

**SMLOUVA O DÍLO**

**Letiště Praha, a.s.**  
jako Objednatel

a

**ICZ a.s.**  
jako Zhotovitel

ev.číslo Smlouvy Objednatele:  
0227008905

ev.číslo Smlouvy Zhotovitele

## SMLOUVA O DÍLO

Strany:

### **Letiště Praha, a. s**

sídlo: Praha 6, K letišti 1019/6, PSČ 161 00  
IČO: 282 44 532  
DIČ: CZ699003361  
zápis v OR Městský soud v Praze, oddíl B, vložka 14003  
bankovní spojení UniCredit Bank Czech Republic and Slovakia, a.s.  
číslo účtu (CZK): 801812025/2700

(dále jen „**Objednatel**“ nebo „**LP**“)

a

### **ICZ a.s.**

sídlo: Na hřebenech II 1718/10, Nusle, 140 00 Praha 4,  
IČO: 25145444,  
DIČ: CZ699000372,  
Zápis v OR Městský soud v Praze, sp. zn. B 4840  
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s.,  
číslo účtu (CZK): 2109164825/2700,

(dále jen „**Zhotovitel**“)

(Objednatel a Zhotovitel dále společně také „**Strany**“ či jednotlivě „**Strana**“)

u z a v í r a j í

**v souladu s ustanoveními § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, a v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění, tuto smlouvu o dílo (dále jen „Smlouva“).**

### **Preambule**

Objednatel prohlašuje, že systém definovaný v předmětu Smlouvy bude součástí základního informačního systému Letiště Praha (dále jen „Z-IS LP“), který byl určen informačním systémem základní služby v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění“.

Objednatel považuje Zhotovitele systému definovaného v předmětu Smlouvy za významného dodavatele v souladu s vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

## **1. DEFINICE A VÝKLAD POJMŮ**

- 1.1.1 Níže uvedené termíny této Smlouvy mají význam definovaný v tomto odstavci 1.1 s tím, že v textu Smlouvy jsou uvedeny vždy velkým počátečním písmenem:
- 1.1.2 „**Administrátor**“ je správce Systému na straně Objednatele, který je odpovědný za správu a konfiguraci Systému v prostředí Objednatele.

- 1.1.3 „**Analýza**“ znamená technický popis integrace Systému do prostředí Objednatele, síťové schéma, popis jednotlivých integrací z požadovaných systémů z technické dokumentace, rozpracované WorkFlow požadované v technické specifikaci, podrobný časový harmonogram Implementace dodržující termíny definované v zadávací dokumentaci, veškeré požadavky na technickou součinnost ze strany Objednatele, definované potřebné síťové prostupy, požadované přístupy a jejich úroveň do integrovaných systémů. Požadavky na akceptaci Analýzy jsou uvedeny v příloze č. 7 této Smlouvy.
- 1.1.4 „**Autorský zákon**“ znamená zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, nebo právní předpis, který jej zcela nebo z části nahradí.
- 1.1.5 „**Cena Díla**“ má význam uvedený v čl. 8.1 této Smlouvy.
- 1.1.6 „**Customizace**“ znamená proces přizpůsobování Systému specifickým potřebám Objednatele, a to nastavením zákaznických parametrů nebo jiných úprav Systému v souladu s Přílohou č. 1 této Smlouvy.
- 1.1.7 „**Dílo**“ znamená
- 1.1.7.1 vypracování Analýzy;
- 1.1.7.2 dodání Systému;
- 1.1.7.3 provedení Customizace, Instalace a Integrace Systému, v souladu s technickou a funkční specifikací, která tvoří přílohu č. 1 této Smlouvy;
- 1.1.7.4 vypracování Dokumentace;
- 1.1.7.5 provedení školení Uživatelů a Administrátorů.
- 1.1.8 „**Dokumentace**“ znamená (i) manuál uživatele, (ii) manuál administrátora a (iii) ostatní dokumentaci podrobně popisující funkcionalitu, provozní charakteristiky, technické parametry a uživatelské, resp. administrátorské charakteristiky Systému v českém jazyce a v elektronické podobě ve formátu docx, případně pdf.
- 1.1.9 „**Důvěrné informace**“ jsou informace, které Strana získá uzavřením této Smlouvy, nebo v souvislosti s plněním dle této Smlouvy, týkající se druhé Strany nebo jejich zástupců, Ovládaných osob, Osob LP a jejich poměrů, vztahů a podnikatelské nebo jiné činnosti, a to včetně informací obsažených v Systému, zejména informací obchodní povahy a informací týkajících se provozu Letiště Václava Havla Praha.
- 1.1.10 „**Faktura**“ znamená daňový doklad vystavený Zhotovitelem za účelem úhrady Ceny Díla, jehož náležitosti stanoví zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
- 1.1.11 „**Implementace**“ znamená proces Instalace, Customizace a Integrace Systému v souladu s Přílohami č. 1 a č. 4 této Smlouvy.
- 1.1.12 „**Instalace**“ znamená provedení veškerých činností nezbytných ke zprovoznění Systému, zahrnující mimo jiné zavedení Systému a jeho komponent v prostředí Objednatele.
- 1.1.13 „**Integrace**“ znamená věcné a funkční propojení Systému s jiným prvkem a/nebo programovým a/nebo hardwarovým vybavením Objednatele.
- 1.1.14 „**Insolvenční zákon**“ znamená zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů nebo jakýkoli jiný právní předpis, který má za následek úpadek, konkurs nebo bankrot některé ze Stran.
- 1.1.15 „**Lhůta pro odpověď**“ znamená lhůtu závazně stanovenou touto Smlouvou, ve které je Zhotovitel povinen telefonicky na čísle ..... (či jiném čísle pro tyto účely oznámeném ze strany Objednatele Zhotoviteli) a prostřednictvím elektronické pošty na adrese ..... (či na jiné elektronické adrese pro tyto účely oznámené ze strany Objednatele Zhotoviteli) informovat Objednatele o tom, jakým postupem bude odstraněna oznámená Vada a jací pracovníci Zhotovitele budou oznámenou Vadu odstraňovat. Lhůta

pro odpověď začíná běžet od okamžiku Oznámení Vady ze strany Objednatele na kontaktní údaje Zhotovitele uvedené v příloze č. 3 této Smlouvy.

