11.5 Po instalaci a propojení Systému PAM s ostatními systémy objednatele bude zahájen zkušební provoz v délce 3 měsíců pro koncové systémy objednatele určené objednatelem v souladu s ustanovením odst. 10.1 rámcové dohody. Systém PAM bude k dispozici uživatelům objednatele, kteří budou ověřovat funkčnost Systému PAM, jeho správné nastavení, a zjišťovat jeho případné nedostatky tak, aby finální verze Systému PAM mohla bezchybně a s plnou konfigurací fungovat ode dne stanoveného v odst. 7.1.6 rámcové dohody. Po dobu tohoto zkušebního provozu se zhotovitel zavazuje poskytnout objednateli a jeho jednotlivým uživatelům plnou součinnost při řešení případných závad či nedostatků Systému PAM či v jeho konfiguraci.
- 11.6 Na Díle provedeném podle této rámcové dohody proběhnou po zkušební provozu dle odst. 11.5 této rámcové dohody akceptační testy, které ověří, že Systém PAM splňuje všechny požadavky stanovené v technické specifikaci, která tvoří Přílohu č. 1 této rámcové dohody, a že Dílo je provedeno v souladu s Analýzou (dále jen „**testy**“). Testy proběhnou dle testovacích plánů, které jsou obsaženy v akceptovaném Plánu implementace. Objednatel je oprávněn vyžádat si doplnění plánu testů o další konkrétní testy, pokud to bude považovat za účelné pro ověření kompletní funkčnosti Systému PAM.
- 11.7 Zhotovitel objednateli navrhne 3 termíny konání testu minimálně 21 dní předem, z nichž objednatel vybere termín konání testů. Jestliže se strany nedohodnou na termínu konání testů, testy se uskuteční v poslední termín navržený zhotovitelem. Testy se uskuteční v pracovní dobu objednatele, tj. v pracovní den od 9 do 17h.
- 11.8 Test se uskuteční v sídle objednatele za přítomnosti zástupců objednatele v souladu s testovací dokumentací dle ustanovení 11.6 této rámcové dohody.

- 11.9 O výsledcích testu zhotovitel vyhotoví do deseti (10) dní od jeho provedení protokol. V případě odmítnutého testu objednatel do deseti (10) dní vyhotoví zprávu o odmítnutí obsahující zjištěné závady, které vedly k odmítnutí testu a zhotovitel je povinen tyto závady bezodkladně a s náležitou péčí odstranit a Systém PAM podrobit novému testu dle shora uvedených pravidel. Ustanovení odst. 7.1.6 této rámcové dohody zůstávají tímto nedotčena.
- 11.10 Zhotovitel odpovídá za to, že Systém PAM po ukončení instalace, konfigurace a testech funkčnosti bude funkční, fungující a kompatibilní se stávajícím prostředím objednatele.

12 Školení

- 12.1 Zhotovitel se zavazuje provést následující školení personálu objednatele za účelem obsluhy, konfigurace a monitorování Systému PAM:
- 12.1.1 základní školení – úvodní seznámení v rozsahu 5 člověkodní se zaměřením na seznámení se se Systémem PAM, jeho instalací, konfigurací a uvedením do provozu. Cílem je porozumění dané technologii pracovníky objednatele z uživatelského pohledu i administračního pohledu tak, aby mohli začít systém používat ve zkušebním provozu,
 - 12.1.2 pokročilé zaškolení pro správce Systému PAM v rozsahu 5 člověkodní, které poskytne určeným pracovníkům objednatele komplexní informace v takovém rozsahu, aby ti to pracovníci dokázali samostatně a dlouhodobě administrovat a provozovat Systém PAM. Součástí zaškolení bude i obnova Systému PAM po havárii, proškolení v provisioningu účtů s použitím automatizačních skriptů, v instalaci nových "jump" serverů pokud budou použité custom instalační skripty a specifické konfigurace odlišující se od běžného postupu uváděného výrobcem. Rozsah a obsah školení bude odpovídat kurzu pro přípravu na certifikaci pro administraci vybrané technologie,
- (dále jen „školení“).
- 12.2 Školení proběhne v sídle objednatele, které je uvedeno v článku 1 této rámcové dohody, případně po domluvě smluvních stran prostřednictvím online konference na platformě Microsoft Teams. Konkrétní termíny a místo školení bude určeno po vzájemné dohodě smluvních stran. Školení proběhne v českém jazyce, případně po vzájemné dohodě smluvních stran v anglickém jazyce.
- 12.3 Zhotovitel zajistí, aby školitel disponoval certifikací výrobce Systému PAM a aby školitel měl praxi v oboru minimálně 5 let. Certifikát je možno nahradit čestným prohlášením zhotovitele/výrobce o způsobilosti daného školitele.
- 12.4 Zhotovitel o provedeném školení vyhotoví zprávu zahrnující obsah školení a prezenční listinu.

13 Dokumentace

- 13.1 Zhotovitel se zavazuje zpracovat a objednateli předat následující dokumentaci:
- 13.1.1 produktovou dokumentaci výrobce ke všem dodávaným modulům PAM,
 - 13.1.2 dokumentaci detailně popisující veškeré změny vůči Analýze, ke kterým došlo v rámci realizace Fáze 1, zejména pak v průběhu implementace a zkušebního provozu,
 - 13.1.3 dokumentaci detailně doplňující Analýzu v bodech, které jsou v Analýze popsány pouze základní specifikací (viz bod 1.4 Přílohy č. 4 této rámcové dohody),
 - 13.1.4 instalační dokumentaci (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj Systému PAM) a dokumentaci k integrovaným systémům,
 - 13.1.5 uživatelskou příručku (manuál) popisující rozhraní Systému PAM z pohledu uživatele (z pohledu majitelů privilegovaných účtů uživatelsky přistupujících k PAM),
 - 13.1.6 administrátorskou příručku popisující Systém PAM z pohledu administrátorů, která obsahuje popis primárních úkonů, které administrátoři Systému PAM budou vykonávat,
 - 13.1.7 popis havarijních plánů pro obnovu služeb Systému PAM,

13.1.8 dokumentaci ke všem logům – popis struktury logů, seznam událostí s jejich významem a vazbou na jednotlivé operace.

13.2 Dokumentaci zhotovitel předloží v elektronické formě v českém jazyce. Produktovou dokumentaci výrobce, včetně dokumentace výrobce popisující strukturu a význam logů, může zhotovitel předložit v anglickém jazyce.

14 Předání a převzetí Díla

14.1 Po podpisu protokolu dle odst. 11.9 této rámcové dohody smluvní strany podepíší protokol o řádném předání a převzetí Díla, který stvrdí, že Dílo bylo řádně předáno objednateli a který zahrnuje:

14.1.1 identifikaci této rámcové dohody,

14.1.2 identifikaci předávající a přejímající strany,

14.1.3 seznam předané dokumentace,

14.1.4 zprávu o provedení školení,

14.1.5 samostatný dokument obsahující následující informace o SW Systému PAM: úplný a nezkrácený název SW včetně verze nebo edice SW, part number nebo SKU SW (dle relevantnosti), licenční model (pokud je nabízeno více licenčních modelů), délku podpory SW včetně počátečního a koncového dne podpory, informace o případném bundle SW s jinými SW výrobce, datum nabytí licenčních práv k SW, informace o zákaznickém účtu objednatele nebo odkaz na rámcovou smlouvu s výrobcem (dle relevantnosti) a množstevní a územní rozsah licence dle odst. 19.1 této rámcové dohody,

14.1.6 samostatný dokument obsahující podrobný seznam a licenční ujednání všech SW licencí třetích stran poskytnutých zhotovitelem v rámci plnění této rámcové dohody. Ke každé SW licenci třetí strany musí být uvedeno minimálně následující: identifikace dokladu, na základě kterého nabyl zhotovitel licenci; přesný název pořízeného software dle výrobce; edice, verze, typ (dle relevantnosti); počet pořízených licencí; omezení licence – např. identifikace jazykové verze, bitové verze, user/device, datacenter, CPU, CORE případně další omezení provozu – lokalitou, zemí a další (dle relevantnosti); informaci o licenci a odkaz na její elektronickou podobu. (např. GPL v2, MIT licence Apache licence apod.); typ licence a licenční program (OEM, OLP, SELECT, případně další); rozsah dodávané podpory (délka, začátek a konec) nebo přesnou vazbu na smlouvu a datum nabytí licenčních práv k SW,

14.1.7 seznam nalezených závad nebo nedodělků, které nebrání převzetí,

14.1.8 datum a místo předání,

14.1.9 podpisy předávající a přejímající strany.

14.2 Přílohou protokolu o řádném předání a převzetí Díla je protokol dle odst. 11.9 této rámcové dohody podepsaný odpovědnými zástupci obou smluvních stran.

14.3 Osobou oprávněnou k převzetí Díla za objednatele je kontaktní osoba uvedená v odst. 16.1.1 této rámcové dohody.

14.4 O splnění ve Fázi 2 smluvní strany podepíší protokol o řádném předání a převzetí plnění dle dílčí smlouvy.

15 Provádění Servisní podpory

15.1 Zhotovitel se zavazuje zajistit dostupnost Systému PAM tak, aby součet všech dob trvání oznámených závad kategorie A nepřesáhl během příslušného kalendářního roku 72 hodin, přičemž závada kategorie A se nesmí vyskytnout více než 3krát za dobu příslušného kalendářního roku.

15.2 Vyhodnocení dostupnosti bude probíhat na měsíční bázi porovnáním reportů o evidovaných závadách Systému PAM na straně objednatele i zhotovitele. Pro potřeby tohoto porovnání se zhotovitel zavazuje zasílat objednateli měsíční reporty o oznámených závadách na kontaktní osobu uvedenou v odst. 16.1.1 této rámcové dohody, a to vždy do patnáctého (15.) dne následujícího měsíce po

vyhodnocovaném měsíci. Takovýto report bude obsahovat soupis všech nahlášených závad s identifikačními čísly závad, časový snímek jejich řešení, stručný popis jejich řešení a vyhodnocení plnění lhůt pro odstraňování závad sjednaných touto rámcovou dohodou.

- 15.3 Nahlášení požadavku na servisní zásah provádí oprávněná osoba objednatele prostřednictvím telefonu na telefonní číslo: [REDAKCE] Po telefonním oznámení musí být tato skutečnost oznámena e-mailem s uvedením data, hodiny a jména pracovníka, který oznámení závady přijal, na výše uvedený email. Součástí požadavku na servisní zásah musí být i klasifikace závažnosti požadavku. Závažnost požadavku se přitom stanovuje podle následujících pravidel:

15.3.1 „Závažnost kategorie A“ znamená:

15.3.1.1 Systém PAM vykazuje takové nestandardní chování, které znemožňuje užívání ostatních provozních systémů objednatele propojených s některou z komponent Systému PAM, nebo

15.3.1.2 Systém PAM je zcela nefunkční nebo vylučuje užívání některé z komponent Systému PAM jako celku.

15.3.2 „Závažnost kategorie B“ znamená závadu, která způsobí závažné omezení funkčnosti Systému PAM či ztrátu plné redundance, výkonnostní degradaci (závažné problémy výkonu).

15.3.3 „Závažnost kategorie C“ znamená závadu, kterou objednatel nezařadil mezi závadu kategorie A nebo závadu kategorie B, a která nebrání nebo má zcela minimální vliv na řádné užívání nebo funkčnost Systému PAM a má minimální vliv na užívání Systému PAM jako celku.

- 15.4 Klasifikaci závažnosti požadavku provedenou objednatelem lze na základě dohody objednatele se zhotovitelem změnit.

- 15.5 Zhotovitel je povinen dodržet pro jednotlivé kategorie požadavků následující maximální lhůty:

Kategorie závady	Lhůta pro odpověď	Lhůta pro odstranění závady	Perioda průběžných informací
Závada kategorie A	4 hodiny	24 hodin	každou 1 hodinu až do odstranění závady
Závada kategorie B	4 hodiny	72 hodin (3 dny)	každých 12 hodin až do odstranění závady
Závada kategorie C	-	30 dní	každých 7 dní až do odstranění závady

- 15.6 Lhůta pro odpověď znamená lhůtu, ve které je zhotovitel povinen telefonicky na čísle +420 220374354 (či jiném čísle pro tyto účely určeném ze strany objednatele prostřednictvím kontaktní osoby uvedené v odst. 16.1 této rámcové dohody) a prostřednictvím elektronické pošty na adrese TIS@ANS.CZ (či na jiné elektronické adrese pro tyto účely určené ze strany objednatele prostřednictvím kontaktní osoby uvedené v odst. 16.1 této rámcové dohody) potvrdit objednateli přijetí požadavku na servisní zásah.

- 15.7 „Lhůta pro odstranění závady“ znamená lhůtu, ve které je zhotovitel povinen odstranit oznámenou závadu, a to prostřednictvím:

15.7.1 instalace softwarových korekcí v případě závady na software, nebo

15.7.2 dohody smluvních stran o jiném způsobu řešení odstranění závady, než je popsáno v předchozím bodu této rámcové dohody. O jiném způsobu odstranění závady, bude-li dohodnut, smluvní strany uzavřou písemnou dohodu.

- 15.8 Odstraňování oznámených závad zahrnuje i odstranění chyb v datech, které nastaly v důsledku vzniku odstraňované závady.
- 15.9 „Perioda průběžných informací“ znamená četnost poskytování průběžných informací o odstraňování závady, jež je zhotovitel povinen poskytovat objednateli. Postup poskytování průběžných informací si smluvní strany sjednávají tak, že zaměstnanec objednatele kontaktuje v rozsahu sjednané periody průběžných informací zhotovitele prostřednictvím kontaktů uvedených v odst. 15.3 této rámcové dohody a zhotovitel se zavazuje jej informovat o aktuálním průběhu procesu odstraňování závady.
- 15.10 Lhůta pro odpověď a lhůta pro odstranění závady začíná běžet po prokazatelném nahlášení požadavku na servisní zásah zhotoviteli ze strany objednatele. Totéž platí pro stanovení periody průběžných informací.
- 15.11 Zhotovitel se zavazuje odstraňovat závadu primárně vzdáleným přístupem, a to VPN připojením. Objednatel je však v případě konkrétní závady oprávněn vyžádat u zhotovitele on-site podporu a zhotovitel je v takovém případě povinen závadu opravit v místě plnění dle odst. 8.1 této rámcové dohody.
- 15.12 Pokud nebude možné odstranit závadu vzdáleným přístupem kompetentních zaměstnanců zhotovitele, je zhotovitel oprávněn vyzvat telefonicky zaměstnance objednatele k součinnosti při odstraňování závady (dále jen „**telefonická podpora**“). Takováto výzva k součinnosti může být vyvolána pouze v případě závady, u které je předpoklad, že čas vynaložený na odstranění závady může být efektivně zkrácen eliminací dojezdového času zaměstnanců zhotovitele do místa plnění.
- 15.13 V případě telefonické podpory se zhotovitel zavazuje postupovat:
 - 15.13.1 s ohledem na znalosti Systému PAM ze strany zaměstnanců objednatele,
 - 15.13.2 v součinnosti se zaměstnancem objednatele takovým způsobem, jako kdyby závadu odstraňoval zhotovitel fyzicky sám s tím, že zhotovitel nese plnou odpovědnost za provedení servisního zásahu.
- 15.14 Nebude-li možné závadu odstranit vzdáleným přístupem ani telefonickou podporou dle odst. 15.12 rámcové dohody, zavazuje se zhotovitel dostavit se do místa plnění dle odst. 8.1 této rámcové dohody. V případě prokázané nefunkčnosti vzdáleného přístupu vinou objednatele se čas technika strávený na cestě do místa plnění objednatele nebude započítávat do lhůty pro odstranění závady. Objednatel je povinen umožnit zhotoviteli přístup do místa plnění a k Systému PAM. V případech, kdy jsou lhůty pro odstranění závady v odst. 15.5 této rámcové dohody sjednány v hodinách, je objednatel povinen umožnit přístup do místa plnění 24 hodin denně.
- 15.15 Jestliže dojde v důsledku servisního zásahu ke změně Systému PAM, je zhotovitel povinen nejpozději do deseti (10) pracovních dnů po provedení změny v Systému PAM aktualizovat uživatelskou a technickou dokumentaci.
- 15.16 Zhotovitel se zavazuje poskytovat Servisní podporu řádným způsobem a v souladu s platnými normami a předpisy, které se na tento druh činnosti vztahují. Veškeré škody, které vzniknou porušením těchto norem a předpisů ze strany zhotovitele, idou k tíži zhotovitele.

16 Práva a povinnosti smluvních stran

- 16.1 Kontaktními osobami pro účely této rámcové dohody jsou:

16.1.1 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- 16.2 Seznam dalších kontaktních osob pro účely této rámcové dohody bude vytvořen a zaslán, případně měněn, prostřednictvím kontaktních osob uvedených v tomto odstavci rámcové dohody. Seznam

kontaktních osob bude zaslán elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS) či datovou schránkou nebo písemnou (listinnou) formou, a to prostřednictvím držitele poštovní licence. Objednatel na vyžádání umožní zhotoviteli přístup na pracoviště, kde bude probíhat plnění této rámcové dohody.

- 16.3 Objednatel na vyžádání předá nebo zprostředkuje zhotoviteli předání nezbytně nutných technických informací o zařízeních, systémech a službách, které mají souvislost se Systémem PAM a jejichž dosažitelnost je podmínkou k provedení této rámcové dohody. Objednatel dále při provádění této rámcové dohody zhotoviteli poskytne veškerou součinnost, kterou lze po něm rozumně požadovat.
- 16.4 Objednatel je oprávněn kontrolovat plnění této rámcové dohody/dílní smlouvy zhotovitelem. Zhotovitel se zavazuje poskytnout objednateli bez zbytečného odkladu přiměřenou součinnost a potřebné podklady, které si objednatel při kontrole důvodně vyžádá.
- 16.5 Jestliže to interní bezpečnostní předpisy objednatele dovolí, objednatel na vyžádání umožní zhotoviteli použít zařízení a hardwarové komponenty objednatele nezbytné pro provedení této rámcové dohody/dílní smlouvy.
- 16.6 Zhotovitel jako zaměstnavatel při provádění prací podle této rámcové dohody/dílní smlouvy odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci, popř. dalšími fyzickými osobami vykonávajícími práci v jeho prospěch. Veškeré škody, které vzniknou porušením těchto předpisů zaměstnanci zhotovitele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k tíži zhotovitele. Pokud zhotovitel svojí činností vytvoří nebezpečná místa nebo situaci na pracovišti, je povinen je sám zabezpečit a neprodleně o tom informovat objednatele.
- 16.7 Vstup externích subjektů do areálů a objektů objednatele
- 16.7.1 Zhotovitel je povinen dodržovat pravidla vstupu externích subjektů do areálů a objektů objednatele. Povinnosti zhotovitele týkající se vstupu externích subjektů do areálů a objektů objednatele jsou uvedeny na následující webové stránce:
- <https://www.rlp.cz/categoriesb?CatCode=A9>
- 16.8 Objednatel poskytne oprávněným zaměstnancům zhotovitele vzdálený přístup a VPN spojení ke spravovanému systému prostřednictvím IP datové sítě objednatele (CADIN) založený na definovaných přístupových oprávněních. Za tímto účelem zašle zhotovitel před vznikem potřeby vzdáleného přístupu objednateli seznam oprávněných zaměstnanců, kterým má být vzdálený přístup umožněn. Objednatel poskytne každému z oprávněných zaměstnanců zhotovitele oproti jejich podpisu RSA SecureID token generující jednorázové přístupové kódy pro zajištění sekundární autentizace. Pokud se tak dohodnou kontaktní osoby smluvních stran uvedené v odst. 16.1 této rámcové dohody, může být sekundární autentizace řešena místo RSA Secure ID tokenu zasíláním jednorázových přístupových kódů prostřednictvím SMS. V takovém případě poskytne zhotovitel objednateli také mobilní telefonní čísla oprávněných zaměstnanců. Seznam oprávněných zaměstnanců zhotovitele (včetně mobilních telefonních čísel v případě ověřování prostřednictvím jednorázového kódu zasláného přes SMS) může být zhotovitelem čas od času měněn, nicméně každá taková změna musí být neprodleně oznámena kontaktní osobě objednatele uvedenou v odst. 16.1 této rámcové dohody. Komunikace mezi kontaktními osobami uvedenými v odst. 16.1 této rámcové dohody dle tohoto odstavce bude probíhat elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS), či datovou schránkou, nebo písemnou (listinnou) formou prostřednictvím držitele poštovní licence.
- 16.9 Vzhledem k tomu, že zhotovitel byl vyhodnocen jako významný dodavatel ve smyslu § 2, písm. n) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), smluvní strany se dohodly, že nedílnou součástí této rámcové dohody je příloha č. 6, která obsahuje požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti (tj. informace týkající se bezpečnostních opatření pro smluvní vztahy s významnými dodavateli). Zhotovitel je povinen plnit povinnosti stanovené touto přílohou č. 6. Kontaktní údaje manažerů kybernetické bezpečnosti předají druhé smluvní straně kontaktní osoby uvedené v odst. 16.1 této rámcové dohody. Tyto kontaktní údaje/osoby mohou být čas od času měněny, nicméně každá taková změna musí být druhé smluvní straně neprodleně oznámena prostřednictvím kontaktních osob uvedených v odst. 16.1 této rámcové dohody. Komunikace ohledně kontaktních

údajů manažera kybernetické bezpečnosti bude mezi uvedenými kontaktními osobami probíhat elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS) či datovou schránkou nebo písemnou (listinnou) formou, a to prostřednictvím držitele poštovní licence.

- 16.10 Zhotovitel je povinen zajistit prostřednictvím odpovědné osoby prokazatelné seznámení všech pracovníků provádějících činnosti související s plněním rámcové dohody/dílní smlouvy s pravidly dle odst. 16.7.1 této rámcové dohody a s bezpečnostními pravidly oznamovanými dle článku 4 přílohy č. 6 této rámcové dohody.
- 16.11 Zhotovitel se zavazuje, že na provádění této rámcové dohody se bude podílet specialista na implementaci PAM, který má zkušenosti minimálně ze 2 implementací PAM, do nichž byl aktivně zapojen.
- 16.12 Kontaktní údaje osoby dle odst. 16.11 této rámcové dohody tvoří Přílohu č. 5 této rámcové dohody. Zhotovitel může tuto osobu čas od času měnit, nicméně každá taková změna musí být objednateli neprodleně oznámena a zhotovitel musí po celou dobu účinnosti této rámcové dohody splňovat podmínky stanovené v odst. 16.11 této rámcové dohody. Tuto skutečnost je zhotovitel povinen prokázat objednateli na základě jeho vyžádání, a to nejpozději do 7 pracovních dní ode dne vyžádání objednatele. Změny v osobě dle odst. 16.11 této rámcové dohody a jejích kontaktních údajů budou zasílány mezi kontaktními osobami objednatele a zhotovitele uvedenými v odst. 16.1 této rámcové dohody, přičemž změna osoby dle odst. 16.11 této dohody neznámá změnu této rámcové dohody. Komunikace mezi uvedenými kontaktními osobami bude probíhat elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf. a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS), či datovou schránkou, nebo písemnou (listinnou) formou, a to prostřednictvím držitele poštovní licence.
- 16.13 Zhotovitel je povinen uchovávat veškerou dokumentaci týkající se plnění dle této rámcové dohody, včetně účetních dokladů minimálně do 31. 12. 2035.
- 16.14 Zhotovitel je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s plněním dle této rámcové dohody zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského účetního dvora (dále také „EÚD“), Nejvyššího kontrolního úřadu (dále také „NKÚ“), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k plnění dle této rámcové dohody a poskytnout jim při provádění kontroly součinnost.
- 16.15 Objednatel je povinen zajistit dodání hardware, který na základě Analýzy zhotovitel označí za potřebný k plnění dle této smlouvy, a to bez zbytečného odkladu.

17 Vlastnické právo a nebezpečí škody

- 17.1 Vlastnické právo ke hmotným částem Díla přechází na objednatele okamžikem podpisu protokolu o řádném předání a převzetí Díla dle odst. 14.1 této rámcové dohody oběma smluvními stranami.
- 17.2 Nebezpečí škody přechází spolu s vlastnickým právem.

18 Záruka a odpovědnost za vady

- 18.1 Zhotovitel odpovídá za to, že Dílo bude provedeno v souladu s touto rámcovou dohodou bez vad, v jakosti a kvalitě odpovídající účelu dle této rámcové dohody, plně použitelné pro účel, pro který bylo pořízeno, a bude kompatibilní se stávajícím prostředím objednatele. Dílo musí být provedeno s vynaložením odpovídající odborné péče a s proaktivním přístupem. Dílo musí být provedeno v souladu s právními předpisy účinnými na území České republiky.
- 18.2 Zhotovitel poskytuje na Dílo záruku za jakost v délce 12 (slovy: dvanáct) měsíců. Záruka počne běžet ode dne podepsání protokolu o řádném předání a převzetí Díla dle odst. 14.1 této rámcové dohody. Přitom se má za to, že objednatel oznámil případně zjištěné vady včas bez ohledu na okamžik jejich zjištění, pokud je oznámil kdykoli během záruční doby.
- 18.3 Vady Díla, které brání akceptaci plnění, nejsou záručními vadami, ledaže objednatel akceptoval Dílo i s těmito vadami; v takovém případě se vady uvedené v akceptačním protokolu či jinak oznámené během akceptace považují od okamžiku akceptace Díla za nahlášené záruční vady. Za nahlášené

záruční vady, se od okamžiku akceptace považují i vady Díla, které nebrání akceptaci a byly uvedené v akceptačním protokolu či jinak oznámené během akceptace.

- 18.4 Během záruční doby zhotovitel poskytuje záruku za vady Díla, které vznikly při provádění preventivní údržby zaměstnanci objednatele při dodržování postupů a instrukcí pro údržbu zhotovitele.
- 18.5 Podmínky stanovené v odst. 18.4 této rámcové dohody zahrnují také situace, kdy je dokumentace pro údržbu nekompletní nebo nedostatečná, což má nežádoucí důsledky na Systém PAM.
- 18.6 Zhotovitel odpovídá za to, že Servisní podpora bude poskytnuta v souladu s touto rámcovou dohodou.
- 18.7 Zhotovitel poskytuje objednateli záruku na všechny servisní zásahy uskutečněné na základě této smlouvy. Záruční doba je stanovena v délce 12 (slovy: dvanáct) měsíců na servisní zásah a počíná běžet ode dne nasazení opravené verze softwaru do Systému PAM. Zhotovitel je povinen bez zbytečného odkladu a odstranit reklamovanou vadu poskytované Servisní podpory v záruční době.
- 18.8 Pro nahlášení reklamace se použije ustanovení odstavce 15.3 této rámcové dohody obdobně.
- 18.9 Záruka se nevztahuje na vady způsobené neodborným zacházením, nedodržením provozních podmínek, nedodržením předepsaných postupů a návodů k použití objednatelem.
- 18.10 Záruční doba se prodlužuje o dobu, po kterou byl Systém PAM nebo jeho část mimo provoz z důvodu vady, která je kryta zárukou či odpovědností za vady. Rozhodujícím datem je datum oznámení vady a datum převzetí Systému PAM nebo jeho části po opravě.
- 18.11 Odstraňování jakýchkoliv vad zjištěných objednatelem během záruční doby jsou součástí ceny dle odst. 5.1.1 této rámcové dohody a paušálu za servisní připravenost a servisní zásahy.
- 18.12 V případě, že zhotovitel nebude plnit řádně a včas podmínky poskytování záruky, je objednatel oprávněn závadu sám odstranit nebo sjednat odstranění závady třetí osobou. Náklady spojené s odstraněním závady nese zhotovitel.
- 18.13 Během záruční doby na Dílo se uplatní podmínky stanovené článkem 15 této rámcové dohody.
- 18.14 Pokud není v této rámcové dohodě uvedeno jinak, řídí se odpovědnost za vady ustanovením § 2615 odst. 2 občanského zákoníku.

19 Autorská práva

- 19.1 Smluvní strany se v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a s občanským zákoníkem, dohodly, že k Dílu, k počítačovým programům, které zhotovitel vytvoří při realizaci Díla, a k veškerému dalšímu plnění zhotovitele podle této rámcové dohody a které bude podléhat ochraně podle autorského zákona, poskytuje zhotovitel objednateli nevýhradní licenci pro území České republiky, v množstevním rozsahu nezbytném pro provozování Díla dle přílohy č. 1 a č. 2 této rámcové dohody, bez omezení způsobu užití, po dobu účinnosti této rámcové dohody (dále jen „**Licence k Dílu**“).
- 19.2 Licence k Dílu není omezena na počet koncových zařízení a řízených účtů v rámci jmenné licence např. při zavedení tierového modelu. Součástí Licence k Dílu je i řešení redundance všech komponent a taktéž geo-redundance (alespoň active-passive) s dodatečnou místní redundancí v druhé geolokaci.
- 19.3 Za účelem vyloučení pochybností smluvní strany uvádějí, že Licence k Dílu zahrnuje licence pro instalaci separátního trvalého testovacího prostředí Systému PAM s plnou funkcí a v plném rozsahu.
- 19.4 Smluvní strany se dohodly, že objednatel je, jak sám, tak prostřednictvím třetích osob, oprávněn upravit či jinak měnit Dílo, jeho název, dále je objednatel oprávněn Dílo spojit s dílem jiným nebo zařadit do díla souborného a Dílo v této podobě následně užít, dále je objednatel oprávněn užít Dílo i v jiném zpracování či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky, a to v rozsahu Licence k Dílu uvedené v tomto článku 19 této rámcové dohody.
- 19.5 Po realizaci úprav a zásahů do Díla dle odstavce 19.4 rámcové dohody neposkytuje zhotovitel záruku, že takové úpravy a zásahy budou funkční i poté, co zhotovitel provede upgrade Díla.

- 19.6 Smluvní strany se dohodly, že objednatel není povinen Licenci k Dílu využít. Udělení Licence k Dílu nelze ze strany zhotovitele po dobu trvání Licence k Dílu vypovědět. Odměna za poskytnutí Licence k Dílu podle tohoto článku 19 je zahrnuta v ceně Díla podle článku 5 této rámcové dohody.
- 19.7 Použije-li zhotovitel k vytvoření Díla tzv. proprietární software, u kterého nemůže objednateli udělit licenci dle odst. 19.4 této rámcové dohody, je zhotovitel oprávněn namísto oprávnění k užití Díla dle odst. 19.4 této rámcové dohody udělit objednateli licenci zahrnující nevýhradní oprávnění užití proprietární software, a to v množstevním rozsahu odpovídajícím potřebám objednatele ve vztahu k jeho využití Systému PAM. Udělení takové licence nelze ze strany zhotovitele po dobu trvání Licence k Dílu vypovědět, nedohodnou-li se smluvní strany výslovně jinak. Zhotovitel je povinen ve svých řešeních pro objednatele omezit využití takového proprietárního software, který je co do licence omezen ve smyslu tohoto odstavce této rámcové dohody. Jestliže jsou s užitím proprietárního software, služeb podpory k němu, či jiných souvisejících plnění spojeny jednorázové či pravidelné poplatky, jsou tyto poplatky zahrnuty v ceně této rámcové dohody.
- 19.8 Pro vyloučení pochybností smluvní strany prohlašují, že veškerá data, konfigurace, uživatelská nastavení či šablony pořízené pomocí Systému PAM nebo v něm obsažené jsou předmětem majetkových práv autorských objednatele a zhotovitel je pouze oprávněn je užívat v rámci poskytování plnění dle této rámcové dohody, a to na základě výslovného pokynu objednatele. Při ukončení této rámcové dohody se zhotovitel zavazuje na žádost objednatele poskytnout veškerou součinnost při migraci výše uvedených dat pro účel jejich dalšího využití. Tato součinnost je zahrnuta v ceně uvedené v odst. 5.1.1 této rámcové dohody.
- 19.9 Zhotovitel odpovídá objednateli za bezvadnost práv nabytých touto rámcovou dohodou, zejména za to, že Dílo, ani jiné plnění zhotovitele dle této rámcové dohody/dílčí smlouvy, včetně Servisní podpory, ani užívání Díla ze strany objednatele dle této rámcové dohody neporušuje ani nebude mít za následek porušení jakéhokoliv práva duševního vlastnictví třetích osob.
- 19.10 Zhotovitel rovněž odpovídá objednateli za škodu vzniklou v souvislosti s uplatněním práv třetích osob. Vznese-li proti objednateli jakákoliv třetí osoba nárok z porušení svých práv v souvislosti s Dílem nebo se Servisní podporou nebo s poskytnutou licencí, je zhotovitel povinen na své náklady účinně bránit objednateli a odškodnit jej v plné výši v případě, že třetí osoba svůj nárok plynoucí z právní vady Díla úspěšně uplatní. V případě, že by nárok třetí osoby vznikl v souvislosti s Dílem, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání Systému PAM, nebo jeho části, je zhotovitel povinen bezodkladně zajistit objednateli náhradní plnění a minimalizovat dopady takovéto situace, a to na své náklady a bez vlivu na cenu plnění sjednanou v této rámcové dohodě, přičemž současně nebudou dotčeny ani nároky objednatele na náhradu škody. V případě takového náhradního plnění zhotovitel zaručí, že dodaný software bude mít stejné funkcionality jako Systém PAM.
- 19.11 Pro vyloučení pochybností se uvádí, že odpovědnost zhotovitele za právní vady Díla nebo Servisní podpory ve smyslu odst. 19.9 této rámcové dohody není omezena záruční dobou sjednanou v této rámcové dohodě.
- 19.12 Objednatel odpovídá zato, že všechny návrhy nebo instrukce, které poskytuje zhotoviteli pro účely plnění této rámcové dohody, nezpůsobí porušení patentových práv, práv k průmyslovému vzoru, práv k obchodní známce nebo autorských práv. V tomto ohledu objednatel případně odškodní zhotovitele stejně, jako je uvedeno v odst. 19.10 této rámcové dohody.

20 Ochrana informací

- 20.1 Obě smluvní strany se zavazují považovat informace, o kterých se dozvěděly na základě této rámcové dohody/dílčí smlouvy nebo v souvislosti s ní za důvěrné a zavazují se zachovat mlčenlivost o takových skutečnostech, a to až do doby, kdy se tyto informace stanou obecně známými, za předpokladu, že se tak nestane porušením povinnosti mlčenlivosti.
- 20.2 Smluvní strany se dohodly užívat stejný stupeň ochrany před prozračením takových předávaných informací třetím stranám, jako používají pro ochranu svých vlastních informací stejné důležitosti. Předání informací se omezí na ty pracovníky obou smluvních stran, kteří se bezprostředně podílejí na činnostech podle této rámcové dohody/dílčí smlouvy.
- 20.3 Poskytnuté informace budou použity pouze k plnění závazků smluvních stran podle podmínek této rámcové dohody/dílčí smlouvy.