- 1.1.16 „**Lhůta pro odstranění Vady**“ znamená touto Smlouvou závazně stanovenou lhůtu, ve které je Zhotovitel povinen odstranit oznámenou Vadu. Lhůta pro odstranění Vady začíná běžet od okamžiku Oznámení Vady ze strany Objednatele na kontaktní údaje Zhotovitele uvedené v příloze č. 3 této Smlouvy.
- 1.1.17 „**Licence**“ znamená oprávnění k výkonu práva užití Dílo ve smyslu ustanovení § 2358 a násl. Občanského zákoníku, v platném znění, a to v rozsahu specifikovaném v článku 6. této Smlouvy.
- 1.1.18 „**Místo dodání**“ znamená místa dle čl. 3.2 této Smlouvy, kam je Zhotovitel povinen Dílo dodat k zahájení provozu.
- 1.1.19 „**Nařízení**“ znamená 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).
- 1.1.20 „**Občanský zákoník**“ znamená zákon č. 89/2012 Sb., občanský zákoník, v platném a účinném znění, nebo právní předpis, který jej zcela nebo z části nahradí.
- 1.1.21 „**Osobní údaje**“ znamená osobní údaje fyzických osob, zejména zaměstnanců Objednatele, jejichž ochrana a zpracování podléhá zákonu č. 110/2019 Sb., o zpracování osobních údajů (dále jen „**ZZOÚ**“) či Nařízením;
- 1.1.22 „**Osoby LP**“ znamená obchodní korporace, které spolu s Objednatelem tvoří koncern ve smyslu ustanovení § 79 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech, v platném znění („**Zákon o obchodních korporacích**“);
- 1.1.23 „**Ovládaná osoba**“ znamená právnickou osobu ovládanou Objednatelem nebo Zhotovitelem ve smyslu Zákona o obchodních korporacích;
- 1.1.24 „**Oznámení**“ znamená telefonické oznámení ze strany Objednatele do Podpůrného centra Zhotovitele o existenci Vady. Každé telefonické oznámení potvrdí Objednatel rovněž zasláním e-mailové notifikace Zhotoviteli na e-mail ticket@i.cz, a to do konce následujícího Pracovního dne.
- 1.1.25 „**Perioda průběžných informací**“ znamená četnost průběžných informací o odstraňování Vad, jež je Zhotovitel povinen poskytovat Objednateli.
- 1.1.26 „**Penetrační testy**“ znamená ověření vlastností Software z hlediska kybernetické bezpečnosti třetí osobou, v rámci kterých budou provedeny pokusy o prolomení zabezpečení Software a v něm uložených dat.
- 1.1.27 „**Podpůrné centrum**“ znamená Centrum servisní podpory Zhotovitele na tel: +420 222 ...  
..., e-mail: .....
- 1.1.28 „**Pracovní den**“ znamená kterýkoliv kalendářní den s výjimkou soboty, neděle, pracovního volna a dne pracovního klidu ve smyslu platných právních předpisů České republiky.
- 1.1.29 „**Práva duševního vlastnictví**“ znamená veškeré patenty, autorská práva, práva k průmyslovým vzorům, ochranným známkám, obchodním jménům a firmám, chráněným označením původu, práva související s právem autorským, zvláštní práva pořizovatele databáze, obchodní tajemství, know-how a všechna další práva duševního vlastnictví jakékoliv povahy (ať již zapsaná nebo nezapsaná), včetně jakýchkoliv přihlášek a výlučných práv přihlásit k ochraně cokoli z výše uvedeného kdekoli na světě.
- 1.1.30 „**Předání**“ znamená den, kdy bude mezi Stranami podepsán Předávací protokol.
- 1.1.31 „**Předávací protokol**“ znamená protokol o předání a převzetí Díla, popř. jeho fáze určené k samostatnému předání, anebo protokol o předání a převzetí doobjednaných uživatelských licencí podepsaný oběma Stranami.

- 1.1.32 „**Servisní doba**“ znamená dobu 24 hodin, 7 dní v týdnu.
- 1.1.33 „**Servisní požadavek**“ je záznam o nahlášení chybového stavu, a/nebo žádost o změnu požadovanou Uživatelem.
- 1.1.34 „**Servisní smlouva**“ znamená smlouvu, jejímž předmětem bude závazek Zhotovitele poskytovat Objednateli servisní služby týkající se Díla spočívající v zajištění funkčnosti, dostupnosti, odezvy a poskytování podpory pro Dílo a závazek Objednatele zaplatit Zhotoviteli za tyto servisní služby měsíční odměnu.
- 1.1.35 „**Služby**“ znamená všechny činnosti, které má Dodavatel poskytnout v průběhu Plnění Smlouvy a jsou potřebné, ke splnění smluvních závazků.
- 1.1.36 „**Systém**“ znamená systém „PAM“, určený pro řízení a správu privilegovaných účtů a přístupů, tzv. „Privileged Access Management“ (dále jen „PAM“), který zajistí jednotnou centrální správu privilegovaných účtů, řízení přístupů k aktivům technologické (hardware/software) infrastruktury informačního systému Letiště Praha a.s. (IS LP) a monitorování operací prováděných privilegovanými osobami (osobami s účty s vyšším oprávněním než user/domain user). Technické a funkční požadavky systému jsou uvedeny v příloze č. 1 této Smlouvy. Rozsah Systému je uveden v příloze 2 této Smlouvy.
- 1.1.37 „**Systém Objednatele**“ znamená aplikace nebo systémy, které obsahují data Objednatele.
- 1.1.38 „**Technická předloha**“ znamená technickou a funkční specifikaci Systému, jak je popsána v příloze č. 1 této Smlouvy,
- 1.1.39 „**Testovací provoz**“ znamená dobu určenou dle harmonogramu v příloze č.4, během které se provede (i) prověření vlastností Systému podle testovacího scénáře připraveného Zhotovitelem a (ii) vyzkoušení funkčnosti Systému. Doba Testovacího provozu může být po písemné dohodě Stran prodloužena až o patnáct (15) Pracovních dnů. Přítomnost zástupců Zhotovitele při Testovacím provozu bude zajištěna minimálně v rozsahu nutném pro úspěšně dokončení Testovacího provozu, nebude-li mezi Stranami písemně dohodnuto jinak. Součástí Testovacího provozu jsou rovněž Penetrační testy dle čl. 1.1.26, resp. 5.1.4 této Smlouvy.
- 1.1.40 „**Uživatel**“ je každá osoba, která využívá a/nebo je oprávněná využívat služby poskytované Objednatelem.
- 1.1.41 „**Vada**“ znamená (i) právní vady Díla nebo (ii) rozpor mezi skutečnými vlastnostmi Díla a vlastnostmi, které jsou stanoveny touto Smlouvou nebo Dokumentací, nebo (iii) jakékoli funkční odchýlení Díla od standardních funkčních vlastností popsaných v této Smlouvě, především v Příloze č. 1 Technická specifikace, nebo Dokumentaci, které negativně postihuje jeho činnost nebo funkčnost.
- 1.1.42 „**Vada kategorie A**“ znamená nejzávažnější Vadu, která se projevuje tím, že
- 1.1.42.1 dodané Dílo má právní vady, nebo
- 1.1.42.2 dodané Dílo nebo jakákoliv jeho část nemá vlastnosti výslovně vymíněné touto Smlouvou nebo uvedené v Dokumentaci, nebo
- 1.1.42.3 dodané Dílo nebo jakákoliv jeho část je zcela nefunkční nebo Objednatel nemůže Dílo nebo jakoukoliv jeho podstatnou část užívat.
- 1.1.43 „**Vada kategorie B**“ znamená Vadu, která se projevuje tím, že užívání nebo funkčnost Díla nebo jakékoliv jeho části je Vadou omezeno a dochází tak k významnému narušení procesů a nárůstu pracnosti u Objednatele a/nebo v důsledku této Vady dojde ke ztrátě dat a/nebo provedené práce uživatele.
- 1.1.44 „**Vada kategorie C**“ znamená Vadu, kterou Objednatel nezařadil mezi Vadu kategorie A nebo Vadu kategorie B a která
- 1.1.44.1 nebrání nebo má zcela minimální vliv na řádné užívání nebo funkčnost Díla nebo jakékoliv jeho části ze strany Objednatele, a

- 1.1.44.2 má minimální vliv na narušení procesů a nárůst pracnosti u Objednatele.
- 1.1.45 „**Zákon o zpracování osobních údajů**“ nebo ve zkratce „“ znamená zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.

- 1.2** Další pojmy mohou být definovány přímo v textu Smlouvy s tím, že definice pojmu je zvýrazněna tučně a uvozena slovy „dále jen“ a při každém dalším výskytu je v textu Smlouvy vyznačena velkým počátečním písmenem.
- 1.3** Slova vyjadřující pouze jednotné číslo zahrnují i množné číslo a naopak, slova vyjadřující mužský rod zahrnují i ženský a střední rod a naopak, a výrazy vyjadřující osoby zahrnují fyzické i právnické osoby a naopak.

## **2. PŘEDMĚT SMLOUVY**

- 2.1** Za podmínek sjednaných v této Smlouvě
- 2.1.1 se Zhotovitel zavazuje, bude-li k tomu Objednatelem vyzván, vytvořit pro Objednatele Analýzu a dále, bude-li k tomu následně vyzván, též ostatní části Díla a předat Objednateli Analýzu, popř. Dílo v souladu s touto Smlouvou a přílohami této Smlouvy, které jsou její nedílnou součástí a poskytnout Objednateli plnění podle této Smlouvy,
- 2.1.2 se Objednatel zavazuje za řádně provedenou Analýzu, popř. Dílo zaplatit Zhotoviteli dohodnutou Cenu a řádně v souladu s touto Smlouvou a jejími přílohami provedenou Analýzu, popř. Dílo od Zhotovitele převzít.