- 20.4 Omezení rozmnožování, prozrazení, zpřístupnění třetím stranám a užití informací nekončí po uplynutí doby trvání této rámcové dohody nebo jejím předčasným ukončením, pokud nenastane některé z následujících:
- 20.4.1 informace je veřejně přístupná nebo se později stane veřejně přístupnou jinak než porušením této rámcové dohody, nebo
 - 20.4.2 informace je poskytnuta třetí stranou bez obdobných omezení důvěrnosti ve vztahu k použití informace třetí stranou a stranou této rámcové dohody, nebo
 - 20.4.3 k prozrazení informace dojde na základě závazného požadavku nebo výzvy státních úřadů, které k tomuto mají z titulu výkonu své pravomoci a působnosti oprávnění.
- 20.5 Dále žádná ze stran nezodpovídá za rozmnožování, zveřejnění nebo použití informace, jež jí byla prozrazena, pokud taková informace byla straně známa před prozračením, nebo byla stranou legálně získána od třetí strany bez závazku důvěrnosti.
- 20.6 Zhotovitel bude považovat za důvěrné informace i všechna data, která jsou uchovávána v systémech a programech objednatele, a to i po neomezenou dobu po ukončení platnosti této rámcové dohody. Takové informace či data nesmí zhotovitel žádným způsobem zpřístupnit jakékoliv třetí osobě.
- 20.7 Zhotovitel se zavazuje plnit tuto rámcovou dohodu tak, aby zaviněním zhotovitele nedošlo ke ztrátě dat objednatele. Dojde-li zaviněním zhotovitele ke ztrátě dat objednatele, odpovídá zhotovitel za škodu tím způsobenou.

21 Smluvní pokuty

- 21.1 V případě, že objednatelem budou vytvořeny podmínky pro plnění v rozsahu uvedeném v této rámcové dohodě, avšak zhotovitel nedodrží termíny pro plnění dle článku 7 této rámcové dohody ani přes písemné upozornění objednatele a poskytnutí dodatečné lhůty ke splnění v délce max. třicet (30) dnů od doručení upozornění zhotoviteli, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny uvedené v odst. 5.1.1 této rámcové dohody za každý započatý den prodlení.
- 21.2 V případě, že objednatelem budou vytvořeny podmínky pro plnění v rozsahu uvedeném v odstavci 16.2 této rámcové dohody, avšak zhotovitel nedodrží kterýkoliv z časů uvedených v odstavci 15.5 této rámcové dohody, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu v částkách uvedených v následující tabulce:

Kategorie závady	smluvní pokuta
Závada kategorie A	15 000 CZK za každou započatou hodinu prodlení
Závada kategorie B	10 000 CZK za každou započatou hodinu prodlení
Závada kategorie C	10 000 CZK za každý započatý den prodlení

- 21.3 Poruší-li zhotovitel svůj závazek dle odst. 15.1 této rámcové dohody, zavazuje se zaplatit objednateli smluvní pokutu ve výši 100 000 CZK za čtvrtou a každou následující závadu kategorie A, která se vyskytne v daném kalendářním roce.
- 21.4 V případě, že zhotovitel během záruční doby na Dílo nedodrží lhůty pro provádění nápravných opatření dle odst. 18.13 této rámcové dohody, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši dle odst. 21.2 této rámcové dohody.
- 21.5 V případě porušení pravidel vstupu externích subjektů dle odst. 16.7 této rámcové dohody je zhotovitel povinen uhradit objednateli smluvní pokutu ve výši 10 000,- Kč (slovy: deset tisíc korun českých), a to za každý jednotlivý případ porušení.
- 21.6 Pokud zhotovitel poruší pravidla pro VPN přístup stanovená v bezpečnostních pravidlech oznamovaných dle článku 4 přílohy č. 6 této rámcové dohody, je zhotovitel povinen uhradit objednateli smluvní pokutu ve výši 100 000,- Kč (slovy: deset tisíc korun českých), a to za každý jednotlivý případ porušení.

- 21.7 V případě nesplnění povinnosti dle odst. 16.11 této rámcové dohody – požadavky na specialistu na implementaci PAM po dobu účinnosti této rámcové dohody, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých) za každý den, kdy zhotovitel nesplňuje podmínky uvedené v odst. 16.11 této rámcové dohody.
- 21.8 Pokud zhotovitel poruší podmínky zabezpečení koncové pracovní stanice stanovené v bezpečnostních pravidlech oznamovaných dle článku 4 přílohy č. 6 této rámcové dohody, je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000,- Kč (slovy: dvacet tisíc korun českých), za každý jednotlivý případ porušení.
- 21.9 Pokud zhotovitel poruší ohlašovací povinnost v oblasti bezpečnostních událostí/incidentů stanovenou v bezpečnostních pravidlech oznamovaných dle článku 4 přílohy č. 6 této rámcové dohody, je objednatel oprávněn požadovat smluvní pokutu ve výši 100 000,- Kč (slovy: sto tisíc korun českých) za každý jednotlivý případ porušení.
- 21.10 Pokud zhotovitel nezajistí v určeném termínu realizaci nápravných opatření vyplývajících ze zákaznického auditu provedeného dle podmínek popsanych v článku 8 přílohy č. 6 této rámcové dohody a dále upřesňované v bezpečnostních pravidlech oznamovaných dle článku 4 přílohy č. 6 této rámcové dohody, je objednatel oprávněn požadovat smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení.
- 21.11 Pokud zhotovitel jakožto zpracovatel (nebo subzpracovatel) nezničí osobní údaje nebo jejich kopie dle podmínek stanovených v příloze č. 7 této rámcové dohody, je objednatel jakožto správce oprávněn požadovat zaplacení smluvní pokuty ve výši 10 000,- Kč (slovy: deset tisíc korun českých) za každý jednotlivý subjekt osobních údajů, jehož osobní údaje nebyly vymazány, a to za každý den prodlení (i opakovaně).
- 21.12 V případě porušení některé povinnosti ochrany důvěrných informací nebo povinnosti mlčenlivosti ohledně důvěrných informací podle této rámcové dohody smluvní stranou vzniká druhé smluvní straně vůči porušující smluvní straně nárok na smluvní pokutu ve výši 1 000 000,- Kč (slovy: jeden milion korun českých), a to za každý jednotlivý případ porušení.
- 21.13 Smluvní pokuty podle této rámcové dohody jsou splatné do 30 dnů od doručení písemné výzvy k jejich úhradě smluvní straně povinné k jejich zaplacení.
- 21.14 Odchylně od § 2050 občanského zákoníku se smluvní strany dohodly, že sjednání jakékoli smluvní pokuty se nedotýká práva na náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje, a nárok na náhradu škody může být uplatněn nezávisle na smluvní pokutě a v plné výši.

22 Odstoupení od rámcové dohody/díli smlouvy, ukončení jejich platnosti

- 22.1 Objednatel je oprávněn odstoupit od této rámcové dohody, případně díli smlouvy, v případě, že zhotovitel poruší tuto rámcovou dohodu, případně díli smlouvu podstatným způsobem, zejména bude-li zanedbávat plnění svých závazků dle této rámcové dohody/díli smlouvy takovým způsobem, že tato skutečnost výrazně ovlivní kvalitu Dila nebo termín jeho dodání nebo kvalitu Servisní podpory. Za podstatné porušení této rámcové dohody, případně díli smlouvy s možností okamžitého odstoupení se považuje zejména:
- 22.1.1 zhotovitel je v prodlení se splněním své povinnosti vyplývající této rámcové dohody nebo díli smlouvy po dobu delší než třicet (30) dní a i přes písemné upozornění objednatele a poskytnutí dodatečné lhůty ke splnění v délce alespoň deset (10) dnů od doručení upozornění zhotoviteli, povinnost nesplnil,
- 22.1.2 zhotovitel je v prodlení s odstraněním řádně nahlášené závady Systému PAM dle článku 15.5 této rámcové dohody po dobu delší než 14 kalendářních dnů u lhůt stanovených na dny a 24 hodin u lhůt stanovených na hodiny, nebo
- 22.1.3 zhotovitel opakovaně (tj. více než dvakrát) porušil svou povinnost vyplývající z článku 16 této rámcové dohody a na takové porušení byl vždy písemně upozorněn,
- 22.1.4 zhotovitel porušil ustanovení Přílohy č. 6 této rámcové dohody nebo bezpečnostních pravidel oznamovaných dle článku 4 přílohy č. 6 této rámcové dohody,

- 22.1.5 zhotovitel porušil pravidla pro zpracování osobních údajů,
- 22.1.6 objednateli vznikl podle této smlouvy nárok na smluvní pokuty v souhrnné výši přesahující deset procent (10%) ceny dle odst. 5.1 této rámcové dohody.
- 22.2 Zhotovitel je od této rámcové dohody, popřípadě dílčí smlouvy, oprávněn odstoupit v případě, že
- 22.2.1 je objednatel v prodlení s platbou ceny za řádně poskytnuté plnění dle této rámcové dohody/dílčí smlouvy po dobu delší než třicet (30) dní i přes písemné upozornění zhotovitele a poskytnutí dodatečné lhůty alespoň deset (10) dnů od doručení upozornění objednateli,
- 22.2.2 objednatel opakovaně (tj. více než dvakrát) porušil svou povinnost vyplývající z článku 16 této rámcové dohody a na takové porušení byl vždy písemně upozorněn.
- 22.3 Objednatel je od této rámcové dohody, popřípadě dílčí smlouvy, oprávněn odstoupit také v případě významné změny kontroly nad zhotovitelem nebo změně kontroly nad zásadními aktivy využívanými zhotovitelem k plnění podle rámcové dohody, přičemž významnou změnou kontroly se rozumí změna ovládající osoby dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.
- 22.4 Objednatel se může do tří měsíců od předčasného ukončení této rámcové dohody/dílčí smlouvy rozhodnout, že se zrušení rámcové dohody/dílčí smlouvy nevztahuje na tu část do té doby dodaného plnění, která má dle uvážení objednatele pro něj samostatný ekonomický smysl a kterou se rozhodne si ponechat. V takovém případě zhotovitel není povinen vrátet přijatou část ceny odpovídající ceně části plnění, kterou si objednatel ponechal, a nebyla-li dosud tato část ceny uhrazena, náleží zhotoviteli úhrada za tuto část plnění. Ve vztahu k objednatelům ponechané části plnění se má za to, že rámcová dohoda/dílčí smlouva zanikla splněním.
- 22.5 Kterákoliv ze smluvních stran je dále oprávněna odstoupit od této rámcové dohody, popřípadě dílčí smlouvy, pokud se druhá smluvní strana dostane do úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
- 22.6 V případě odstoupení kterékoliv smluvní strany od této rámcové dohody, popřípadě dílčí smlouvy, nastávají účinky odstoupení dnem doručení písemného oznámení o odstoupení od této rámcové dohody/dílčí smlouvy druhé smluvní straně. Odstoupení bude zasláno doporučeným dopisem prostřednictvím držitele poštovní licence nebo datovou schránkou.
- 22.7 Odstoupení od této rámcové dohody/dílčí smlouvy nemá vliv na nároky ze smluvních pokut a náhrady škody dle této rámcové dohody vzniklé před účinností odstoupení od této rámcové dohody/dílčí smlouvy.
- 22.8 Tato rámcová dohoda/dílčí smlouva může být ukončena vzájemnou dohodou smluvních stran.
- 22.9 V případě předčasného ukončení platnosti této rámcové dohody/dílčí smlouvy jsou si obě smluvní strany povinny vzájemně vyrovnat všechny doposud existující závazky.

23 Náhrada majetkové a nemajetkové újmy

- 23.1 Pro náhradu majetkové újmy (škody) a nemajetkové újmy platí příslušná ustanovení občanského zákoníku. Majetková újma se nahrazuje v penězích, nedohodnou-li se smluvní strany v konkrétním případě jinak. Smluvní strany prohlašují, že dojde-li porušením povinností zhotovitele ke vzniku újmy na pověsti nebo obchodní firmě objednatele či k jiné nemajetkové újmě, uhradí zhotovitel objednateli i přiměřené zadostiučinění.
- 23.2 Žádná ze smluvních stran není povinna nahradit škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. V případě, že objednatel poskytl zhotoviteli chybné zadání a zhotovitel s ohledem na svou povinnost provádět rámcovou dohodu s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se zhotovitel ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání objednatele písemně upozornil a objednatel trval na původním zadání.
- 23.3 Zhotovitel prohlašuje, že je dostatečně pojištěn pro případ odpovědnosti za škodu způsobenou při provádění Díla a poskytování Servisní podpory objednateli nebo třetí osobě. Uzavřením rámcové dohody se zhotovitel též zavazuje, že pojištění bude ve stejném nebo větším rozsahu udržovat až do

ukončení platnosti této rámcové dohody. Zhotovitel se po tuto dobu zavazuje objednateli na jeho výzvu do dvou (2) pracovních dnů předložit doklad o trvání takového pojištění.

24 Poddodavatelé

- 24.1 Žádná smluvní strana nesmí převést svá práva a povinnosti dle této rámcové dohody/dílčí smlouvy na třetí osobu bez předchozího písemného souhlasu druhé smluvní strany, takový souhlas nesmí být neodůvodněně odepřen. Zhotovitel je oprávněn při plnění rámcové dohody/dílčí smlouvy využívat služeb třetích osob, za jejichž plnění však nese plnou odpovědnost.

25 Ostatní ujednání

25.1 Uveřejňování

Zhotovitel bere na vědomí, že objednatel je povinen uveřejnit tuto rámcovou dohodu a dílčí smlouvy ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů a ZZVZ. Zhotovitel bere dále na vědomí, že objednatel je povinen poskytnout informace podle zákona č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Při uveřejnění této rámcové dohody v registru smluv budou v jejím textu znečitelněny zejména tyto údaje: bankovní spojení zhotovitele uvedené v článku 1 této rámcové dohody a v článku 1 přílohy č. 3 této rámcové dohody, emailová adresa zhotovitele pro odesílání faktur uvedená v odst. 6.15 této rámcové dohody, kontaktní údaje uvedené v odst. 15.3 a 16.1 této rámcové dohody a v Příloze č. 5 této rámcové dohody, podpisy na rámcové dohodě a dále obchodní tajemství ve smyslu § 504 občanského zákoníku specifikované v odst. 25.2 této rámcové dohody.

25.2 Obchodní tajemství

Podle § 504 občanského zákoníku jsou obchodním tajemstvím technická specifikace uvedená v Příloze č. 1 této rámcové dohody, kalkulace ceny uvedená v odst. 5.1.4, 6.1.1, 6.1.2, 6.1.4 a 6.1.5 této rámcové dohody a v Příloze č. 2 této rámcové dohody, a proto nebudou tyto údaje uveřejněny, ani poskytnuty podle odst. 25.1 této rámcové dohody.

25.3 Bezpečnost v civilním letectví

Zhotovitel podpisem této rámcové dohody bere na vědomí, že není oprávněn sdělovat či jakkoliv šířit informace, kterými by mohla být narušena bezpečnost v civilním letectví, a to z důvodů požadavků na zachování bezpečnosti v civilním letectví, které vyplývají z příslušných právních předpisů (zejména Letecký předpis L 17), a které ukládají zhotovitelům letových provozních služeb přijmout taková adekvátní opatření, na základě kterých bude zajištěna ochrana civilního letectví před protiprávními činy. Zhotovitel nesmí zejména jakkoliv reprodukovat a dále šířit informace, o nichž se dozvěděl v souvislosti s plněním této rámcové dohody.

25.4 Ochrana osobních údajů

Vzhledem k tomu, že v rámci plnění předmětu této rámcové dohody dochází ke zpracovávání osobních údajů a dále vzhledem k tomu že, od 25. 5. 2018 je účinné nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „nařízení GDPR“), prohlašují smluvní strany, že při zpracování osobních údajů na základě této smlouvy bude postupováno v souladu s nařízením GDPR. Požadavky nařízení GDPR (tj. informace týkající se zpracování osobních údajů zpracovatelem, jak vyžaduje čl. 28 odst. 3 nařízení GDPR; a případně ekvivalentní požadavky jiných právních předpisů na ochranu osobních údajů) jsou do této smlouvy implementovány formou přílohy č. 7 této rámcové dohody.

Kontaktní údaje pověřence pro ochranu osobních údajů/osoby odpovědné za ochranu osobních údajů předají druhé smluvní straně kontaktní osoby uvedené v odst. 16.1 této rámcové dohody. Tyto kontaktní údaje/osoby mohou být čas od času měněny, nicméně každá taková změna musí být druhé smluvní straně neprodleně oznámena prostřednictvím kontaktních osob uvedených v odst. 16.1 této rámcové dohody. Komunikace ohledně kontaktních údajů pověřence pro ochranu osobních údajů/osoby odpovědné za ochranu osobních údajů bude mezi uvedenými kontaktními osobami probíhat elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do

formátu pdf a podepsány minimálně uznávaným elektronickým podpisem (v souladu s eIDAS) či datovou schránkou nebo písemnou (listinnou) formou, a to prostřednictvím držitele poštovní licence.

26 Vyšší moc

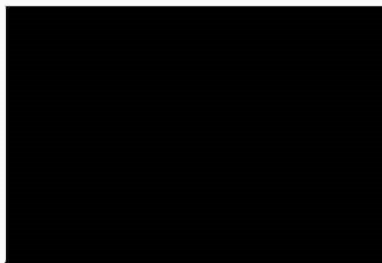
- 26.1 Smluvní strany se osvobozují od odpovědnosti za částečné nebo úplné nesplnění smluvních závazků, jestliže se tak prokazatelně stalo v důsledku vyšší moci. Za vyšší moc se pokládají okolnosti, které vznikly po uzavření této rámcové dohody/dílčí smlouvy v důsledku smluvními stranami nepředvídaných a neodvratitelných událostí, mimořádné povahy a mají bezprostřední vliv na plnění předmětu této rámcové dohody. Nastanou-li výše uvedené okolnosti, jsou obě smluvní strany povinny se neprodleně o těchto okolnostech vzájemně informovat.
- 26.2 Lhůty pro plnění povinností podle této rámcové dohody/dílčí smlouvy se prodlužují o dobu, po kterou prokazatelně trvá okolnost vylučující odpovědnost za částečné nebo úplné nesplnění smluvních závazků.
- 26.3 Jestliže důsledky vyplývající ze zásahu vyšší moci prokazatelně trvají déle než tři měsíce, může kterákoliv ze smluvních stran od této rámcové dohody/dílčí smlouvy odstoupit s tím, že se nároky smluvních stran vyrovnají tak, aby žádné ze smluvních stran nevzniklo bezdůvodné obohacení.

27 Řešení sporů

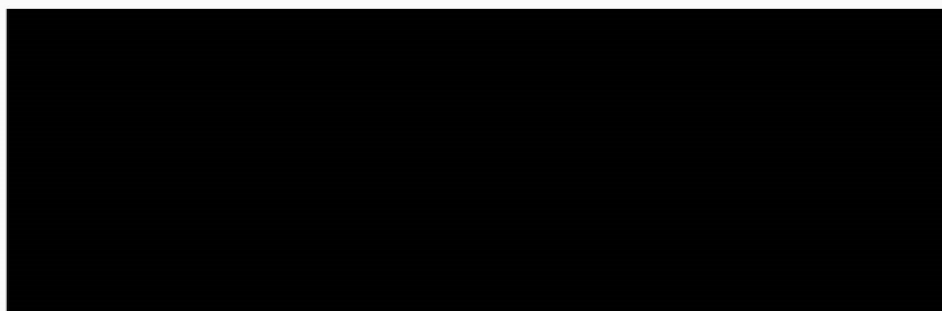
- 27.1 Všechny spory vyplývající z této smlouvy nebo v souvislosti s ní budou konečně rozhodnuty příslušným soudem České republiky. Smluvní strany se dohodly, že příslušným soudem je obecný soud dle sídla objednatele.
- 27.2 Tato smlouva se řídí českým právem.

28 Závěrečná ustanovení

- 28.1 Tuto rámcovou dohodu lze měnit nebo doplňovat pouze výslovným oboustranně potvrzeným smluvním ujednáním, a to ve formě písemných vzestupně číslovaných dodatků k této rámcové dohodě, podepsaných oprávněnými zástupci obou smluvních stran.
- 28.2 Obě smluvní strany prohlašují, že jednotlivé články této rámcové dohody jsou dostatečné z hlediska náležitosti pro vznik smluvního vztahu, a že bylo využito smluvní volnosti stran a tato rámcová dohoda se uzavírá určitě, vážně a srozumitelně.
- 28.3 Tato rámcová dohoda se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**
- 28.4 Tato rámcová dohoda se uzavírá na dobu určitou, a to na 60 po sobě jdoucích kalendářních měsíců od data vstupu této rámcové dohody v účinnost.
- 28.5 Tato rámcová dohoda vstupuje v platnost dnem jejího podpisu smluvními stranami a účinnosti nabývá dnem jejího uveřejnění v registru smluv.
- 28.6 Nedílnou součástí této rámcové dohody tvoří následující přílohy:
- Příloha č. 1 – Technická specifikace
 - Příloha č. 2 – Cenová kalkulace
 - Příloha č. 3 – Vzor dílčí smlouvy
 - Příloha č. 4 – Specifikace analýzy Systému PAM
 - Příloha č. 5 – Kontaktní údaje specialisty PAM
 - Příloha č. 6 – Zajištění opatření v oblasti informační a kybernetické bezpečnosti
 - Příloha č. 7 – Zajištění ochrany osobních údajů dle nařízení GDPR



.....
objednatel
Ing. Jan Klas
generální ředitel
Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)



zhotovitel
Mgr. Dan Rosendorf
předseda představenstva
ICZ a.s.

Příloha č. 1 – Technická specifikace

Příloha č. 1 rámcové dohody č. 181/2023/IS/140 - Technická specifikace				
č. o.	č. p.	Oblast / požadavek	Popis požadavku na řešení	Způsob provedení, možnosti ověření (doplň zhotovitel)
1. Základní funkční požadavky				
1	1	Řízení přístupů	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.	Nabízené řešení je založené na produktu CyberArk PAM, který slouží k zajištění kompletního životního cyklu privilegovaných účtů, včetně bezpečného SSO přihlašování ke koncovým systémům za současného zajištění detailní auditní stopy při použití těchto účtů. Přístup uživatelů k účtům je řízen jemně škálovatelným oprávněním, kdy uživatelé vidí pouze ty účty, na které mají povolenou některou z úrovně oprávnění (oprávnění k připojení, zobrazení hesla, apod.).
1	2	Striktní oddělení přístupových oprávnění	Řešení plně podporuje multi-tenant prostředí a umožňuje striktní oddělení přístupových oprávnění. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atd. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.	CyberArk PAM definuje role, na základě kterých má přihlášení uživatel k dispozici pouze definované funkce v rámci rozhraní řešení. Zároveň je na úrovni oprávnění řízena úroveň přístupu pro každého uživatele či skupinu uživatelů k jednotlivým účtům spravovaných řešením. Takto granulární nastavení oprávnění umožňuje docílit stavu, kdy ani administrátor nemusí mít přístup k žádnému účtu spravovanému řešením, nebo zaznamenané auditní informace.
1	3	Funkční požadavky	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování	CyberArk PAM disponuje funkcí schvalovacího workflow, které umožňuje generování žádostí o přístup ke spravovaným účtům na definovaný časový interval a následně dvouúrovňové schvalování těchto žádostí. Schvalovací workflow lze v případě připojování na koncový systém neaplikovat. Informace o stavu schvalovacího workflow jsou zasílány zainteresovaným osobám, případně jsou dostupné ve webovém rozhraní.

			přístupu lze vynutit odděleně pro přístup k přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozorněni emailem nebo notifikací přímo v řešení.	
1	4	Bezpečnostní parametry	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaných přihlašovacích údajů, jsou uloženy v jednom centrálním a vysoce zabezpečeném úložišti dat. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat.	Centrálním úložištěm je proprietární databáze - Digital Vault, která pro bezpečné uložení používá prostředky asymetrické kryptografie. V této centrální databázi jsou uloženy spravované účty, konfigurace, logy, auditní nahrávky apod. Digital Vault a další komponenty řešení jsou například v souladu se standardem FIPS 140-2. Rovněž veškerá komunikace mezi komponentami probíhá v rámci šifrované komunikace. Řešení zároveň umožňuje takové jemné nastavení rolí a oprávnění, že ani administrátor řešení nemusí mít oprávnění k žádnému spravovanému účtu, auditním logům či nahrávkám.
1	5	Jednotná centrální správa	Správa celého řešení je umožněna z jednoho centrálního místa.	Správa účtů, politik, přístup k auditním záznamům včetně nahrávek apod. je zajištěn přes webové rozhraní realizované komponentou CyberArk Password Vault Web Access.
1	6	Dostupnost admin portálu	Uživatelské prostředí administrátorského portálu je přístupné přes webové rozhraní s plnou podporou následujících prohlížečů v jejich poslední stabilní verzi a vyšší v OS Windows, Mac,	V rámci webového rozhraní realizovaného komponentou CyberArk Password Vault Web Access je i uživatelské prostředí, kde má uživatel k dispozici přehled dostupných uživatelských účtů integrovaných systémů s možností jejich použití pro přihlášení či dalším operacím definovaných na základě oprávnění. Pro přístup do webového rozhraní jsou podporovány webové prohlížeče Edge, Chrome a Firefox na OS Windows a Linux/UNIX.

			a Linux: Microsoft Edge, Mozilla Firefox, Google Chrome.	
1	7	Integrace s ticketing nástroji	Řešení musí umožňovat integraci s ticketing nástrojem třetích stran (např. ServiceNow, BMC, Jira) - žádost o schválení přístupu, přístup na základě existujícího tiketu.	Podporované ticketovací nástroje jsou Service Now a BMC Remedy, ostatní systémy se mohou napojit na REST API PVWA.
1	8	Podpora MS Active Directory	Řešení nabízí plnou integraci s Microsoft Active Directory (AD) na úrovni informací o uživateli, příslušnosti ke skupinám a emailech. Integrace musí umožňovat mapování rolí v PAM řešení v ná vaznosti na skupiny v AD.	Microsoft Active Directory je možné s řešením integrovat pro potřeby autentizace uživatelů, získání emailových adres pro notifikace, či pro definování rolí nebo přístupových oprávnění na úrovni skupiny uživatelů či konkrétního uživatele.
1	9	Integrace s AD / LDAP	Řešení musí mít nativní integraci se službou Active Directory, Azure AD a libovolným řešením, které podporuje protokol LDAP.	CyberArk obsahuje nativní podporu integrace s Microsoft Active Directory či jinými adresářovými službami pomocí LDAP protokolu.
1	10	Synchronizace (online integrace) s AD	Integrace služby Active Directory řešení musí umožňovat konfigurovatelný plán synchronizace (online integrace) pro automatizaci onboardingu nových uživatelů.	Onboarding/provisioning nových uživatelů řešení je možné realizovat na základě konfigurace jejich členství ve skupinách v AD. Členstvím v AD skupině tak uživatelský účet dostane přidělenou roli a příslušné oprávnění. Tato konfigurace členství je automaticky synchronizována do CyberArk PAM.
1	11	Podpora RADIUS	Řešení musí podporovat jakékoli řešení vícefaktorového ověřování založené na protokolu RADIUS.	CyberArk PAM podporuje integraci vícefaktorového ověřování pomocí RADIUS protokolu.
1	12	Omezení přístupu dle IP	Řešení musí podporovat omezení IP adres pro přístupové uživatele.	CyberArk PAM umožňuje omezit zdrojové adresy jak přístupujících uživatelů, tak i technických uživatelských účtů.

1	1 3	Uživatelské rozhraní	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a řešení musí podporovat okamžitou integraci dvou faktorového ověření (DUO, FIDO2, RSA a jakékoliv jiné řešení TOTP a nebo prostřednictvím protokolu RADIUS).	K autentizaci uživatelů je možné použít Microsoft Active Directory společně s dalším autentizačním faktorem realizovaným např. pomocí RADIUS protokolu nebo SAML standardu, či případně využít k autentizaci PKI.
1	1 4	Správa řešení pomocí Rest API	Řešení je možné spravovat pomocí API a to minimálně s funkcemi vytváření, čtení, aktualizace a mazání záznamů.	CyberArk PAM obsahuje bohatou podporu operací realizovaných pomocí REST API (https://docs.cyberark.com/pam-self-hosted/14.0/en/Content/WebServices/Implementing%20Privileged%20Account%20Security%20Web%20Services%20.htm).
1	1 5	Auditování rozhraní API	Použití rozhraní API řešení musí být auditovatelné řešením.	Aktivity realizované v rámci REST API jsou auditovány stejně jako aktivity provedeny v rámci webového rozhraní CyberArk PVWA.
1	1 6	Podpora Rest API či SDK a knihoven	Řešení musí nabízet Rest API, či SDK nebo programovací knihovny, které budou zahrnuty do zdrojového kódu interně vyvinutého softwaru.	CyberArk PAM nabízí jak REST API tak i SDK pro vlastní integrace s řešením (https://docs.cyberark.com/pam-self-hosted/14.0/en/Content/HomeTilesLPs/LP-Tile5.htm?tocpath=Developer%7C____0).
1	1 7	Auditování SDK	API/SDK/knihovny řešení musí být auditovatelné.	CyberArk PAM vývojová rozhraní podporují možnost auditování aktivit.
1	1 8	Popis SDK	Výrobce musí poskytovat veřejně dostupný (URL na veřejnou webovou stránku) popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací, s konkrétními příklady nasazení.	Dokumentace řešení CyberArk PAM, včetně dokumentace k vývojovým rozhraním, je dostupná na webových stránkách produktu (https://docs.cyberark.com/pam-self-hosted/14.0/en/Content/HomeTilesLPs/LP-Tile5.htm?tocpath=Developer%7C____0).
1	1 9	Silná autentizace	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro	Pro zajištění bezpečné a silné autentizace uživatelů CyberArk PAM umožňuje využít vícefaktorového ověřování pomocí RADIUS protokolu, SAML standardu či PKI.

			bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RADIUS, Kerberos, DUO, atd.). Řešení umožňuje integraci s MFA nástroji třetích stran.	
1	20	Automatické odhlásování	Řešení musí umožňovat automatické odhlášení z centrální konzole po nastavitelné době neaktivity	Webové rozhraní CyberArk PVWA umožňuje automatické odhlášení uživatele po definované době jeho nečinnosti.
1	21	Přímá podpora technologií	Řešení musí podporovat minimálně následující technologie a typy uložených hesel (neomezuje se na): Active Directory účet Cisco účet (ssh nebo telnet), Cisco VPN účet SSH klíč Kontakt, Generické heslo, Pin, Produktový licenční klíč HP iLO účet (SSH) Databázové účty: MySql účet, SQL Server účet, Sybase účet Office365 účet, OpenLDAP účet, Oracle účet, SAP účet Hesla do operačních systémů Unix, Windows, Linux VMware ESX/ESXi	CyberArk PAM podporuje kromě uvedených širokou řadu technologií tzv. out-of-box (https://cyberark.my.site.com/mplace/s/). V případě dalších či proprietárních systémů obsahuje vývojové nástroje pro zajištění jejich integrace.
1	22	HSM integrace	Řešení musí podporovat přesměrování správy hlavního šifrovacího klíče na modul hardwarového zabezpečení (integrace s HSM).	CyberArk PAM podporuje HSM moduly (https://docs.cyberark.com/pam-self-hosted/14.0/en/Content/PASIMP/Intro-Distributed-Vault-HSM.htm).
2. Password Management				

2	1	Vyhledávání a přidávání privilegovaných účtů	Řešení umožňuje vyhledávat privilegované účty v systémech a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Řešení musí být schopno zjistit účty alespoň následující typy účtů:	CyberArk PAM podporuje discovery účtů na koncových systémech a jejich automatický onboarding.
2	1.1	Vyhledávání a přidávání privilegovaných účtů	Služba Active Directory (všechny účty)	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.2	Vyhledávání a přidávání privilegovaných účtů	Lokální účty na systémech Windows, Unix/Linux a Mac	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.3	Vyhledávání a přidávání privilegovaných účtů	Účty služeb (Service Accounts)	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.4	Vyhledávání a přidávání privilegovaných účtů	LDAP účty (OpenLDAP, Oracle Directory Server EE, atd.)	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.5	Vyhledávání a přidávání privilegovaných účtů	Uživatelské účty pro webové aplikace a systémy třetích stran	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.6	Vyhledávání a přidávání privilegovaných účtů	Databázové účty (ODBC, MySQL, MS SQL, IBM, SAP, Oracle, PostgreSQL, etc.)	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.7	Vyhledávání a přidávání privilegovaných účtů	Účty síťových zařízení	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	1.8	Vyhledávání a přidávání privilegovaných účtů	VMWare ESX/ESXi lokální účty	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.

2	1. 9	Vyhledávání a přidávání privilegovaných účtů	SSH klíče a jejich závislosti (uložení s heslem i bez hesla)	CyberArk PAM umožňuje onboarding účtů v souladu s odpovědí Zadavatele ze dne 19.2.2024 na doplňující dotaz č.1, kdy je možný automatický onboarding účtu dle připraveného seznam účtů. Pro data k vytvoření seznamu může být například použit nástroj CyberArk DNA, který umí v prostředí identifikovat účty v rámci OS, databází, běhu služeb, Ansible, IIS apod.
2	2	Sdílené účty	Řešení musí podporovat sdílené privilegované účty. Řešení musí zajistit jasné vlastnictví sdíleného účtu, například pomocí funkce vypůjčení, což zajistí, že vždy jen jeden uživatel může používat sdílený účet.	CyberArk PAM zajišťuje plnou tzv. accountability, kdy je díky auditování přístupu a celé relace zajištěna nepopiratelnost použití daného účtu konkrétní identitou. Zároveň obsahuje funkcionalitu exkluzivního přístupu, kdy je možné zajistit použití účtu pouze jednou identitou v čase.
2	3	SSH klíče	Řešení musí umožňovat ukládání nejen hesel, ale i ukládání a správu SSH klíčů. Řešení musí umožňovat generovat, rotovat a spravovat SSH klíče.	CyberArk PAM umožňuje kromě uložení hesla pro spravovaný účet i ukládání SSH klíčů, a to včetně zajištění jejich automatické verifikace a změny/rotace.
2	4	Ověřování hesel	Řešení kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci, nebo zašle upozornění správci.	CyberArk PAM umožňuje pravidelnou verifikaci shody a funkčnosti uložených autentizačních údajů s autentizačními údaji na koncových systémech. V případě zjištěného rozdílu umožňuje přihlašovací údaje na koncovém systému opravit pomocí tzv. reconcile účtu. Zároveň je možné zaslat emailovou informaci o zjištěné neshodě administrátorovi řešení.
2	5	Rotace hesel	Řešení musí poskytovat pravidelnou rotaci hesel, založenou na časovém limitu nebo v plánovaných intervalech.	Součástí politiky při konfiguraci účtů spravovaných CyberArk PAM je i definování periody platnosti hesla, kdy dojde k automatické změně hesla před uplynutím této periody.
2	6	SSH a RDP Proxy	Řešení musí poskytovat funkcionalitu proxy pro vzdálená SSH a RDP připojení.	Relace na koncové systémy je možné navázat pomocí RDP, nebo SSH proxy připojení.
2	7	Automatické spuštění vzdáleného sezení	Řešení musí umožnit automatické spuštění vzdáleného sezení (remote session) bez	Přihlašování na koncové systémy pomocí účtů spravovaných v CyberArk PAM je realizováno bez potřeby zobrazení autentizačních údajů uživateli.

			odhalení přihlašovacích údajů.	
2	8	Zobrazení přihlašovacích údajů	Řešení musí obsahovat mechanismus pro zobrazení přihlašovacích údajů v čitelné podobě v případě nedostupnosti síťového propojení na daný systém, pokud je samozřejmě uživatel dostatečně oprávněn.	U účtů spravovaných v rámci CyberArk PAM je možné zobrazení uložených autentizačních údajů, pokud má k této operaci přihlášený uživatel pro daný účet oprávnění.
2	9	Webový přístup	Řešení musí být ovladatelné pouze pomocí webového prohlížeče, bez nutnosti používat těžkého klienta. Komunikace s webovým serverem je prováděna přes protokol HTTPS.	Ovládání přístupů uživatelů je v rámci webového rozhraní pomocí komponenty CyberArk Password Vault Web Access a kdy tak není zapotřebí SW třetích stran. Komunikace s webovým rozhraním je přes protokol HTTPS.
2	10	Nezávislost webového prostředí	Webové rozhraní řešení nesmí být závislé na softwaru třetích stran, jako je například Adobe Flash Player a Silverlight.	Webové rozhraní CyberArk PVWA je podporováno v běžných webových prohlížečích a nevyžaduje další SW třetích stran.
2	11	Dočasné povolení přístupů	Řešení musí umožňovat dočasné povolení k užívání přístupových údajů na základě žádosti.	CyberArk PAM disponuje funkcí schvalovacího workflow, které umožňuje generování žádostí o přístup ke spravovaným účtům na definovaný časový interval a následně dvouúrovňové schvalování těchto žádostí.
2	12	Vypůjčení a vrácení přístupových údajů	Řešení musí podporovat schopnost vypůjčení/vrácení přístupových údajů (takzvaný Check-in a Check-out).	Účty je možné nastavit jako exkluzivní, kdy je povoleno připojení pouze jednomu uživateli v čase pomocí tzv. check-out a check-in autentizačních údajů.
2	13	Vynucené navrácení přístupových údajů	Řešení musí umožňovat vynucené navrácení zapůjčených přístupových údajů, tedy vynucený Check-out.	Účty je možné nastavit jako exkluzivní, kdy je povoleno připojení pouze jednomu uživateli v čase pomocí tzv. check-out a check-in autentizačních údajů. Uvolnění účtu k dalšímu použití může být buď manuální, nebo automatické po uplynutí definovaného intervalu.