## **3. DOBA A MÍSTO DODÁNÍ**

- 3.1** Zhotovitel se zavazuje dodat Analýzu do 60 Pracovních dnů ode dne kdy k tomu byl Objednatelem vyzván po podpisu Smlouvy oběma Stranami a dále, bude-li k tomu Objednatelem vyzván, úspěšně dokončit Testovací provoz základní fáze Díla definované v příloze č. 2 této Smlouvy nejpozději do doby určené harmonogramem z přílohy č.4 Smlouvy o dílo, kdy byl Objednatelem vyzván k zahájení Implementace, to vše v souladu s podrobným harmonogramem Implementace, který tvoří přílohu č. 4 této Smlouvy (dále jen „**Harmonogram**“). Testovací provoz fáze 2 Díla definované v příloze č. 2 této Smlouvy se Zhotovitel zavazuje úspěšně dokončit do doby, která bude uvedena v objednávce zaslané Objednatelem Zhotoviteli k realizaci této fáze. Takováto objednávka může být zaslána Objednatelem Zhotoviteli nejpozději do 4 let od podpisu Smlouvy. V této objednávce bude upřesněn počet množstevních jednotek uživatelských licencí (dle přílohy č. 2 této Smlouvy). Strany výslovně sjednávají, že Smlouva nezakládá závazek Objednatele realizovat fázi 2 Díla. Bude-li Objednatel fázi 2 realizovat, je pak oprávněn postupně doobjednávat uživatelské licence, a to od okamžiku předání a převzetí fáze 2 Díla až do doby 4 let od předání a převzetí základní fáze Díla, přičemž zhotovitel se zavazuje tyto licence Objednateli předat do termínu uvedeného v příslušné objednávce.
- 3.2** Místem dodání Díla jsou: prostory v lokalitách na adresách (i) K Letišti 1019/6, Praha 6 tzv. Bílý dům a (ii) Jana Kašpara 1069/1, Praha 6, budova APC nebo jiná místa v areálu mezinárodního letiště Praha/Ruzyně určené Objednatelem. Zhotovitel je oprávněn vykonávat práce na Díle i mimo Místo dodání Díla výhradně na základě předchozího písemného souhlasu Objednatele.

## **4. PRÁVA A POVINNOSTI STRAN**

- 4.1** Objednatel je oprávněn vytisknout, užívat a doplňovat Dokumentaci týkající se Systému v neomezeném počtu kopií pro svoji potřebu a ve svůj prospěch jakož i pro potřebu a ve prospěch Osob LP a dalších třetích osob a tuto Dokumentaci předat Osobám LP a dalším třetím osobám k užívání. Zhotovitel tímto výslovně souhlasí s užíváním této Dokumentace Objednatelem a Osobami LP.
- 4.2** Zhotovitel se zavazuje:

- 4.2.1 provést Dílo v souladu s touto Smlouvou a jejími přílohami, pokyny pověřených zaměstnanců Objednatele na svůj náklad a na své nebezpečí a odstranit jakékoli Vady vytčené při předání nebo v záruční době podle článku 7.4 této Smlouvy;
- 4.2.2 provést Dílo (nebo jeho část) podle této Smlouvy osobně, přičemž na plnění a Implementaci všech fází Díla musí participovat specialista na implementaci PAM, prostřednictvím, kterého Zhotovitel prokazoval svoji technickou kvalifikaci v zadávacím řízení, které předcházelo uzavření této Smlouvy. V případě nepřítomnosti tohoto specialisty musí být tento specialista nahrazen specialistou s obdobnou kvalifikací, a to po předchozím písemném souhlasu Objednatele. Objednatel bezdůvodně neodmítne osobu, která bude disponovat obdobnou kvalifikací jako specialista, kterým byla prokázána technická kvalifikace v zadávacím řízení, avšak bez jeho souhlasu není Zhotovitel oprávněn pokračovat v plnění Díla. Zhotovitel není oprávněn provést Dílo (nebo jeho část) prostřednictvím subdodavatele, aniž by k tomu dal Objednatel předchozí písemný souhlas. V případě, že by Objednatel předchozí písemný souhlas s provedením Díla (nebo jeho části) podle této Smlouvy prostřednictvím subdodavatele Zhotoviteli udělil, Zhotovitel bude Objednateli za provedení Díla (či jeho části) podle této Smlouvy subdodavatelem odpovídat Objednateli ve stejném rozsahu, jako by Dílo zhotovil Zhotovitel sám. Ustanovení subdodavatele nemá vliv na odpovědnost Zhotovitele zhotovit Dílo v souladu s touto Smlouvou, kterou má po celou dobu trvání této Smlouvy Zhotovitel vůči Objednateli;
- 4.2.3 dodržovat veškeré obecně závazné právní předpisy a předpisy Objednatele v oblasti s nakládáním s odpady a odpady vzniklé při provádění Díla likvidovat v souladu s platnou právní úpravou na své náklady;
- 4.2.4 okamžitě e-mailem divizi bezpečnosti (BZP) Letiště Praha, a. s. ohlásit každou ztrátu, odcizení, poškození ID karty (včetně návštěvnických) nebo jiného oprávnění vydaného jemu nebo jeho zaměstnancům. Stejně tak je Zhotovitel povinen vrátit jemu a jeho zaměstnancům vydaná povolení či další karty při ukončení jejich platnosti;
- 4.2.5 zajistit, aby jeho zaměstnanci nebo zaměstnanci jeho subdodavatele podle článku 4.2.2 této Smlouvy dodržovali zákaz požívání alkoholických nápojů či zneužívání jiných návykových látek. V případě porušení tohoto zákazu je Objednatel oprávněn takovému zaměstnanci Zhotovitele zakázat přístup do Místa dodání. Vznikne-li takovýmto způsobem prodlení v plnění předmětu Smlouvy, odpovídá za takovéto prodlení Zhotovitel. Strany se dohodly, že obdobně se bude též postupovat v případě, kdy se zaměstnanec Zhotovitele nebo jeho subdodavatele podle článku 4.2.2 této Smlouvy dopustí krádeže v Místě dodání, dojde k porušení povinností podle článku 11 a/nebo 12 této Smlouvy nebo v případech násilného chování vůči zaměstnancům Objednatele nebo jiným osobám v Místě dodání;
- 4.2.6 zajistit, aby jeho zaměstnanci podléající se na plnění této Smlouvy při pobytu v Místě dodání dodržovali vnitřní předpisy, pokyny a směrnice, předpisy upravující pohyb osob, vozidel, materiálu, požární bezpečnost, ochranu zdraví při práci a další předpisy, se kterými budou Objednatelem seznámeni;
- 4.2.7 zaškolení zaměstnance Objednatele případně zaměstnance Osob LP v oblastech užití, správy a administrace Systému, a to v rozsahu dle Přílohy č. 1 této Smlouvy. Kromě zaškolení, které proběhne v před podpisem Předávacího protokolu k dané fázi Díla je Zhotovitel povinen po dohodě s Objednatelem a dle jeho požadavků v souladu s Přílohou č. 1 této Smlouvy realizovat též další školení s časovým odstupem. Cena za školení v rozsahu stanoveném touto Smlouvou je zahrnuta v Ceně Díla. Cena za školení zaměstnanců bude na faktuře za Dílo vyčíslena samostatně;
- 4.2.8 předat Objednateli veškeré zdrojové kódy/installační soubory vytvořené v rámci Implementace Díla u Objednatele, tj. vztahující se k software vytvořenému na míru Objednateli. Strany se dohodly, že Objednatel je oprávněn číst a měnit a to i za pomoci třetích osob a dále je, dle své libovůle, poskytnout třetím osobám, které jsou rovněž oprávněny je číst a měnit ve svůj prospěch.

- 4.2.9 nelze-li na Zhotoviteli spravedlivě požadovat, nemusí být Objednateli předány zdrojové kódy k proprietárnímu softwaru a stejně tak nemusí být poskytnuto právo Objednatele do proprietárního softwaru zasahovat, vždy však musí být předána kompletní Dokumentace.
- 4.3** Zhotovitel se zavazuje informovat Objednatele o nezaplacených pohledávkách po lhůtě splatnosti vzniklých na základě této Smlouvy nejpozději tři (3) Pracovní dny po splatnosti tak, aby je mohl Objednatel bez jakéhokoli odkladu uhradit.
- 4.4** Objednatel se zavazuje poskytnout Zhotoviteli součinnost spočívající v zajištění:
- 4.4.1 přístupu do Místa plnění,
- 4.4.2 poskytnutí Zhotoviteli veškerých informací, materiálů a potřebné součinnosti v rozsahu a čase nezbytném pro realizaci předmětu Smlouvy,
- 4.4.3 zajištění provozu veškeré technické (SW i HW) infrastruktury okolních systému souvisejících s předmětem této Smlouvy.
- 4.5** Zhotovitel ve vztahu k případným subdodavatelům neuplatní horší platební podmínky, než jak jsou nastaveny mezi Objednatelem a Zhotovitelem v čl. 8 této Smlouvy, přičemž Zhotovitel je povinen plnění této povinnosti Objednateli prokázat do 3 pracovních dnů na písemnou výzvu, kterou může zaslat Objednatel Zhotoviteli kdykoliv v průběhu plnění této Smlouvy, a to i opakovaně.
- 4.6** Zhotovitel se zavazuje umožnit, aby na vývoji systému, který zajistí jednotnou centrální správu privilegovaných účtů participovali alespoň dva studenti VŠ a/nebo absolventi VŠ (do jednoho roku po ukončení studia) technických a/nebo IT oborů a doložit Objednateli doklady (např. čestné prohlášení) o jejich participaci včetně jmenného seznamu těchto studentů a/nebo absolventů a jejich stručného vlastnoručně podepsaného vyjádření, co jim tato participace přinesla pro jejich budoucí profesní život.
- 4.7** Zhotovitel se zavazuje v souladu s čl. 5k Nařízení Rady (EU) 2022/576 ze dne 8. dubna 2022, kterým se mění nařízení (EU) č. 833/2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině (dále jen „Nařízení Rady“) po celou dobu trvání Smlouvy nebyť:
- a) ruským státním příslušníkem, fyzickou či právnickou osobou nebo subjektem či orgánem se sídlem v Rusku,
  - b) právnickou osobou, subjektem nebo orgánem, které jsou z více než 50 % přímo či nepřímo vlastněny některým ze subjektů uvedených v písm. a) tohoto odstavce, nebo
  - c) fyzickou nebo právnickou osobou, subjektem nebo orgánem, které jednájí jménem nebo na pokyn některého ze subjektů uvedených v písm. a) nebo písm. b) tohoto odstavce,
- a zajistit, aby se na realizaci předmětu plnění ze všech smluv uzavřených mezi Objednatelem a Zhotovitelem v rámci veřejné zakázky nepodílel v rozsahu více než 10 % souhrnné hodnoty předmětu plnění ze všech smluv dle této věty poddodavatel splňující znaky dle některého z písm. a) – c) výše. Pro účely tohoto odstavce Smlouvy se za souhrnnou hodnotu plnění považuje celková nabídková cena v Kč bez DPH, kterou Zhotovitel uvedl ve své nabídce pro veřejnou zakázku.
- 4.8** V případě, že souhrnná hodnota plnění ze všech smluv dle předchozího odstavce realizovaná prostřednictvím konkrétního poddodavatele dosáhne 10 % souhrnné hodnoty plnění dle předchozího odstavce, do 10 kalendářních dnů tuto skutečnost Objednateli písemně oznámit spolu s uvedením identifikačních údajů tohoto poddodavatele. Pokud Objednatel shledá, že tento poddodavatel splňuje znaky dle některého z písm. a) – c) odst. 4.7 Smlouvy, sdělí tuto skutečnost bez zbytečného odkladu písemně Zhotoviteli. Zhotovitel následně není oprávněn realizovat jakékoli další plnění prostřednictvím tohoto poddodavatele.
- 4.9** V případě jakékoli změny skutečností dle odst. 4.7 Smlouvy se Zhotovitel zavazuje takovou změnu do 10 kalendářních dnů Objednateli písemně oznámit.



## 5. PŘEDÁNÍ A PŘEVZETÍ DÍLA

- 5.1** Předání a převzetí základní fáze Díla proběhne na základě akceptační procedury, která se skládá ze sedmi (7) fází:
- 5.1.1 Dodávka Analýzy,
  - 5.1.2 Dodávka HW a jeho Instalace,
  - 5.1.3 Implementace,
  - 5.1.4 Testovací provoz, Penetrační testy,
  - 5.1.5 Dodávka Dokumentace,
  - 5.1.6 Školení,
  - 5.1.7 Podepsání Předávacího protokolu.
- 5.2** Lhůta pro dodání Analýzy Zhotovitelem činí v souladu s Harmonogramem 60 Pracovních dnů ode dne, kdy k tomu byl Zhotovitel Objednatelem vyzván po podpisu Smlouvy oběma Stranami.
- 5.3** Lhůta pro posouzení Analýzy a vyjádření ze strany Objednatele je stanovena Harmonogramem na 15 Pracovních dnů, není-li mezi Stranami dohodnuto jinak.
- 5.4** V případě, že Analýza nebude splňovat akceptační kritéria uvedená v příloze č. 7 Smlouvy, anebo, dle posouzení Objednatele, nebude směřovat k dosažení záměru, pro který je tato Smlouva uzavřena a který je z ní zřejmý a Zhotoviteli je znám, zavazuje se Zhotovitel zjednat nápravu do pěti (5) Pracovních dnů od vyjádření Objednatele, během kterých doplní či upraví požadované informace do Analýzy v souladu s vyjádřením Objednatele. Zhotovitel poté vyzve Objednatele k opakovanému posouzení Analýzy a Objednatel opětovně posoudí Analýzu do pěti (5) Pracovních dnů od doby výzvy. Tento proces posouzení a následného dopřesňování Analýzy se bude opakovat, dokud Zhotovitel nesplní veškerá akceptační kritéria uvedená v příloze č. 7, popř. dokud z Analýzy nebude zřejmé, že směřuje k dosažení záměru, pro který je tato Smlouva uzavřena, a to maximálně dvakrát (2x) nejpozději však do třiceti (30) Pracovních dnů od prvního termínu odevzdání Analýzy, není-li mezi Stranami dohodnuto jinak.
- 5.5** V případě, že Analýza bude splňovat akceptační kritéria uvedená v příloze č. 7 Smlouvy, Objednatel Analýzu schválí a převezme od Zhotovitele, což bude stvrzeno podpisem protokolu o předání a převzetí Analýzy.
- 5.6** V případě že Analýza nebude schválena ve lhůtě dle čl. 5.4 této Smlouvy, Zhotovitel nemá nárok na její úhradu, není oprávněn zahájit Implementaci a tato Smlouva končí a ustanovení vztahující se k dalším částem Díla se neaplikují.
- 5.7** V případě, že Analýza bude schválena ve lhůtě dle čl. 5.4 této Smlouvy, Zhotovitel má právo na její úhradu na základě faktury vystavené dle čl. 8 této Smlouvy. Zhotovitel však není oprávněn zahájit Implementaci a plnění dalších částí Díla, pokud mu nebude Objednatelem doručena výzva k zahájení Implementace. V případě, že výzva k zahájení implementace nebude zaslána Objednatelem zhotoviteli do doby 10 Pracovních dní od jejího schválení, tato Smlouva končí a ustanovení vztahující se k dalším částem Díla se neaplikují.
- 5.8** Zhotovitel nezahájí Implementaci bez schválení Analýzy Objednatelem. V případě, že Analýza nebude Objednatelem schválena ani v její druhé opakované úpravě ze strany Zhotovitele, tato Smlouva končí a ustanovení vztahující se k dalším částem Díla se neaplikují.
- 5.9** Lhůta pro zahájení Testovacího provozu činí deset (10) Pracovních dnů od vyzvání Objednatele Zhotovitelem, není-li mezi Stranami dohodnuto jinak. Lhůty stanovené v ustanovení čl. 1.1.39 Smlouvy tímto nejsou dotčeny.
- 5.10** O provedeném Testovacím provozu sepíše Strany zápis.
- 5.11** Bude-li během Testovacího provozu zjištěno, že počet Vad nepřevyšuje následující hodnoty:
- (a) Vady kategorie A ..... 0

(b)	Vady kategorie B .....	0
(c)	Vady kategorie C .....	15

Zhotovitel písemně vyzve Objednatele k převzetí Díla.