2	1 4	Schvalovací procesy žádostí o přístupy	Řešení umožňuje vytvářet vlastní schvalovací procesy kolem žádostí o přidělení přístupu. Musí být možné nastavit automatické, jednoúrovňové a víceúrovňové schvalování.	CyberArk PAM disponuje funkcí schvalovacího workflow, které umožňuje generování žádostí o přístup ke spravovaným účtům na definovaný časový interval a následně jedno nebo dvouúrovňové schvalování těchto žádostí.
2	1 5	Remote Password Changing	Řešení musí podporovat automatizaci změn hesel řízených událostmi - Remote Password Changing před a po použití secretu.	CyberArk PAM podporuje tzv. one-time password, kdy je po použití účtu jeho heslo automaticky řešením orotováno. Případně je možné účty nastavit jako exkluzivní, kdy je povoleno připojení pouze jednomu uživateli v čase.
2	1 6	Integrace ticketovacích systémů	Do vlastních schvalovacích procesů v rámci řešení je nutné mít možnost integrovat stávající ticketovací nástroje např. ServiceNow, BMC, atd.	Podporované ticketovací nástroje jsou Service Now a BMC Remedy.
2	1 7	Jednorázové heslo	Řešení musí podporovat metodu jednorázového přístupu a vygenerování jednorázového hesla s určitou časovou životností.	CyberArk PAM podporuje tzv. one-time password, kdy je po použití účtu jeho heslo automaticky řešením orotováno. Případně je možné účty nastavit jako exkluzivní, kdy je povoleno připojení pouze jednomu uživateli v čase.
2	1 8	Automatizace procesů	Řešení musí podporovat automatizaci procesů řízených událostmi v rámci platformy, aby správci mohli vytvářet přizpůsobené pracovní postupy, které mohou být automaticky spouštěny událostmi ovlivňujícími přihlašovací údaje v rámci PAM. Příklad RPC - Remote Password Changing před a po použití secretu.	CyberArk PAM podporuje tzv. one-time password, kdy je po použití účtu jeho heslo automaticky řešením orotováno. Případně je možné účty nastavit jako exkluzivní, kdy je povoleno připojení pouze jednomu uživateli v čase.

2	19	Podpora tagů nebo full search	Řešení musí podporovat volně konfigurovatelné Tagy pro označení účtů nebo možnost full search pro následné zjednodušené vyhledávání, filtrování apod. (např. typ systémů, kritičnost atd.).	Kartu parametrů účtů spravovaných v CyberArk PAM lze rozšířit o vlastní atributy, které lze následně použít i pro vyhledávání konkrétních účtů či jejich filtraci.
2	20	Upozornění na změnu hesla	Řešení musí umět zasílat upozornění na pokusy o změnu nebo reálně provedené změny k danému uloženému heslu. Jakákoliv změna jeho konfigurace nebo jeho sdílení povede k upozornění vlastníka nebo administrátora.	Změny autentizačních údajů (hesla, SSH klíče, apod.) jsou auditovány a jsou logovány, včetně například zaslání informace o změně pomocí Syslog. Zároveň je možné nastavit emailové notifikace na konkrétní situace - například zaslání emailové notifikace administrátorovi v případě neúspěšné rotace hesla.
2	21	Řízení aplikačních účtů	Řešení poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. Řešení umožňuje odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. Systém musí umožňovat různé API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty.	Součástí nabízeného řešení je i tzv. CyberArk Credential Provider, což je SW část instalovaná na server, na kterém se mají bezpečným způsobem používat současné hard-coded autentizační údaje. Credential Provider například obsahuje binární soubory, které lze použít ve skriptech pro vyčtení autentizačních údajů. Bezpečnost použití takového volání ve skriptech je pak možné ošetřit ověřováním kontrolního součtu skriptu, IP adresy nebo hostname, na kterém je skript spuštěn, kontrolou uživatelského jména, pod kterým je skript spuštěn, apod. Pokud nebudou tyto kontroly úspěšné, volání k vyčtení autentizačních údajů žádné autentizační údaje nevrátí. Pro vyzvedávání autentizačních údajů lze zároveň použít i tzv. Central Credential Provider, který je centralizovanou analogií uvedeného SW instalovaného na každý server. Autentizační údaje spravované CyberArk PAM jsou zároveň vyčitatelné i přes REST API.
2	22	Bezpečná autentizace aplikací	Řešení musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů (například dle hostname/IP adresa aplikačního serveru, certifikátu, dvoufaktorové ověření). Příklad: aplikace, nebo skript,	Součástí nabízeného řešení je i tzv. CyberArk Credential Provider, což je SW část instalovaná na server, na kterém se mají bezpečným způsobem používat současné hard-coded autentizační údaje. Credential Provider například obsahuje binární soubory, které lze použít ve skriptech pro vyčtení autentizačních údajů. Bezpečnost použití takového volání ve skriptech je pak možné ošetřit ověřováním kontrolního součtu skriptu, IP adresy nebo hostname, na kterém je skript spuštěn, kontrolou uživatelského jména, pod kterým je skript spuštěn, které tak může sloužit jako další faktor k ověření. Pokud nebudou tyto kontroly úspěšné, použité volání k vyčtení autentizačních údajů žádné autentizační údaje nevrátí.

			který používá uložené secrety by měla využívat nativní SDK řešení nebo API pro autentifikaci a autorizaci, případně využití uživatelského dvoufaktorového ověření, pokud uživatel spouští skript manuálně.	
2	2 3	Vulnerability Scanners – RPA - Orchestration/Response	Řešení musí umožňovat integraci s nástroji typu Vulnerability Management nebo RPA pro automatické a bezpečné vyzvedávání secrets pomocí API rozhraní.	CyberArk PAM podporuje širokou řadu integraci s nástroji sloužícími pro skenování zranitelností jako jsou Qualys, Rapid7, Tenable apod. (https://cyberark.my.site.com/mplace/s/#---Category__c-VulnerabilityManagement) a zároveň obsahuje REST API pro přístup k uloženým autentizačním údajům.
3. Řízení vzdálených relací				
3	1	Izolace relací	Izolace session je zprostředkována bez agenta pomocí JumpServeru/RD S Serveru/SSH proxy nebo pomocí agenta. Agentské řešení musí poskytovat flexibilní možnosti spuštění relací a musí umožňovat alespoň všechny následující metody definované v podbodech 3.1.1., 3.1.2. a 3.1.3 (pro bezagentské řešení jsou tyto body nerelevantní a uchazeč vyplní do popisu N/A).	Veškeré relace navázané v rámci CyberArk PAM na koncový systém jsou navazovány ze serverů CyberArku, a to konkrétně z Windows RDS serverů (tzv. RDP proxy), nebo z Linux SSH proxy serverů. Uživatelské relace jsou tak navazovány pouze na tyto uvedené servery, čímž dojde k oddělení/izolaci těchto dvou relací.
3	1. 1	Izolace relací	Spuštění relace založené na agentovi, který otevře aplikaci lokálně na počítači uživatele a připojí uživatele přímo k cílovému serveru bez ničeho mezi tím.	N/A
3	1. 2	Izolace relací	Spuštění relace založené na agentovi, který otevře aplikaci lokálně na	N/A

			počítači uživatelů a proxy relaci prostřednictvím řešení PAM. Proxy server musí podporovat SSH, RDP a obecnou relaci TCP.	
3	1. 3	Izolace relací	Zásuvný modul / rozšíření webového prohlížeče, které automaticky vloží přihlašovací údaje do odpovídajících polí na stránkách. Plugin musí být k dispozici ve všech standardních prohlížečích: Edge, Chrome, Firefox a Safari alespoň.	N/A
3	2	Nahrávání relací	Pro všechny výše uvedené možnosti spuštění relace musí být k dispozici možnosti nahrávání relací ve videu a textu.	CyberArk PAM zaznamenává relace navázané na koncový systém v podobě videa a metadat v případě RDP proxy připojení, a v textové podobě včetně metadat s možností přehrání jako videosekvence v případě SSH proxy připojení.
3	3	Vyhledávání v nahrávkách	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat - minimálně u SSH relací jednotlivé příkazy. Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp...) a je	Relace navázané v rámci CyberArk PAM na cílový server jsou auditovány v podobě záznamu souvislé videosekvence samotné relace doplněné o metada relace (úhozy kláves, názvy spuštěných oken). Tento audit se děje bez potřeby instalace agenta či jiné SW komponenty na cílový server. Nahrané relace je možné prohledávat podle parametrů účtů použitých pro připojení a podle metadat relace. Přehrání zaznamenané relace v rámci webového rozhraní CyberArk PAM nevyžaduje žádný dodatečný SW.

			dostupné z GUI dodávaného řešení.	
3	4	Záznam metadat	Navrhované řešení musí umožňovat záznam metadat, jako je Keystroke pro SSH a RDP session bez instalace jakéhokoliv agenta na cílový server.	Relace navázané v rámci CyberArk PAM na cílový server jsou auditovány v podobě záznamu videosekvence samotné relace doplněné o metada relace (úhozy kláves, názvy spuštěných oken). Tento audit se děje bez potřeby instalace agenta či jiné SW komponenty na cílový server.
3	5	Detekce stisků kláves	Navrhované řešení musí zaznamenávat stisky kláves všech aplikací spuštěných ze jumpserveru (Microsoft RDS Server).	CyberArk PAM umožňuje auditování uživatelských relací navázaných přes řešení. Součástí auditu jsou kromě záznamu videosekvence i metadata, kterými jsou úhozy kláves, nebo názvy otevřených oken v případě Windows prostředí.
3	6	Předkonfigurované spouštěče aplikací	Navrhované řešení musí poskytovat předkonfigurované spouštěče aplikací pro spuštění relací (RDP, SSH, PowerShell, SSMS atd.).	CyberArk PAM obsahuje vyšší desítky předpřipravených integrací, které se následně používají pro definování parametrů účtů sloužících k připojení na koncové systémy. Přehled out-of-box integrací je například dostupný na stránkách CyberArk Marketplace (https://cyberark.my.site.com/mplace/s/).
3	7	Prohledávání záznamů	Všechna metadata zachycená navrhovaným řešením musí být prohledávatelná a kombinovaná s videozáznamem, aby auditor mohl přeskočit na přesné místo ve videu, kde byla metadata zachycena.	Záznam relací na koncový systém je obohacen o metada, pomocí kterých lze záznamy prohledávat a následně tato metada použít pro určení místa v relaci, kde se tato metada vyskytla.
3	8	Vlastní spouštěče aplikací	Řešení musí poskytovat možnost přidat vlastní spouštěče relací aplikací, které mají být konfigurovány bez nutnosti profesionálních služeb.	Přidávání nových účtů do CyberArk PAM řešení, které uživatelé následně používají pro navázání relací na koncový systém, se provádí v rámci webového rozhraní CyberArk PVWA, kde se pouze definují parametry účtu a vybere se tzv. platforma, která definuje způsob připojení na koncový systém a postupy pro automatickou práci s daným účtem (změna hesla, verifikace hesla apod.). Přidání účtu pro nové relace je tak velice jednoduché.
3	9	Command block-listing	Řešení musí poskytnout metodu pro řízení příkazů, které uživatel	CyberArk PAM umožňuje v rámci SSH proxy definovat tzv. Command Access Control, což jsou allow a deny seznamy příkazů sloužící k povolení či zakázání v rámci relace.

			může na koncovém systému využívat v rámci jeho SSH session na základě přístupu Commands Block-listing a Allow-listing.	
3	10	Podpora SUDO a SU	Řešení musí poskytnout metodu automatického vkládání přihlašovacích údajů sudo/su na spuštěných relacích SSH, když uživatel provede zvýšené příkazy bez odhalení hesla.	CyberArk PAM umožňuje použití automatického vkládání přihlašovacích údajů při použití příkazů typu sudo/su. Tímto způsobem je například zajištěno přihlašování pomocí tzv. logon účtů v případech, kdy není povoleno SSH přihlášení účtem root na koncový systém. V rámci logon skvencí je možné tuto funkcionalitu použít i pro další příkazy v rámci SSH relací.
3	11	Terminace relací	Řešení musí umožňovat administrátorům monitorovat sezení v téměř reálném čase a existuje možnost, v případě nutnosti, sezení manuálně ukončit.	CyberArk PAM umožňuje přistoupit autorizovanému účtu k probíhající relaci a v případě potřeby relaci ukončit.
3	12	Možnost sledování relací v reálném čase	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol).	CyberArk PAM umožňuje přistoupit autorizovanému účtu k probíhající relaci v rámci webového prohlížeče a HTTPS protokolu.
3	13	Historická kontrola relací	Řešení umožňuje autorizovanému personálu centrálně prohledávat v nahrávkách podle data, systému a uživatele.	V uložených nahrávkách je možné vyhledávat jak podle parametrů použitých účtů, tak i podle metadat uložených u nahrávek. Prohledávací okno je možné omezit časovým intervalem.
4. Audit a reporting				
4	1	Auditing nástroj	Řešení musí zahrnovat auditní stopy všech interních i externích	Auditovány jsou v rámci CyberArk PAM jak externí aktivity uživatelů přistupující k spravovaným účtům, tak i interní aktivity řešení, kdy například interní automatizace verifikuje či mění heslo spravovaného účtu.

			činností a akcí v rámci platformy.	
4	2	Reporting nástroj	Řešení poskytuje integrovaný reportovací nástroj s předpřipravenými reporty a možností vytváření vlastních reportů.	CyberArk PAM obsahuje sadu reportů pro zobrazení aktivit, oprávnění k účtům, compliance apod., které je možné parametrizovat k vytvoření reportu s požadovaným výstupem.
4	3	Zobrazení aktivit uživatele	Řešení musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.	Veškeré operace provedené nad účty spravované řešením jsou auditované a je zajištěna tzv. accountability - je jednoznačně identifikován uživatel, který danou aktivitu provedl. Aktivita provedené nad jednotlivými účty jsou dostupné v podobě textových záznamů u těchto účtů v rámci webového rozhraní, případně je možné tyto aktivity zobrazit v rámci reportů.
4	4	Audit administrátorských akcí	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.	Veškeré operace provedené nad účty spravované řešením jsou auditované a je zajištěna tzv. accountability - je jednoznačně identifikován uživatel, který danou aktivitu provedl. Aktivita provedené nad jednotlivými účty jsou dostupné v podobě textových záznamů u těchto účtů v rámci webového rozhraní, případně je možné tyto aktivity zobrazit v rámci reportů.
4	5	Přístup k reportům	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele nebo role.	Přístup k funkci reportů je zajištěn pomocí role/oprávnění pro uživatele či skupinu uživatelů.
4	6	Nezpochybnitelný auditní záznam	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy.	Veškeré operace provedené nad účty spravované řešením jsou auditované a je zajištěna tzv. accountability - je jednoznačně identifikován uživatel, který danou aktivitu provedl. Aktivita provedené nad jednotlivými účty jsou dostupné v podobě textových záznamů u těchto účtů v rámci webového rozhraní, případně je možné tyto aktivity zobrazit v rámci reportů.
4	7	Zabezpečení auditních záznamů	Auditní záznamy a logy veškerých aktivit v zabezpečeném úložišti jsou chráněné proti změnám a smazání všemi uživateli (včetně všech administrátorských rolí řešení). Auditní záznamy musí být bezpečně uloženy, tak aby k nim měl přístup pouze oprávněný uživatel.	Žádná role ani oprávnění v řešení neumožňuje změnit či smazat auditní záznam, včetně náhravek. Přístup k auditním záznamům je pouze read-only a je definován oprávněním.
4	8	Omezení mazání náhravek relací	Žádná role řešení včetně všech administrátorských rolí nesmí být jakkoliv schopná	Řešení umožňuje definovat dobu retence dat, včetně náhravek. Případná změna retence náhravek se dotkne až náhravek nových. Žádná role v CyberArk PAM nemá oprávnění ke smazání či změně náhravek. Role může mít definováno maximálně read oprávnění k přístupu k náhrávkám.