- 5.12** V případě, že ze zápisu o provedeném Testovacím provozu vyplývá, že Dílo nesplňuje kritéria uvedená v čl. 5.11 této Smlouvy, zavazuje se Zhotovitel odstranit zjištěné Vady a po jejich odstranění vyzvat Objednatele k zahájení Testovacího provozu s tím, že čl. 5.9 až 5.11 této Smlouvy se použijí obdobně. Tento proces testování a následného odstraňování Vad se bude opakovat, dokud Zhotovitel nesplní akceptační kritéria uvedená v čl. 5.11 této Smlouvy, a to maximálně dvakrát (2x) nejpozději však do lhůty stanovené v čl. 3.1 této Smlouvy.
- 5.13** Poté, co bude úspěšně ukončen Testovací provoz, Penetrační testy a splněna akceptační kritéria podle článku 5.11 této Smlouvy, Objednatel zkontroluje a potvrdí úplnost Dokumentace a bude Zhotovitelem realizováno školení dle odst. 4.2.7 Smlouvy, zavazují se Strany bezodkladně podepsat Předávací protokol. Předávací protokol bude obsahovat soupis zbývajících Vad s lhůtou pro jejich odstranění s tím, že nebude-li tato lhůta dohodnuta, má se za to, že činí dvacet (20) Pracovních dnů ode dne podpisu Předávacího protokolu.
- 5.14** První Penetrační testy jsou prováděny na účet a náklady Objednatele, opakované Penetrační testy na účet Zhotovitele.
- 5.15** Strany se dohodly, že současně s touto smlouvou o Dílo uzavřou Servisní smlouvu.
- 5.16** Předání a převzetí fáze 2 Díla proběhne na základě akceptační procedury, která bude specifikována v objednávce Objednatele.

## 6. LICENCE

- 6.1** V souladu s Autorským zákonem v platném znění a s Občanským zákoníkem v platném znění, se Strany dohodly, že k těm částem Díla, k počítačovým programům, které Zhotovitel vytvoří při realizaci Díla pro Objednatele, a k veškerému dalšímu plnění Zhotovitele podle této Smlouvy, které Zhotovitel vytvoří při realizaci Díla pro Objednatele a které bude podléhat ochraně podle Autorského zákona, poskytuje Zhotovitel Objednateli Licenci, teritoriálně neomezenou, v množstevním rozsahu nezbytném pro provozování Díla dle přílohy č. 1 této Smlouvy, pro úpravy Díla a zásahy do Díla, bez omezení způsobu užití, na dobu trvání majetkových autorských práv k Dílu. K těm částem Díla, která jsou vytvořena třetí stranou odlišnou od Zhotovitele se Zhotovitel zavazuje zajistit Objednateli licenci k užívání po dobu trvání Servisní smlouvy (dále jen „**Licence k Dílu**“).
- 6.2** Zhotovitel uděluje Objednateli Licenci k Dílu jako nevýhradní, a to s výjimkou těch částí Díla, které jsou vytvořeny na míru Objednateli, a ke kterým Zhotovitel uděluje Objednateli Licenci výhradní. Zhotovitel se dále zavazuje zajistit, že k veškerému software třetích osob, který je součástí Díla, bude získána licence ve prospěch Objednatele. Strany se dohodly, že Objednatel není povinen Licenci k Dílu využít. Strany se dohodly, že Objednatel je 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 jiným zpracované 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 6 Smlouvy.
- 6.3** Objednatel je rovněž, za podmínek uvedených v následující větě, oprávněn po dobu trvání Licence k Dílu Dílo upravovat, a to jak sám tak prostřednictvím jakékoli třetí osoby (zejména svého subdodavatele) a Zhotovitel uděluje podpisem této Smlouvy Objednateli souhlas se zpřístupněním Díla jakékoli třetí osobě za účelem provedení úprav a zásahů do Díla dle tohoto článku a rovněž je oprávněn poskytnout licenci (udělit podlicenci) třetím osobám, a to všemi nebo určitými způsoby užití i místně a časově neomezeně podle libovolné úvahy Objednatele.
- 6.4** Zhotovitel souhlasí, aby Objednatel Dílo užil v rozsahu uvedeném v článku 6.1 této Smlouvy ve svůj prospěch a pro svoji potřebu, jakož i ve prospěch a pro potřebu Osob LP a dalších třetích osob. Objednatel je oprávněn oprávnění tvořící součást Licence k Dílu zcela nebo zčásti poskytnout Osobám LP a dalším třetím osobám (podlicence).

- 6.5** Pokud je součástí Díla software vytvořený třetí stranou odlišnou od Zhotovitele, jehož užití je podřízeno vlastním licenčním podmínkám, a ke kterému Zhotovitel není oprávněn poskytnout Objednateli licenci ani podlicenci, a ke kterému lze licenci nabýt jedním ze způsobů v licenčních podmínkách k tomuto software uvedených, potom se na takový software výše uvedená ustanovení tohoto článku týkající se úprav Díla, zásahů do Díla, změn Díla a jeho spojování do díla souborného nevztahují. Zhotovitel převádí na Objednatele právo takový software užívat ode dne předání Díla a Objednatel ho k tomuto dni do užívání přijímá, přičemž Zhotovitel se zavazuje zajistit, aby Objednatel disponoval licenci k užívání takového software vytvořeného třetí stranou odlišnou od Zhotovitele po dobu trvání Servisní smlouvy.
- 6.6** Odměna za poskytnutí Licence k Dílu podle tohoto článku 6 včetně odměny za licenci k software vytvořenému třetí stranou odlišnou od Zhotovitele je zahrnuta v Ceně Díla podle článku 8 této Smlouvy.

## **7. ZÁRUKY**

- 7.1** Zhotovitel tímto poskytuje Objednateli záruku, že Systém bude fungovat v souladu s touto Smlouvou a Dokumentací vztahující se k Systému, a že bude řádně bezpečně a spolehlivě zpracovávat data a zajišťovat funkce vyplývající z technických požadavků zadání ve všech svých rozhraní a to jak datových, aplikačních, systémových tak uživatelských.
- 7.2** Zhotovitel tímto poskytuje Objednateli záruku za to, že Dílo ve své dodané podobě nebude obsahovat viry, které by na základě předem definované skutečnosti nebo jiným způsobem zabránily Objednateli užívat Dílo nebo jeho fungování omezit anebo jinak negativně ovlivnit, případně jakkoliv negativně ovlivnit nebo poškodit Systémy Objednatele a/nebo Osob LP.
- 7.3** Zhotovitel prohlašuje, že je oprávněn poskytnout Objednateli Licenci k Dílu v rozsahu podle článku 6 této Smlouvy. Zhotovitel tímto poskytuje Objednateli záruku za to, že Dílo ani jiné plnění Zhotovitele dle této Smlouvy ani užívání Díla ze strany Objednatele dle této Smlouvy neporušuje ani nebude mít za následek porušení jakéhokoliv práva duševního vlastnictví třetích osob. V případě, že Zhotovitel poruší svůj závazek vyplývající ze záruky uvedené v tomto odstavci, je Zhotovitel odpovědný za veškeré důsledky z toho plynoucí, zejména je povinen neprodleně na vlastní náklady zajistit Objednateli právo užívat Dílo, jež nebude narušovat práva duševního vlastnictví třetích osob a nahradit Objednateli veškerou škodu, která mu tím byla způsobena, a to včetně nemajetkové újmy.
- 7.4** Záruka poskytnutá Zhotovitelem dle čl. 7.1 a 7.2 této Smlouvy platí po dobu čtyřiceti osmi (48) měsíců od podepsání Předávacího protokolu podle článku 5.13 této Smlouvy. Ukáže-li se v průběhu lhůty uvedené v předchozí větě některé z ujištění dle čl. 7.1 nebo 7.2 této Smlouvy jako nepravdivé, má Dílo Vady, které se Zhotovitel zavazuje odstranit na svoje náklady. Zahájit odstraňování těchto Vad se Zhotovitel zavazuje, nedohodnou-li se Strany na lhůtě delší, do níže uvedených lhůt od oznámení Vady na kontaktní údaje Zhotovitele uvedené v příloze č. 3 této Smlouvy. Lhůty uvedené v tabulce v tomto článku 7.4 běží v Servisní době.

položka (kategorie Vady)	Lhůta pro odpověď/zahájení odstraňování Vady	Lhůta pro odstranění Vady	Periodicita informovanosti (Perioda průběžných informací)
kategorie Vady A	do 1 hodiny	do 12 hodin	Každou 1 hodinu do odstranění Vady
kategorie Vady B	do 1 hodiny	do 72 hodin	Každých 12 hodin do odstranění Vady
kategorie Vady C	Do následujícího Pracovního dne	do 14 dní, pokud se strany nedohodnou písemně jinak	Každých 7. den do odstranění Vady

## 8. CENA A PLATEBNÍ PODMÍNKY

- 8.1** Cena Analýzy podle této Smlouvy činí **684 000,- Kč** (slovy: **šest set osmdesát čtyři tisíc korun českých**) bez DPH (dále jen „Cena Analýzy“). Cena základní fáze Díla ponížená o cenu Analýzy podle této Smlouvy činí **5 051 330,- Kč** (slovy: **pět milionů padesát jedna tisíc tři sta třicet korun českých**) bez DPH. Cena fáze 2 Díla podle této Smlouvy **9 642 170,- Kč** (slovy: **devět milionů šest set čtyřicet dva tisíc jedno sto sedmdesát korun českých**) bez DPH (dále společně jen „Cena Díla“). Cena zahrnuje veškeré náklady Zhotovitele na realizaci Díla a poskytnutí plnění Zhotovitele podle této Smlouvy a její podrobný rozpis je uveden v příloze č. 2 této Smlouvy. Cena Analýzy a Cena Díla zahrnuje odměnu za poskytnutí Licence k příslušné části Díla podle článku 6 této Smlouvy.
- 8.2** Zhotovitel je oprávněn fakturovat Cenu Analýzy na základě protokolu o předání a převzetí Analýzy dle čl. 5.5 této Smlouvy a Cenu příslušné fáze Díla po podpisu Předávacího protokolu k příslušné fázi Díla dle čl. 5.13 této Smlouvy oběma Stranami, přičemž u fáze 2 Díla bude v ceně zohledněn počet licencí objednaných Objednatelům v rámci této fáze, a to dle jednotkových cen uvedených v příloze č. 2 této Smlouvy. Zhotovitel je dále v rámci fáze 2 oprávněn fakturovat Objednatelům doobjednané licence po podpisu Předávacího protokolu ve vztahu k takto doobjednaným licencím, přičemž jednotkové ceny uvedené v příloze č. 2 této Smlouvy u nich budou poměrně kráceny, a to za každý ukončený rok od podpisu smlouvy. Zhotovitel je oprávněn před dokončením základní fáze Díla fakturovat samostatně Hardware dodaný Objednateli po podpisu samostatného předávacího protokolu k takto dodanému Hardware a instalovanému Hardware dle odst. 5.1.2 této Smlouvy. V případě, že Zhotovitel této možnosti využije, bude cena základní fáze Díla fakturovaná po jejím protokolárním předání dle čl. 5.13 této Smlouvy ponížena nejen o cenu Analýzy dle čl. 5.1.1 Smlouvy, ale i o cenu takto dodaného Hardware dle čl. 5.1.2 Smlouvy. Den podpisu Předávacího protokolu a/nebo samostatného předávacího protokolu je i dnem zdanitelného plnění.
- 8.3** Strany sjednávají, že daňové doklady vystavené na základě této Smlouvy mohou mít listinnou nebo elektronickou podobu ve formátu pdf.
- 8.4** Doba splatnosti Zhotovitelem vystavené Faktury je třicet (30) dnů ode dne jejího doručení Objednateli na adresu uvedenou v čl. 8.8. Nedílnou přílohou Faktury bude oběma Stranami podepsaný Předávací protokol. Případně-li termín splatnosti na sobotu, neděli nebo jiný den pracovního klidu, 31.12. nebo den, který není pracovním dnem podle zákona č. 370/2017 Sb., o platebním styku ve znění pozdějších předpisů, posouvá se termín splatnosti na nejbližší následující pracovní den. K vyrovnání závazku Objednatel dojde odepsáním fakturované částky z účtu Objednatel.
- 8.5** Došlá Faktura musí obsahovat interní číslo objednávky a splňovat všechny náležitosti daňového dokladu ve smyslu platných právních předpisů ČR, zejména zákona č. 235/2004 Sb., o dani

z přidané hodnoty, v platném znění a musí obsahovat ve vztahu k plnění věcně správné údaje a interní referenční číslo, které Zhotoviteli sdělí na vyžádání kontaktní osoba Objednatele uvedená v příloze č. 3 této Smlouvy. Faktura musí být Objednateli doručena do 15. dnů od data uskutečnění zdanitelného plnění na doručovací adresu, uvedenou v bodě 8.8 této Smlouvy. Objednatel má po obdržení faktury patnáct (15) dní na posouzení toho, zda je v pořádku a na její vrácení, pokud obsahuje chyby. Vrácením chybně vystavené Faktury se doba splatnosti přerušuje a po doručení správně vystavené Faktury Objednateli začíná běžet doba splatnosti od počátku.

**8.6** Cena bude hrazena přímo na bankovní účet Zhotovitele vedený u banky v České republice a specifikovaný v této Smlouvě, jehož číslo je správcem daně zveřejněno způsobem umožňujícím dálkový přístup (v souladu s platným zněním zákona č. 235/2004 Sb., o dani z přidané hodnoty), nebude-li na Faktuře uveden bankovní účet jiný a jehož číslo je správcem daně zveřejněno způsobem umožňujícím dálkový přístup (v souladu s platným zněním zákona č. 235/2004 Sb., o dani z přidané hodnoty).

**8.7** Pokud v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, Zhotovitel:

8.7.1 bude rozhodnutím správce daně určen jako nespolehlivý plátc, nebo

8.7.2 bude vyžadovat úhradu za zdanitelné plnění poskytnuté dle této Smlouvy na bankovní účet, který není správcem daně zveřejněn způsobem umožňujícím dálkový přístup, nebo na bankovní účet vedený poskytovatelem platebních služeb mimo území ČR,

je Objednatel oprávněn uhradit na bankovní účet Zhotovitele pouze Cenu Díla za poskytnuté zdanitelné plnění bez daně z přidané hodnoty (dále jen „DPH“). DPH, je-li účtovaná a je-li dle Smlouvy součástí úhrady ze strany Objednatele, je Objednatel oprávněn uhradit přímo na účet příslušného správce daně. V takovém případě se částka ve výši DPH nepovažuje za neuhrazený závazek vůči Zhotoviteli, Zhotovitel tak není oprávněn požadovat doplatek DPH ani uplatňovat jakékoliv smluvní sankce, úroky z prodlení či smluvní pokuty. O tomto postupu je Objednatel povinen Zhotovitele informovat, a to nejpozději k datu úhrady Ceny Díla.