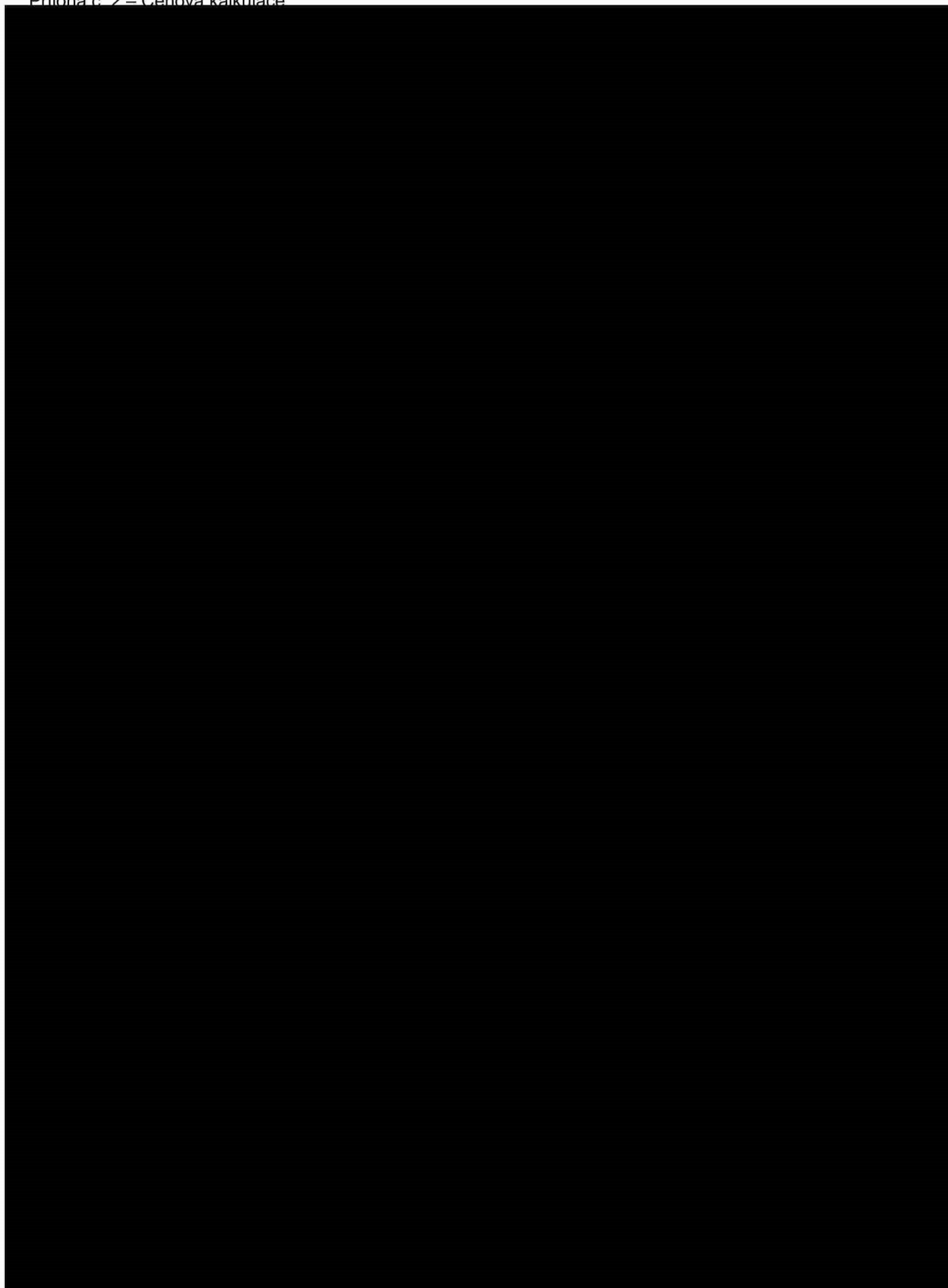
			smazat nahrávky relací a řešení musí zajistit, že nahrávky budou dostupné po původně nastavenou dobu bez ohledu na pozdější změnu konfigurace.	
4	9	Integrace se SIEM	Řešení musí podporovat předávání protokolů na libovolnou platformu SIEM a podporovat formát protokolů syslog i CEF.	CyberArk PAM podporuje out-of-box integraci se SIEM systémy ArcSight, enVision, Qradar, McAfee ESM a zároveň obsahuje prostředky v podobě XSL pro integraci do dalších SIEM systémů. Logy je možné zasílat v CEF formátu pomocí Syslog protokolu.
5. Infrastrukturní a architektonické požadavky				
5	1	Vysoká dostupnost řešení	Řešení musí podporovat nasazení ve vysoké dostupnosti, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat.	Nabízené řešení umožňuje distribuované nasazení jednotlivých komponent v HA režimu. V případě DR scénáře jsou stále aplikovány bezpečnostní konfigurace stejně jako v případě standardního provozu. Zálohování dat je zajištěno zálohou databáze Digital Vault, která je souborová a šifrovaná.
5	2	Automatická instalace	Veškeré komponenty řešení musí umožňovat automatickou instalaci v cloud i on-premise prostředí. Řešení minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci.	CyberArk PAM je možné provozovat jak on-premise, tak i v cloud prostředí. Řešení se instaluje na OS Windows a Linux, kdy výrobce poskytuje sady skriptů pro kontrolu připravenosti OS, samotnou instalaci komponent, či jejich hardening.
5	3	Administrátoři řešení	Administrátoři řešení jsou účty vytvořené lokálně pomocí administračního rozhraní v bezpečném úložišti dat pro konfigurační a nouzové účely. Tyto účty nejsou synchronizovány s AD nebo jakýmkoliv jiným prostředím kromě úložiště	Účty systému CyberArk PAM mohou být jak externí (AD, LDAP, apod.) tak i interní. Tyto interní účty nejsou synchronizovány s externím adresářem a běžně se používají pro administraci a jako break-glass účty pro nouzové situace. Účty jsou uloženy v zabezpečeném centrálním datovém úložišti - Digital Vault.

			dat řešení a budou použity pouze pro počáteční nasazení, údržbu a v případě potřeby ve scénáři Break-Glass.	
5	4	Hardening úložiště dat	Řešení musí poskytovat automatický hardening úložiště dat, který bude nezávislý na zásahu správců systémů a bude minimalizovat možnou lidskou chybu. Musí se jednat o standardizovaný postup, jehož stabilita a bezpečnost je ověřená z předchozích nasazení řešení.	Data systému CyberArk PAM jsou uložena v centrálním databázovém úložišti - Digital Vault, které pro bezpečné uložení používá prostředky asymetrické kryptografie. V této centrální databázi jsou uloženy spravované účty, konfigurace, logy, auditní nahrávky apod. Digital Vault se instaluje na OS Windows Server, kdy je při instalaci OS hardenován instalačními skripty dle bezpečnostního nastavení výrobce.
5	5	Break glass scénáře	Řešení musí pokrývat tzv. "break glass" scénáře s postupy, jak jednat v situacích s fatálním dopadem na PAM systém. Dodavatel uvede rámcový popis pro řešení disaster recovery a break-glass scénářů, který bude detailně rozpracován při analýze.	Během fáze Analýza bude definován proces nouzového přístupu na koncové systémy v případě nemožnosti použít k tomuto běžné účty spravovaného nabízeným řešením. Pro tento nouzový přístup budou definovány tzv. break-glass účty, které budou ideálně lokální na všech koncových systémech, aby jejich použití nebylo závislé na funkci jiné infrastrukturní služby (síť, adresářové služby, apod.), budou zároveň nakonfigurovány v nabízeném řešení CyberArk PAM, které bude pravidelně ověřovat, že účty jsou funkční (heslo neexpirovalo, nebylo změněno, apod.). Použití těchto účtů je následně vhodné vyhodnocovat v SIEM nástroji, který bude identifikovat přihlášení na koncový systém pomocí break-glass účtu. Kritické komponenty budou nasazeny v režimu vysoké dostupnosti a ve více instancích s ohledem na maximálně zabezpečenou architekturu. To včetně centrální komponenty Digital Vault, která může být nasazena v režimu active-pasive v různých geograficky oddělených lokalitách, kdy se pasivní komponenta synchronizuje s aktivní a v případě výpadku aktivní komponenty kompletně přebírá její funkci a ostatní komponenty řešení se automaticky přeregistrují na komunikaci s touto novou databázovou komponentou.
5	6	Data-at-rest	Navrhované řešení musí chránit data-at-rest. Popište prosím, jak navrhované řešení splňuje tento požadavek.	Data systému CyberArk PAM jsou uložena v centrálním databázovém úložišti - Digital Vault, které pro bezpečné uložení používá prostředky asymetrické kryptografie. V této centrální databázi jsou uloženy spravované účty, konfigurace, logy, auditní nahrávky apod. Digital Vault a další komponenty řešení jsou například v souladu se standardem FIPS 140-2.
5	7	Data-in-motion	Navrhované řešení musí chránit data-in-motion. Popište prosím, jak navrhované řešení splňuje tento požadavek.	Veškerá komunikace mezi komponentami CyberArk PAM řešení probíhá pomocí proprietárního šifrovaného protokolu. Stejně tak i přístup uživatelů k webovému rozhraní CyberArk PVWA je zabezpečen protokolem HTTPS.
6. Výkonové a kapacitní požadavky				

6	1	Počet uživatelů	Řešení musí být kapacitně dimenzované minimálně pro 50 souběžných uživatelů pro Fázi 1. Pro Fázi 2 musí být řešení dimenzované pro dalších minimálně 250 souběžných uživatelů. Tedy po Fázích 1 a 2 musí být řešení celkově dimenzované pro minimálně 300 souběžných uživatelů.	Nabízené řešení je škálovatelné co se týče výkonostních a kapacitních požadavků. Různé požadavky na kapacitu či výkonost se naplňují různě výkonnými servery či navýšením jejich počtu. Přesný počet požadovaných serverů bude identifikován v rámci fáze analýza, kdy bude zohledněn požadavek na počet současně navázaných relací společně s návrhem architektury.
6	2	Retence nahrávaných relací privilegovaných uživatelů	Řešení musí být dimenzované tak, aby uchovávalo nahrávky relací minimálně po dobu 365 dní.	Požadavek na retenci dat bude zohledněn při návrhu architektury řešení během fáze Analýza, kdy budou navrženy dostatečné kapacity a výkonostní parametry serverů tak, aby byla zajištěna požadovaná retence 365 dní.
6	3	Počet spravovaných hesel v bezpečném úložišti	Řešení musí být dimenzované tak, aby umožňovalo uložit minimálně 15 tisíc hesel.	Řešení založená na produktu CyberArk PAM jsou škálovatelná co se týče výkonostních a kapacitních požadavků. Různé požadavky na kapacitu či výkonost se naplňují různě výkonnými servery či navýšením jejich počtu. Požadavek na uložení 15 tisíc hesel bude zohledněn při návrhu ve fázi Analýza.
6	4	Zajištění vysoké dostupnosti	Celé řešení musí splňovat zajištění vysoké dostupnosti včetně umístění klíčových komponent (databáze/trezor hesel) ve dvou geograficky oddělených lokalitách. DR scénáře musí při úplném výpadku primární lokality počítat s možností okamžitého přístupu k uloženým datům (heslům) z lokality druhé.	Nabízené řešení umožňuje distribuované nasazení jednotlivých komponent v HA režimu. Během fáze Analýza dojde k návrhu takové architektury řešení, aby byla zajištěna požadovaná HA a DR funkcionalita.
6	5	Provozní Dohled systému	Řešení musí být integrované do centrálního monitorovacího systému ŘLP. Součástí integrace je základní ICMP stav serverů a kontinuální snmp monitoring klíčových parametrů pro chod systému a určení jejich optimálních, varovných a	CyberArk PAM je provozován na standardní HW platformě a operačních systémech Windows a Linux, které je možné monitorovat klasickým způsobem, jako jiné servery s těmito OS.

			kritických hodnot. Typicky se monitoruje vytížení RAM, CPU, HDD, stavy běžících procesů, případně monitoring HW (větráky, teplota, apod).	
6	6	Škálovatelnost	Řešení musí být jednoduše škálovatelné dokoupením licencí nebo zvýšením výkonu jednotlivých komponent	Architekturu CyberArk PAM je možné rozšiřovat instalací dalších komponent podle aktuálních výkonových a kapacitních požadavků.
7. Ostatní požadavky				
7	1	HW	Provoz nabízeného řešení musí být realizovatelný s HW, který je běžně dostupný na trhu. HW není součástí předmětu plnění.	Nabízené řešení je možné provozovat na běžně dostupném serverovém HW architektury x86 (32-bit, 64-bit), které je patřičně dimenzováno s ohledem na prostředí a požadavky zákazníka.
7	2	Omezení Open source	Nabízené řešení nesmí být založeno na tzv. Open Source technologii.	Nabízené řešení je založené na produktu CyberArk PAM od společnosti CyberArk. Jedná se o komerční produkt veřejně obchodovatelné společnosti, která je leader v oblasti systémů pro správu identit, privilegovaných účtů a bezpečného přístupu za použití těchto účtů.

Příloha č. 2 – Cenová kalkulace



2. Preambule

Tato dílčí smlouva je uzavíraná na základě rámcové dohody č. 181/2023/IS/140, uzavřené mezi smluvními stranami dne [*] (dále jen „**rámcová dohoda**“). Tato dílčí smlouva blíže určuje předmět rámcové dohody, co do druhu a množství a specifikuje konkrétní dílčí plnění, které musí být v souladu s rámcovou dohodou.

3. Předmět dílčí smlouvy

- 3.1 Touto dílčí smlouvou se zhotovitel zavazuje na základě rámcové dohody objednateli poskytnout nevýhradní licence pro území České republiky, v rozsahu a v souladu se specifikací dle Přílohy č. 1 této dílčí smlouvy (dále jen „**Licence**“).
- 3.2 Objednatel se zavazuje Licence převzít a zaplatit za ně odměnu za podmíněk stanovených v rámcové dohodě a této dílčí smlouvě.
- 3.3 Zhotovitel se zavazuje předat objednateli dokumentaci k Licencím v souladu s odst. 14.1.6 rámcové dohody.

4. Cena

- 4.1 Cena za Licence podle této dílčí smlouvy činí:

[*] Kč

(slovy: [*] korun českých) bez DPH za měsíc.

- 4.2 K ceně uvedené v této dílčí smlouvě bude účtována příslušná sazba DPH v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
- 4.3 Cena za předplatné Licencí bude uhrazena na základě faktury - daňového dokladu vystaveného nejdéle do 15 kalendářních dnů ode dne uskutečnění zdanitelného plnění, přičemž za den uskutečnění zdanitelného plnění je považován den poskytnutí Licence. Na faktuře musí být uvedeno období, za které se předplatné Licencí platí.

5. Termín a způsob plnění

- 5.1 Zhotovitel se zavazuje předat objednateli Licence podle této dílčí smlouvy nejpozději do [*] kalendářních dnů od zveřejnění této dílčí smlouvy v registru smluv.
- 5.2 O předání Licencí smluvní strany podepíší protokol o řádném předání a převzetí plnění.

6. Místo plnění

- 6.1 Licence budou v termínu dle článku 5 této dílčí smlouvy předány objednateli v sídle objednatele uvedeném v článku 1 této dílčí smlouvy.

7. Smluvní pokuty

- 7.1 V případě, že zhotovitel nedodrží termín předání Licencí podle této dílčí smlouvy, je zhotovitel povinen zaplatit objednateli smluvní pokutu ve výši 0,05 % z ceny dle této dílčí smlouvy za každý započatý den prodlení.
- 7.2 Smluvní pokuta podle této dohody je splatná do 30 dnů od doručení písemné výzvy k její úhradě zhotoviteli.

- 7.3 Odchylně od § 2050 občanského zákoníku se smluvní strany dohodly, že sjednání jakékoli smluvní pokuty se nedotýká práva na náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje, a nárok na náhradu škody může být uplatněn nezávisle na smluvní pokutě a v plné výši.

8. Závěrečná ustanovení

- 8.1 Tuto dílčí smlouvu lze měnit nebo doplňovat pouze písemně výslovným oboustranně potvrzeným smluvním ujednáním, a to ve formě dodatku k této dílčí smlouvě, podepsaným oprávněnými zástupci obou smluvních stran.
- 8.2 Tato dílčí smlouva vstupuje v platnost dnem podpisu obou smluvních stran a účinnosti nabývá dnem jejího uveřejnění v registru smluv.
- 8.3 Při uveřejnění této dílčí smlouvy v registru smluv budou v jejím textu znečitelněny zejména tyto údaje: bankovní spojení zhotovitele v článku 1 této dílčí smlouvy, podpisy na dílčí smlouvě a dále obchodní tajemství ve smyslu § 504 občanského zákoníku, kterým je kalkulace ceny v příloze č. 1 této dílčí smlouvy.
- 8.4 Obě smluvní strany prohlašují, že jednotlivé články této dílčí smlouvy jsou dostatečné z hlediska náležitosti pro vznik smluvního vztahu, a že bylo využito smluvní volnosti stran a tato dílčí smlouva se uzavírá určitě, vážně a srozumitelně.
- 8.5 **Tato dílčí smlouva se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**
- 8.6 Nedílnou součástí této dílčí smlouvy je její Příloha č. 1 – Rozsah a specifikace plnění

.....
objednatel

[*]
[*]

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

.....
zhotovitel

Mgr. Dan Rosendorf
předseda představenstva
ICZ a.s.