**8.8** Korespondenční adresa pro doručování Faktur je následující:

8.8.1 v listinné podobě na adresu:

Letiště Praha, a. s.

evidence faktur

Jana Kašpara 1069/1

160 08 Praha 6

nebo

8.8.2 elektronicky ve formátu PDF na e-mailovou adresu:

invoices@prg.aero.

**8.9** V případě prodlení Objednatele s úhradou faktury je Zhotovitel oprávněn požadovat po Objednateli smluvní úrok z prodlení ve výši 0,02% z dlužné částky za každý byt započatý den prodlení.

## 9. SEZNAM OSOB

**9.1** V organizačně technických věcech jsou v rozsahu této Smlouvy oprávněni jednat zaměstnanci nebo pověřené osoby uvedené v příloze č. 3 této Smlouvy.

**9.2** Zaměstnanec a pověřené osoby uvedené v příloze č. 3 této Smlouvy mohou Strany změnit po písemném oznámení druhé Straně.

## 10. TRVÁNÍ SMLOUVY

**10.1** Tato Smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou Stran a účinnosti dnem jejího uveřejnění v registru smluv. Tato Smlouva končí svoji platnost a účinnost:

- 10.1.1 písemnou dohodou Stran;
- 10.1.2 uplynutím lhůty 3 měsíců po jejím uzavření v případě, že Zhotovitel nebyl Objednatelem vyzván k dodání Analýzy;
- 10.1.3 marným uplynutím lhůty uvedené v čl. 5.4 této Smlouvy podle čl. 5.6 této Smlouvy;
- 10.1.4 marným uplynutím lhůty uvedené v čl. 5.7 této Smlouvy podle čl. 5.7 této Smlouvy;
- 10.1.5 marným uplynutím lhůty uvedené v čl. 5.8 této Smlouvy podle čl. 5.8 této Smlouvy;
- 10.1.6 odstoupením podle tohoto čl. 10 této Smlouvy;
- 10.1.7 splněním všech závazků z této Smlouvy s výjimkou závazků, které přetrvávají po jejím skončení.

**10.2** Strany se dohodly, že Objednatel je oprávněn od této Smlouvy odstoupit vyjma případů uvedených v platných právních předpisech také v případě, že:

- 10.2.1 Zhotovitel nesplní akceptační kritéria pro skončení Testovacího provozu ani po provedení dvou Testovacích provozů dle čl. 5.13 této Smlouvy, nebo
- 10.2.2 Zhotovitel nesplní svou povinnost uvedenou v článku 3.1 této Smlouvy;
- 10.2.3 Zhotovitel uzavře smlouvu nebo smlouvy se subdodavatelem nebo subdodavatelem na provedení Díla nebo jeho části bez souhlasu Objednatele, nebo
- 10.2.4 Zhotovitel poruší některou z povinností dle čl. 4.2 této Smlouvy a nápravu nezjedná ani ve lhůtě dvacet (20) Pracovních dnů od doručení písemné výzvy Objednatele,
- 10.2.5 se Zhotovitel ocitne v situaci, kdy (i) soud zahájí insolvenční řízení v souladu s platným a účinným zákonem upravující insolvenční řízení, úpadek a způsoby jeho řešení (dále jen „Insolvenční zákon“) nebo (ii) soud rozhodne o úpadku v souladu s Insolvenčním zákonem nebo (iii) soud rozhodne o zrušení konkursu, protože majetek dlužníka zcela nepostačuje pro uspokojení pohledávek věřitelů nebo (iv) Zhotovitel sám na sebe podá insolvenční návrh v souladu s Insolvenčním zákonem nebo (v) je přijato rozhodnutí o povinném nebo dobrovolném zrušení Zhotovitele (vyjma případů sloučení nebo splynutí či jiného případu právního nástupnictví),
- 10.2.6 dojde k významné změně kontroly nad Zhotovitelem nebo změny kontroly nad zásadními aktivy využívanými Zhotovitelem k plnění podle této Smlouvy.

**10.3** Zhotovitel je oprávněn odstoupit od této Smlouvy v případě, že

- 10.3.1 Objednatel je v prodlení se zaplacením Zhotovitelem oprávněně fakturované částky a toto prodlení trvá po dobu delší než třicet (30) dní po písemném upozornění Zhotovitele doručeném Objednateli.

**10.4** Odstoupení je účinné okamžikem, kdy bylo druhé Straně doručeno.

**10.5** Strany sjednávají, že i po ukončení této Smlouvy některým ze způsobů uvedených ve Smlouvě či v platných právních předpisech zůstává zachována platnost a účinnost ustanovení upravující smluvní pokuty, čl. 11. a čl. 12 této Smlouvy.

## 11. DŮVĚRNÉ INFORMACE

**11.1** Strany se dohodly, že veškeré Důvěrné informace, které si sdělily v rámci uzavírání a plnění této Smlouvy, dále informace, tvořící její obsah a informace, které si sdělí nebo jinak vyplynou i z jejího plnění, zůstanou dle jejich vůle utajeny.

- 11.2** Strany se dohodly, že Důvěrné informace nikomu neprozradí a přijmou taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:
- 11.2.1 mají Strany této Smlouvy opačnou povinnost stanovenou zákonem; a/nebo
  - 11.2.2 takové informace sdělí:
    - 11.2.2.1 osobám, které mají ze zákona stanovenou povinnost mlčenlivosti; a/nebo
    - 11.2.2.2 subdodavatelům, nebo jiným poradcům, zaměstnancům za předpokladu, že (i) dotčená Strana bude o takovém zpřístupnění v dostatečném předstihu informována, a že (ii) příslušné osoby, kterým budou Důvěrné informace poskytnuty, se písemně zaváží zachovat mlčenlivost a důvěrnost poskytnutých informací, a to minimálně v rozsahu stanoveném touto Smlouvou, a/nebo
  - 11.2.3 Objednatel Osobám LP a/nebo Ovládaným osobám včetně společnosti Letiště Praha, a. s.; a/nebo
  - 11.2.4 se takové informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku; a/nebo
  - 11.2.5 jedna Strana udělí Straně druhé písemný souhlas ke zpřístupnění informace třetí osobě.
- 11.3** Zhotovitel se zavazuje zajistit, aby povinnosti stanovené tímto článkem 11 dodržovali všichni jeho zaměstnanci a subdodavatelé jakýmkoliv způsobem se podílející na plnění předmětu této Smlouvy a jakékoliv třetí osoby, kterým byly Důvěrné informace Objednatele jakýmkoliv způsobem ze strany Zhotovitele zpřístupněny. Zhotovitel tímto pro vyloučení jakýchkoliv pochybností prohlašuje a souhlasí s tím, že v plném rozsahu odpovídá za jakékoliv porušení povinností stanovených v tomto článku 11 ze strany svých zaměstnanců a/nebo subdodavatelů a/nebo třetích osob, kterým byly Důvěrné informace Objednatele jakýmkoliv způsobem ze strany Zhotovitele zpřístupněny a Objednateli v plném rozsahu nahradí veškerou vzniklou újmu, a také odčiní Objednateli veškerou nemajetkovou újmu.
- 11.4** Objednatel se zavazuje zajistit, aby povinnosti stanovené tímto článkem 11 dodržovali všichni jeho zaměstnanci jakékoliv třetí osoby, kterým byly Důvěrné informace Zhotovitele jakýmkoliv způsobem ze strany Objednatele zpřístupněny. Objednatel tímto pro vyloučení jakýchkoliv pochybností prohlašuje a souhlasí s tím, že v plném rozsahu odpovídá za jakékoliv porušení povinností stanovených v tomto článku 11 ze strany svých zaměstnanců a/nebo třetích osob, kterým byly Důvěrné informace Zhotovitele jakýmkoliv způsobem ze strany Objednatele zpřístupněny a Zhotoviteli v plném rozsahu nahradí veškerou vzniklou újmu, a také odčiní Zhotoviteli veškerou nemajetkovou újmu.
- 11.5** Závazky obsažené v tomto odstavci týkající se zachovávání důvěrného charakteru informací zůstanou v plném rozsahu platné a účinné neohledně na ukončení platnosti této Smlouvy.