Specifikace analýzy prostředí objednatele

1. Obecné požadavky:

- 1.1 Analýza bude zadavateli předána ve formě Microsoft Word a bude v českém jazyce. Mohou v ní být použité části v anglickém jazyce, např. ilustrace přímo od výrobce technologie apod., ale s doplňujícím vysvětlením, případně výkladem odborných pojmů v českém jazyce.
- 1.2 Analýza bude obsahovat veškeré informace potřebné pro následnou implementaci systému PAM do prostředí objednatele.
- 1.3 Analýza musí obsahovat dostatečně detailní popis HW (a souvisejícího SW) potřebného pro implementaci systému PAM. V Analýze budou popsány jednotlivé druhy požadovaného HW s parametry a počty kusů.
- 1.4 Některé z bodů Analýzy (např. disaster recovery proces) mohou být vzhledem ke svojí specifické povaze vázané na způsob implementace PAM řešení. Pokud se takové vyskytnou, musí být během fáze Analýzy popsány minimálně základní specifikací. Finální a detailní dokumentace takových bodů bude součástí dokumentace předávané dle odst. 3.2.1.8 rámcové dohody.

2. Obsahové požadavky:

- 2.1 Analýza bude popisovat minimálně tyto body:
 - 2.1.1. Základní popis řešení, technologií a technických konceptů.
 - 2.1.2. Obecné technické předpoklady a požadavky na realizaci řešení.
 - 2.1.3. Architektura řešení s jejím vysvětlením.
 - 2.1.4. Procesy a služby systému s jejich rozpisem a vysvětlením jejich účelu v rámci řešení.
 - 2.1.5. Popis systémů třetích stran a jejich integrace.
 - 2.1.6. Integrační architektura s infrastrukturními a monitorovacími systémy objednatele (SIEM, SNMP, AD, SMTP, NTP).
 - 2.1.7. Popis nakládání s daty, jejich uložení, zabezpečení, ochrana.
 - 2.1.8. Detailní síťový a komunikační model řešení včetně interní komunikace mezi vnitřními prvky řešení.
 - 2.1.9. Návrh politik PAM řešení detailně specifikovaných během analýzy a vycházející z „best practice“ doporučení výrobce technologie.
 - 2.1.10. Technologické požadavky na zajištění provozu.
 - 2.1.11. Popis konfigurace komponent PAM řešení.
 - 2.1.12. Detailní popis instalačních postupů, a to včetně testovacího prostředí.
 - 2.1.13. Detailní popis zálohování a obnovy PAM systému, řešení DR scénářů včetně návrhů testovacích scénářů zahrnujících totální výpadek a obnovy do provozního stavu (bude součástí akceptačních testů).
 - 2.1.14. Návrh metodiky nakládání s break-glass účty a scénáře na jejich otestování (bude součástí akceptačních testů).
 - 2.1.15. Popis způsobů aktualizace PAM řešení (všechny části PAM).
 - 2.1.16. Bezpečnostní zajištění řešení včetně souladu se ZoKB.
 - 2.1.17. Soulad s GDPR.
 - 2.1.18. Monitoring PAM řešení.
 - 2.1.19. Návrh harmonogramu projektu a procesních kroků pro implementaci řešení včetně návrhu konfigurace řešení v jednotlivých fázích implementace a definice finální podoby

dodávaného řešení. Harmonogram musí být v souladu s termíny plnění stanovenými v Rámcové dohodě č. 181/2023/IS/140.

- 2.1.20. Popis náběhu systému (popis pilotní/zkušební fáze až do doby akceptace).
- 2.1.21. Postup testování a testovacích scénářů.
- 2.1.22. Požadavky na součinnost.
- 2.1.23. Detailní specifikace lokální podpory zhotovitele potažmo výrobce a definování postupů pro její využití.
- 2.1.24. Specifikace a rozsah školení zástupců objednatele (v rozsahu standardizovaných školení administrátorů od výrobce technologie).
- 2.1.25. Návrh maximálně automatizovaného discovery procesu privilegovaných účtů po zavedení PAM.
- 2.1.26. Návrh na provádění assesment analýz Systému PAM zaměstnanci objednatele (četnost, rozsah, hlavní oblasti assesmentu, automatizace assesment procesu, scoring apod.).
- 2.1.27. Návrh procesu technické profylaxe PAM řešení (musí probíhat minimálně jednou ročně) ze strany zhotovitele, případně za součinnosti s výrobcem.

2.2 Analýza musí zohlednit specifika ATM systémů zejména v těchto bodech:

- 2.2.1. ATM systémy jsou součástí kritické informační infrastruktury dle ZoKB.
- 2.2.2. Dostupnost ATM systémů je velmi kritická.
- 2.2.3. Administraci ATM systémů provádí certifikovaný personál – ATSEP.
- 2.2.4. Administrace ATM systémů probíhá dosud odděleně od administrace ostatních systémů ŘLP, v rámci nasazení PAM se požaduje konsolidace.
- 2.2.5. Konsolidací administrace nesmí dojít ke zvýšení bezpečnostních rizik.
- 2.2.6. Součástí konsolidace administrace musí být konsolidace stávajících JUMP serverů objednatele, jak technologicky, tak i vytvoření hardening pravidel.
- 2.2.7. Zajištění vzdáleného přístupu pro administrátory a dodavatele ATM.
- 2.2.8. Přenos souborů musí být řízen a zaznamenáván.
- 2.2.9. Bezpečnostní kontroly souborů a dat vstupujících do ATM systémů musí být prováděny před vstupem do ATM systémů.
- 2.2.10. ATM systémy jsou designovány na provoz v oddělených chráněných sítích, proto je izolace session z okolních prostředí kritická.
- 2.2.11. V ATM systémech není možné nasazovat změny bez asistence dodavatele systému.
- 2.2.12. Změny v ATM systémech vynucují re-certifikace systému, proto většinou nelze využívat standardních bezpečnostních opatření.

2.3 Analýza musí dále obsahovat detailní popis disaster recovery procesu a modelu pro break-glass účty, a to minimálně pro následující scénáře:

- 2.3.1. Kompletní výpadek celého PAM systému.
- 2.3.2. Výpadek některého ze základních systémů ŘLP, např. virtualizační platformy.
- 2.3.3. Výpadek konektivity na některé ze základních prvků PAM.
- 2.3.4. Selhání některého z prvků PAM a doporučený postup pro jeho zálohování a obnovu.
- 2.3.5. Výpadek bezpečného úložiště dat včetně fatálního výpadku, jak primárního, tak sekundárního nodu.
- 2.3.6. Výpadek webového portálu a scénáře pro přístup k úložišti dat.
- 2.3.7. Doporučené postupy na zajištění dostupnosti webového portálu.
- 2.3.8. Výpadek konektivity v prostředí objednatele a řešení přihlašování privilegovaných uživatelů.

- 2.3.9. Doporučené postupy pro nasazení break-glass účtů, způsob úschovy, periodicita změn, nakládání s nimi apod.
 - 2.3.10. Speciální pozornost bude zhotovitel věnovat v DR scénářích síťovým administrátorům a řešení jejich přístupu k síťovým prvkům, které v důsledku nějaké závady nejsou dostupné přes síť, a je nutné se k nim připojovat pomocí lokálního fyzického připojení privilegovaným účtem.
- 2.4 Kromě výše uvedených základních bodů musí zhotovitel v rámci analýzy vytvořit návrh konkrétních kroků včetně stanovení odpovědností pro tyto body:
- 2.4.1. Vytvoření nového uživatele v PAM – Založení nového účtu na úrovni PAM řešení pro uživatele PAM (např. interní/externí administrátor, správce PAM, auditor, popř. další subjekty).
 - 2.4.2. Zrušení uživatele PAM – Zrušení účtu na úrovni PAM řešení v případě, že účet není nadále používán (např. v případě ukončení zaměstnaneckého poměru zaměstnance u objednatele, odebrání účtu externího dodavatele apod.).
 - 2.4.3. Dynamické přidělování/odebírání licencí pro externí uživatele PAM - Návrh postupu dynamického přidělování/odebírání licencí externích uživatelů, který bude optimalizován podle maximálního počtu souběžně připojených externích uživatelů PAM a povede k efektivnímu využití licencí externích uživatelů PAM.
 - 2.4.4. Přidělení/odebrání role uživateli PAM – Přidělení/odebrání role (např. správce PAM, uživatel, auditor) uživateli PAM.
 - 2.4.5. Přidání nového privilegovaného účtu do PAM – Přidání privilegovaného účtu do PAM (např. v případě objevení nového privilegovaného účtu, který má být spravován pomocí PAM), nastavení politik a přidělení privilegovaného účtu k používání konkrétním uživatelům PAM (tj. administrátorům).
 - 2.4.6. Použití privilegovaného účtu – Poskytnutí přístupu uživatele PAM (interního/externího administrátora) k privilegovanému účtu prostřednictvím PAM řešení (tj. v případě že má uživatel přístup schválen).
 - 2.4.7. Použití privilegovaného účtu na vyžádání (elevace oprávnění) – Poskytnutí přístupu uživatele PAM (interního/externího administrátora) k privilegovanému účtu na vyžádání na definované časové období (tj. v případě že daný administrátor nemá standardně k privilegovanému účtu oprávnění, přístup je umožněn pouze na dočasnou dobu na základě schválení). Popis bude zahrnovat i případný onboarding nového účtu, a to se zaměřením na externí privilegované uživatele.
 - 2.4.8. Použití privilegovaného účtu (nouzový přístup) – Poskytnutí nouzového přístupu v případě, kdy je potřeba získat okamžitě přístup k privilegovanému účtu a není dostupný příslušný odpovědný administrátor.
 - 2.4.9. Disaster recovery proces – Poskytnutí přístupu k privilegovaným účtům v případě, že PAM infrastruktura nebo její část není dostupná (např. z důvodu havárie nebo jiné neočekávané události).
 - 2.4.10. Žádost o změnu konfigurace – Zpracování žádosti o změnu konfigurace PAM (např. vytvoření nové/změna stávající politiky).
 - 2.4.11. Revize uživatelů PAM – Provedení revize uživatelů PAM a privilegovaných účtů, kterými jednotliví uživatelé disponují (může být vyřešeno v rámci bodů pro Discovery a Assessment procesy).
 - 2.4.12. Sledování či ukončení relace – Sledování aktivní relace nebo její předčasné ukončení odpovědnou osobou (např. člen dohledového týmu).

- 2.4.13. Žádost o nahrávání relace – Zpracování žádosti o nahrávání relací pro konkrétního uživatele (na vyžádání, pokud PAM systém není nastaven k nahrávání všech relací).
- 2.4.14. Žádost o zpřístupnění nahrávky – Zpracování žádosti o zpřístupnění nahrávky relace pořízené pomocí PAM řešení.

3. Požadavky na strukturu dokumentu:

Struktura Analýzy musí rozsahem odpovídat minimálně tomuto referenčnímu seznamu kapitol:

ÚVOD (Kontext řešení)

PŘEHLED ŘEŠENÍ

- Jednotlivé komponenty řešení
 - Jump server (Windows/Linux)
 - Webová konzole (primární, sekundární, další)
 - Úložiště hesel (primární, sekundární)
 - Úložiště hesel (2. lokalita)
 - Distribuce a řízení hesel
 - Monitorování, nahrávání a řízení relací
 - Řízení HTML relací
 - Vzdálený přístup
 - Multifaktorová autentizace
 - Služby pro zasílání zpráv – email
 - Napojení na SIEM
 - SNMP monitoring
 - LDAP, AD
- Navrhované kontroly (Proposed Controls)

POŽADAVKY

- Kategorie požadavků
- Business požadavky
- Funkční požadavky

ARCHITEKTURA ŘEŠENÍ

- Fyzická architektura
- Rozdělení kritičnosti prostředí
- Infrastrukturní prostředí
- Nástroje síťové bezpečnosti
- Požadavky na porty pro vzdálenou změnu hesla

FUNKČNÍ SPECIFIKACE

- Základní funkční specifikace
 - Správa privilegovaných uživatelů
 - Zdroj uživatelských identit
 - Uživatelé PAM
 - Administrátoři PAM
 - Proces pro přidělování uživatelských přístupů
 - Synchronizace uživatelů
 - Uživatelská autentizace PAM
 - Multi-faktorová autentizace
 - Heslová politika lokální uživatelů
 - Přihlašovací údaje
 - Autorizace
 - Role
 - Skupiny

- Definice privilegovaného přístupu
- Privilegované jmenné účty
- Privilegované nejmenší účty
- Správa PAM
- Počáteční zavádění jmenných účtů
- Přidělování přístupů jmenných účtů
- Odhalení nejmenších účtů
- Monitorování a nahrávání relací
 - Predikce možných scénářů nestandardních stavů
- Specifikace integrace technologických platforem
 - Doménová platforma
 - Platforma Windows technologie
 - Platforma pro databáze
 - Vmware ESXi platforma

PROVOZNÍ SPECIFIKACE

- Zálohování
 - Nastavení zálohování
 - Naplánované úlohy zálohování
 - Obnova záloh
- Nouzový přístup při kritickém výpadku
- Monitorování
 - Konfigurace monitorování
- Logování
 - Druhy integrace
 - SIEM integrační nástroje
 - Logy
- Reportování
 - Reporty přizpůsobené na míru
- Provozní podpora
 - Struktura provozní podpory
 - Provozní doba podpory

PŘÍLOHA

- Příloha A: Slovník

4. Použité zkratky

AD – Active Directory

DR – Disaster Recovery

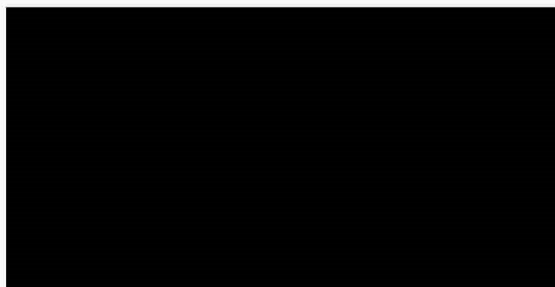
PAM – Privileged Access Management

ZoKB – Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

ÚCL – Úřad pro civilní letectví

Příloha č. 5 – Kontaktní údaje specialisty PAM

Kontaktní údaje specialisty PAM



Příloha č. 6 – Zajištění opatření v oblasti informační a kybernetické bezpečnosti

Zajištění opatření v oblasti informační a kybernetické bezpečnosti

„Smluvní zajištění opatření v oblasti informační a kybernetické bezpečnosti ve smyslu § 8, odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů“

1. Preambule

- 1.1 Zhotovitel bere na vědomí, že je významným dodavatelem dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti pro objednatele Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s. p.), který je správcem informačních a komunikačních systémů kritické informační infrastruktury.
- 1.2 Informačním/komunikačním systémem, k němuž se vztahuje role významného dodavatele, je: **PAM (systém řízení privilegovaných účtů).**
- 1.3 Zhotovitel se zavazuje dodržovat požadavky systému řízení bezpečnosti chráněných informací uvedené v této příloze rámcové dohody a bezpečnostních pravidlech distribuovaných v souladu s čl. 4 této přílohy rámcové dohody.

2. Definice pojmů

- 2.1 „Aktivem“ se rozumí souhrn informací a služeb, které jsou nezbytné pro provozování informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy rámcové dohody.
- 2.2 „Bezpečnostním incidentem“ se rozumí narušení bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy rámcové dohody.
- 2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy rámcové dohody, jeho dostupnosti a spolehlivosti v kybernetickém prostoru.
- 2.4 „Bezpečnostní politikou“ je soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
- 2.5 „Bezpečnostní událostí“ taková událost, která může způsobit narušení bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy rámcové dohody.
- 2.6 „Zhotovitelem“ zhotovitel dle rámcové dohody, který je zároveň významný dodavatel dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti.
- 2.7 „Kritickou informační infrastrukturou“ prvek nebo systém prvků nezbytný pro provozování informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy rámcové dohody.

3. Bezpečnost chráněných informací

- 3.1 Zhotovitel je povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy rámcové dohody a vést o nich bezpečnostní dokumentaci.

- 3.2 Výchozí podmínkou pro nastavení bezpečnostních opatření jsou požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhlášky o kybernetické bezpečnosti, případně norem ČSN ISO/IEC 27001.
- 3.3 Provádění bezpečnostních opatření u zhotovitele ověřuje objednatel postupem dle čl. 8 této přílohy rámcové dohody nebo platným certifikátem ISO/IEC 27001, případně jiným zavedeným a platným mezinárodně uznávaným systémem řízení bezpečnosti informací u zhotovitele.

4. Dodržování bezpečnostní politiky objednatele

- 4.1 Zhotovitel je povinen dodržovat Bezpečnostní pravidla pro významné dodavatele objednatele, která jsou uvedena na následující webové stránce:

https://www.rlp.cz/content/documents/Bezpecnostni_pravidla_pro_vyznamne_dodavatele.pdf

(dále jen „**bezpečnostní pravidla**“). Zhotovitel tímto potvrzuje, že se s bezpečnostními pravidly seznámil a souhlasí s nimi.

- 4.2 Objednatel prostřednictvím manažera kybernetické bezpečnosti do 10ti dnů od účinnosti této rámcové dohody oznámí zhotoviteli detaily bezpečnostních standardů objednatele, a to prostřednictvím elektronicky podepsaného emailu.
- 4.3 Objednatel může bezpečnostní pravidla po uzavření rámcové dohody měnit, a to v souvislosti se změnami právních předpisů, rozhodnutími nebo varováními Národního úřadu pro kybernetickou a informační bezpečnost, rozhodnutími dalších správních úřadů nebo plněním nápravných opatření vyplývajících ze státního dozoru. Změny bezpečnostních pravidel budou distribuovány *elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány manažerem kybernetické bezpečnosti minimálně uznávaným elektronickým podpisem (v souladu s eIDAS) či datovou schránkou nebo písemnou (listinnou) formou s podpisem manažera kybernetické bezpečnosti, a to prostřednictvím držitele poštovní licence s potvrzením o doručení na adresu manažera kybernetické bezpečnosti zhotovitele*. V případě, že zhotovitel do 10ti pracovních dnů od doručení oznámení o změně nevyjádří s provedenou změnou nesouhlas, platí, že se změnou souhlasí a je povinen dodržovat takto upravená bezpečnostní pravidla.
- 4.4 Zhotovitel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy rámcové dohody prokazatelné seznámení s bezpečnostními pravidly.

5. Řízení změn

- 5.1 Zhotovitel je povinen řídit rizika související s plněním dle rámcové dohody. Na vyžádání manažera kybernetické bezpečnosti objednatele nebo osob provádějících kontrolní činnost dle čl. 8 této přílohy rámcové dohody je povinen způsob řízení těchto rizik doložit.
- 5.2 Zhotovitel bere na vědomí, že objednatel při provádění změn postupuje v souladu s § 11 vyhlášky o kybernetické bezpečnosti.
- 5.3 U významných změn provádí objednatel analýzu rizik v souladu s metodikou CRAMM, nástrojem RAMSES.

- 5.4 Zhotovitel poskytne objednateli nezbytnou součinnost a bude nápomocen při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatelem. Takovou součinnost je zhotovitel povinen zajistit i u svých poddodavatelů.
- 5.5 Zhotovitel, který v rámci svého řešení nezbytného pro poskytování služeb dle rámcové dohody využije technické nebo programové prostředky společností Huawei Technologies Co., Ltd. nebo ZTE Corporation, včetně jejich dceřiných společností, v průběhu zadávacího řízení objednateli předložil analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost.

6. Informační povinnost

- 6.1 Zhotovitel bezodkladně informuje objednatele prostřednictvím manažera kybernetické bezpečnosti, pokud zjistí narušení bezpečnosti chráněných informací v důsledku kybernetické bezpečnostní události a poskytne objednateli dostatečné informace, které umožní odstranit následky takové události, vyšetřit ji a ohlásit ji Národnímu úřadu pro kybernetickou bezpečnost v souladu s požadavky vyhlášky o kybernetické bezpečnosti. Zhotovitel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.
- 6.2 Zhotovitel prostřednictvím manažera kybernetické bezpečnosti průběžně a bezodkladně informuje objednatele o všech jemu známých významných a kritických hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatelem.
- 6.3 Zhotovitel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládání zhotovitele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných zhotovitelem k plnění podle rámcové dohody s objednatelem. Má se za to, že významnou změnou ovládání se rozumí změna ovládající osoby dle § 74 a násl. zákona č. 90/2012, Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.
- 6.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech.

7. Poddodavatelé

- 7.1 Zhotovitel objednatele dle § 105 odst. 4 ve spojení s odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, předem písemně informuje o úmyslu využít poddodavatele, kterého neoznámil v průběhu zadávacího řízení, včetně jeho identifikace a detailů činností, které má poddodavatel provádět a zpřístupňovaných dat. Identifikační údaje poddodavatelů, kteří se po uzavření rámcové dohody zapojí do plnění veřejné zakázky, předmět činností, které má poddodavatel provádět a zpřístupňovaná data, je zhotovitel povinen objednateli sdělit před zahájením plnění ze strany dotyčného poddodavatele.
- 7.2 Pokud zhotovitel sjedná s poddodavatelem provádění činností nebo zpřístupňování dat ve smyslu této přílohy rámcové dohody, je povinen uzavřít s poddodavatelem smlouvu nebo jiný právní akt, jež zakládá stejná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti jako jsou stanovené v této příloze rámcové dohody. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům vyhlášky o kybernetické bezpečnosti.

7.3 Ve vztahu ke každému poddodavateli, zhotovitel:

- a) vynaloží veškeré přiměřené úsilí, aby prověřil, že poddodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována smlouvou;
- b) zajistí, aby při řetězení poddodavatelů byla vzájemná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti upravena písemnou smlouvou obsahující podmínky, které nabízejí alespoň stejnou úroveň ochrany jako ty, které jsou uvedeny ve smlouvě a splňují požadavky příslušných právních předpisů vztahujících se ke smluvnímu plnění;
- c) poskytne na vyžádání objednateli kopie vybraných částí smluv s poddodavateli (nebo obdobné podklady) relevantních pro plnění rámcové dohody;
- d) zajistí v rozsahu jeho činnosti, aby každý poddodavatel plnil povinnosti vyplývající z rámcové dohody, které se vztahují na ochranu v oblasti informační a kybernetické bezpečnosti prováděnou tímto poddodavatelem, jako by byl stranou této rámcové dohody namísto zhotovitele.

7.4 V případě, že součástí uzavírané dohody s poddodavateli či mezi poddodavateli je poskytnutí bezpečnostních pravidel, je zhotovitel povinen o této skutečnosti informovat objednatele předem. Objednatel je oprávněn do pěti pracovních dnů od doručení oznámení o nutnosti poskytnutí bezpečnostních pravidel poddodavatelům namítnout, že poskytnutí bezpečnostních pravidel poddodavatelům není nezbytně nutné nebo že poskytnutí bezpečnostních pravidel konkrétnímu poddodavateli znamená pro objednatele bezpečnostní riziko a následně zhotoviteli poskytnutí těchto bezpečnostních pravidel poddodavatelům nebo konkrétnímu poddodavateli zakázat. V takovém případě musí zhotovitel prokázat nezbytnou potřebu poskytnutí těchto bezpečnostních pravidel konkrétnímu poddodavateli nebo navrhnout využití jiného poddodavatele. Jestliže objednatel tuto potřebu shledá důvodnou nebo nevyhodnotí nového poddodavatele jako bezpečnostní riziko, povolí poskytnutí těchto bezpečnostních informací konkrétnímu poddodavateli.

8. Kontrola

- 8.1 Zhotovitel zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou rámcové dohody a umožní a bude nápomocen při auditech a inspekcích prováděných jakýmkoli auditorem pověřeným objednatel. Takovou součinnost je zhotovitel povinen zajistit i u svých poddodavatelů.
- 8.2 S přiměřeným předstihem před zahájením kontroly informuje objednatel zhotovitele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrnému narušení prostor, zařízení, personálu a činnosti zhotovitele. Zhotovitel není povinen při provádění kontroly umožnit přístup do svých prostor pouze v případě, že:
 - a) osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;
 - b) je kontrola prováděna mimo běžnou pracovní dobu, ledaže kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil zhotoviteli, že se jedná o takový případ.

- 8.3 Zhotovitel bere na vědomí, že objednatel provádí periodické hodnocení dodavatelů v souladu s požadavky normy ČSN ISO/IEC 9001.

Příloha č. 7 – Zajištění ochrany osobních údajů dle nařízení GDPR

Příloha č. 7 - „Zajištění ochrany osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob související se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (dále jen „**nařízení GDPR**“)

1. Definice pojmů

- 1.1 **„osobními údaji“** se pro účely této přílohy rozumí, ve smyslu nařízení GDPR, veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „**subjekt údajů**“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
- 1.2 **„zpracováním“** se pro účely této přílohy rozumí, ve smyslu nařízení GDPR, jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
- 1.3 **„správcem“** se pro účely této přílohy rozumí, ve smyslu nařízení GDPR, fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Správcem ve smyslu této přílohy rámcové dohody je ŘLP ČR, s.p.
- 1.4 **„zpracovatelem“** se pro účely této přílohy rozumí, ve smyslu nařízení GDPR, fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Zpracovatelem ve smyslu této přílohy rámcové dohody je zhotovitel.
- 1.5 **„subzpracovatelem“** se pro účely této přílohy rozumí, ve smyslu nařízení GDPR, fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt (s výjimkou zaměstnance zpracovatele), který zpracovává osobní údaje na základě pověření zpracovatelem pro správce.
- 1.6 **„porušením zabezpečení osobních údajů“** se účely této přílohy rozumí, ve smyslu nařízení GDPR, porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

2. Předmět zpracování

- 2.1 Předmětem zpracování osobních údajů je: činnosti zpracování osobních údajů zaměstnanců a smluvních partnerů správce v rámci řízení privilegovaného přístupu uživatelů k informační infrastruktuře správce.

3. Doba trvání zpracování

- 3.1 Osobní údaje budou zpracovávány po dobu trvání rámcové dohody.

4. Povaha a účel zpracování

- 4.1 Povaha a účel zpracování osobních údajů jsou vymezeny následovně: plnění rámcové dohody č. 282/2022/IS/140.

5. Typ zpracovávaných osobních údajů

- 5.1 Zpracovávané osobní údaje jsou tohoto typu: jméno a příjmení, osobní číslo, email, telefon, pracovní pozice, uživatelský účet (login), uživatelská role.

6. Kategorie subjektu zpracovávaných osobních údajů

- 6.1 Kategorie subjektu zpracovávaných osobních údajů jsou následující: zaměstnanci správce, smluvní partneři správce, zaměstnanci smluvních partnerů správce.

7. Povinnosti zpracovatele

- 7.1 Zpracovatel musí dodržovat všechny aplikovatelné právní předpisy na ochranu údajů, zejména pak nařízení GDPR.
- 7.2 Zpracovatel nesmí zpracovávat osobní údaje poskytnuté správcem jiným způsobem a za jiným účelem než dle dokumentovaných pokynů správce, pokud zpracování nevyžadují platné právní předpisy, které se vztahují na tohoto zpracovatele. V takovém případě zpracovatel informuje správce o tomto právním požadavku ještě před zpracováním těchto osobních údajů.
- 7.3 Zpracovatel neprodleně informuje správce v případě, že podle jeho názoru určitý pokyn porušuje nařízení GDPR nebo jiné předpisy Evropské Unie nebo členského státu týkající se ochrany osobních údajů.
- 7.4 Zpracovatel zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, pokud se na ně již nevztahuje zákonná povinnost mlčenlivosti.
- 7.5 S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různé míře pravděpodobnosti a různě závažným rizikům pro práva a svobody subjektů údajů, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku včetně opatření uvedených v čl. 32 nařízení GDPR.

8. Subzpracovatelé

- 8.1 Zpracovatel správce dle § 105 odst. 4 ve spojení s odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, předem písemně informuje o úmyslu využít subzpracovatele, kterého neoznámil v průběhu zadávacího řízení, včetně jeho identifikace a detailů činností, které má subzpracovatel provádět a popisu zpracovávaných osobních údajů. Identifikační údaje subzpracovatelů, kteří se po uzavření rámcové dohody zapojí do plnění veřejné zakázky, předmět činností, které má subzpracovatel provádět a zpracovávané osobní údaje, je zpracovatel povinen správci sdělit před zahájením plnění ze strany dotyčného subzpracovatele.

- 8.2 Pokud zpracovatel sjedná se subzpracovatelem provádění činností nebo zpracování osobních údajů ve smyslu této přílohy rámcové dohody, je povinen uzavřít se subzpracovatelem smlouvu nebo jiný právní akt, jež zakládá stejná práva a povinnosti ve vztahu ke zpracovávaným osobním údajům jako jsou stanovené v této příloze rámcové dohody. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům nařízení GDPR. Pokud subzpracovatel nesplní své povinnosti týkající se ochrany údajů, zpracovatel zůstává plně odpovědný správci za plnění těchto povinností subzpracovatele.
- 8.3 Ve vztahu ke každému subzpracovateli, zpracovatel:
- 8.3.1. vynaloží veškeré přiměřené úsilí, aby prověřil, že subzpracovatel poskytuje úroveň ochrany osobních údajů, jež je vyžadována rámcovou dohodou;
 - 8.3.2. zajistí, aby při řetězení subzpracovatelů byla vzájemná práva a povinnosti ve vztahu k ochraně osobních údajů upravena písemnou smlouvou obsahující podmínky, které nabízejí alespoň stejnou úroveň ochrany osobních údajů jako ty, které jsou uvedeny v této příloze resp. v rámcové dohodě, a splňují požadavky článku 28 nařízení GDPR;
 - 8.3.3. pokud zpracování osobních údajů provádí subzpracovatel, který je usazen mimo EHP a zároveň země jeho usazení nebyla Evropskou komisí označena za zemi poskytující dostatečnou úroveň ochrany, zajistí, aby zpracovatelská smlouva uzavřená s takovým subzpracovatelem obsahovala standardní smluvní klauzule; a
 - 8.3.4. poskytne na vyžádání správci kopie zpracovatelských smluv (nebo obdobné podklady) se subzpracovateli, které mohou být upraveny za účelem odstranění důvěrných obchodních informací, které nejsou relevantní pro požadavky této rámcové dohody.
- 8.4 Zpracovatel zajistí, aby každý subzpracovatel plnil povinnosti vyplývající z této přílohy rámcové dohody, které se vztahují na zpracování osobních údajů prováděné tímto subzpracovatelem, jako by byl stranou této rámcové dohody namísto zpracovatele.
- 8.5 Správce je oprávněn do pěti pracovních dnů od doručení oznámení zpracovatele o nutnosti využít nového subzpracovatele namítnout, že využití nového subzpracovatele není nezbytně nutné nebo že využití nového subzpracovatele znamená pro správce bezpečnostní riziko a následně zpracovateli využití nového subzpracovatele zakázat. V takovém případě musí zpracovatel prokázat nezbytnou potřebu využití nového subzpracovatele nebo navrhnout využití jiného subzpracovatele. Jestliže správce tuto potřebu shledá důvodnou nebo nevyhodnotí nového subzpracovatele jako bezpečnostní riziko, povolí zpracovateli využití tohoto nového subzpracovatele.

9. Výkon práv subjektu údajů

9.1 Zpracovatel

- 9.1.1. neprodleně informuje správce, pokud (nebo jakýkoli subzpracovatel) obdrží od subjektu údajů žádost směřující k výkonu práv subjektu údajů dle GDPR; a
- 9.1.2. zajistí, že on (nebo jakýkoli subzpracovatel) nebude odpovídat na žádosti směřující k výkonu práv subjektu údajů dle GDPR jinak než dle písemných pokynů správce a/nebo do té míry, jak je vyžadováno v souladu s aplikovatelnou právní úpravou. V takovém případě však zpracovatel informuje správce o tomto právním požadavku ještě před tím, než zpracovatel (nebo subzpracovatel) odpoví na tuto žádost.

10. Porušení zabezpečení osobních údajů

- 10.1 Zpracovatel informuje správce bez zbytečného odkladu, pokud zpracovatel nebo jakýkoli subzpracovatel zjistí porušení zabezpečení osobních údajů a poskytne správci dostatečné informace, které umožní splnění všech povinností hlásit nebo informovat subjekty osobních údajů o porušení zabezpečení osobních údajů podle platných právních předpisů o ochraně osobních údajů.
- 10.2 Zpracovatel je povinen spolupracovat se správcem a přijmout finančně přiměřené kroky, které nařídí správce za účelem nápomoci při vyšetřování, zmírňování a nápravě každého takového porušení osobních údajů.

11. Zničení osobních údajů

- 11.1 V případě ukončení rámcové dohody nebo v případě ukončení zpracování osobních údajů dle rámcové dohody (dále jen „datum ukončení“) zpracovatel neprodleně, nejpozději však do 15 dnů vymaže všechny osobní údaje (včetně jejich kopií).
- 11.2 Správce může zpracovateli písemně oznámit do 5 dnů od data ukončení, že požaduje, aby zpracovatel:
- 11.2.1. vrátil veškeré osobní údaje (včetně kopií) správci zabezpečeným přenosem souborů ve strojově běžně čitelném formátu; a
- aby odstranil a zajistil vymazání všech ostatních osobních údajů (včetně kopií) zpracovávaných jakýmkoli subzpracovatelem. Zpracovatel vyhoví této písemné žádosti do 10 dnů od data ukončení.
- 11.3 Každý zpracovatel (a subzpracovatel) může nad rámec stanovený rámcovou dohodou zpracovávat osobní údaje v rozsahu požadovaném příslušnými právními předpisy a pouze v rozsahu a po dobu, která je těmito právními předpisy vyžadována. Zpracovatel dále zajistí, že tyto osobní údaje budou zpracovávány pouze v rozsahu a pro účely uvedené v příslušných právních předpisech, a že s nimi bude nakládáno jako s důvěrnými informacemi.
- 11.4 Zpracovatel poskytne správci písemné potvrzení o splnění povinnosti týkající se vymazání osobních údajů (včetně kopií).

12. Kontrola

- 12.1 Zpracovatel zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou rámcové dohody a umožní a bude nápomocen při auditech a inspekcích, jakýmkoli auditorem pověřeným správcem. Takovou součinnost je zpracovatel povinen zajistit i u svých subzpracovatelů.
- 12.2 Informační práva a práva na kontrolu zpracování osobních údajů správce vznikají pouze tehdy a do té míry, pokud dle rámcové dohody nejsou správci poskytovány tyto informace a nevyplývají mu auditorská práva, která by splňovala požadavky vyplývající z aplikovatelných právních předpisů (včetně případného ustanovení čl. 28 odst. 3 písm. h) nařízení GDPR).
- 12.3 S přiměřeným předstihem před zahájením kontroly zpracování osobních údajů informuje správce zpracovatele o této kontrole. Správce dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrného narušení prostor, zařízení, personálu a činnosti zpracovatele. Zpracovatel není povinen při provádění umožnit přístup do svých prostor pouze v případě, že.

- 12.3.1. osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;
- 12.3.2. je kontrola prováděna mimo běžnou pracovní dobu, leda že kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil zpracovateli, že se jedná o takový případ.