## **12. OCHRANA OSOBNÍCH ÚDAJŮ**

- 12.1** Smluvní strany se zavazují postupovat při plnění této Smlouvy v souladu s Nařízením jakož i v souladu se ZZOÚ.
- 12.2** Smluvní strany provádějí zpracování osobních údajů výhradně za účelem plnění Smlouvy. Pokud Dodavatel provádí zpracování osobních údajů pro jiné účely, činí tak v rozporu se Smlouvou, Objednatel nenesе za takové zpracování osobních údajů odpovědnost a Dodavatel je ve vztahu k těmto osobním údajům v postavení správce osobních údajů dle Nařízení a ZZOÚ.
- 12.3** Dodavatel se zavazuje provádět zpracování osobních údajů po dobu trvání Smlouvy a po dobu max. následujících tří (3) měsíců po jejím skončení a po uplynutí této doby se zavazuje tyto údaje zlikvidovat. Pokud Dodavatel provádí zpracování osobních údajů pro skončení takto určené doby, činí tak v rozporu se Smlouvou, Objednatel nenesе za takové zpracování osobních údajů

odpovědnost a Dodavatel je ve vztahu k těmto osobním údajům v postavení správce osobních údajů dle Nařízení a ZZOU.

- 12.4** Dodavatel se dále zavazuje technicky a organizačně zabezpečit zpracovávání osobních údajů tak, aby osobní údaje byly dostatečně chráněny a bylo s nimi nakládáno v souladu s Nařízením a ZZOU. Osobní údaje budou zpracovávány prostřednictvím výpočetní techniky a přístup k nim musí být dostatečným způsobem zabezpečen, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich neoprávněné změně, zničení či jinému zneužití osobních údajů.
- 12.5** Dodavatel se zavazuje nesdružovat osobní údaje zpracovávané za účelem plnění této Smlouvy s žádnými jinými osobními údaji získanými nebo zpracovanými za jiným účelem.
- 12.6** Dodavatel je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů a na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

### **13. SMLUVNÍ POKUTY A NÁHRADA ÚJMY**

- 13.1** V případě, že Zhotovitel nedodrží termín dodání Analýzy a/nebo dodání Díla, popř. samostatně objednaných uživatelských licencí uvedený v čl. 3.1 této Smlouvy, zaplatí Zhotovitel Objednateli smluvní pokutu ve výši 0,05 % z Ceny Analýzy a/nebo Ceny příslušné fáze Díla a/nebo uživatelských licencí podle článku 8 této Smlouvy za každý i započatý den prodlení.
- 13.2** Neodstraní-li Zhotovitel Vady uvedené v Předávacím protokolu ve lhůtě uvedené v článku 5.13 Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč, a to za každý i započatý den prodlení.
- 13.3** Nezahájí-li Zhotovitel odstraňování Vady ve lhůtě uvedené v článku 7.4 Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 1.000,- Kč za každou i započatou hodinu prodlení.
- 13.4** Neodstraní-li Zhotovitel Vady uvedené ve lhůtě uvedené v článku 7.4 Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč, a to za každých i započatých po sobě jdoucích 24 hodin prodlení, případně za každý započatý den prodlení, je-li to aplikovatelné.
- 13.5** Poruší-li Zhotovitel povinnost podle článku 11 a/nebo článku 12 této Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení.
- 13.6** Poruší-li Zhotovitel záruku podle článku 7.3 této Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení.
- 13.7** Poruší-li Zhotovitel jakoukoliv povinnost dle čl. 4 této Smlouvy, vyjma povinností vymezených v čl. 4.7 – 4.9 této Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 2.000,- Kč za každé jednotlivé porušení.
- 13.8** Poruší-li Zhotovitel jakoukoliv povinnost dle přílohy č. 6 této Smlouvy, anebo povinnost dle čl. 15.3 této Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 20.000,- Kč za každé takové porušení.
- 13.9** Poruší-li Zhotovitel jakoukoliv povinnost vymezenou v čl. 4.7 – 4.9 této Smlouvy, zavazuje se Zhotovitel uhradit Objednateli smluvní pokutu ve výši 20.000,- Kč za každé takové porušení.
- 13.10** Právo Objednatele požadovat zaplacení náhrady plné výše újmy vzniklé Objednateli v důsledku porušení kterékoliv ze smluvních povinností Zhotovitele zajištěných smluvní pokutou podle této Smlouvy není zaplacením příslušné smluvní pokuty dotčeno. I v případě kdy bude smluvní pokuta snižena soudem, zůstává zachováno právo Objednatele na náhradu škody či újmy v plné výši. Pokud jakýkoliv právní předpis stanoví pokutu (penále) pro porušení smluvních povinností (kdykoliv během trvání této Smlouvy), pak nebude takovým nárokem nijak dotčeno právo Objednatele na náhradu škody či újmy v plné výši.
- 13.11** Smluvní pokuta je splatná do čtrnácti (14) dnů ode dne doručení písemné výzvy Objednatele Zhotoviteli k jejímu uhrazení.



- 13.12** Zhotovitel se tímto výslovně zavazuje odčinit Objednateli jakoukoliv nemajetkovou újmu vzniklou Objednateli porušením povinností Zhotovitele podle této Smlouvy a/nebo v souvislosti s ním.
- 13.13** Strany se dohodly, že povinnost Objednatele k náhradě újmy vůči Zhotoviteli vzniklé Zhotoviteli porušením povinností Objednatele podle této Smlouvy a/nebo v souvislosti s ním je vyloučena v maximálním rozsahu povoleném platnými právními předpisy.
- 13.14** Má-li být Objednateli Zhotovitelem hrazena jakákoli finanční částka, která se úročí, sjednávají si Strany výslovně, že v těchto případech lze požadovat úrok z úroku.
- 13.15** V případě, že jednou okolností dojde k porušení více článků této Smlouvy a tedy by mělo dojít ke vzniku povinnosti Zhotovitele uhradit smluvní pokutu dle dvou nebo více ustanovení čl. 13. této Smlouvy, je Zhotovitel povinen uhradit Objednateli smluvní pokutu pouze podle toho ustanovení čl. 13 této Smlouvy, které zakládá povinnost uhradit smluvní pokutu vyšší.

## **14. KONTAKTNÍ ÚDAJE A DORUČOVÁNÍ**

- 14.1** Jakékoliv oznámení nebo dokument, který má být podle této Smlouvy učiněn písemně, musí být, pokud Smlouva nestanoví jinak, doručen osobně nebo zaslán doporučenou poštovní zásilkou či kurýrem na kontaktní údaje druhé Strany. Kontaktní údaje Stran jsou uvedeny v Příloze č. 3 této Smlouvy.
- 14.2** Jinou komunikaci, než která je uvedena v předešlém čl. 14.1 této Smlouvy může kterákoli ze Stran, pokud Smlouva nestanoví jinak, provádět vůči druhé Straně prostřednictvím elektronické pošty (e-mailem) na kontaktní údaje druhé Strany.
- 14.3** Každá Strana oznámí bez zbytečného odkladu druhé Straně jakékoliv změny kontaktních údajů uvedených v čl. 1.1.24, 1.1.27 a v Příloze č. 3 této Smlouvy formou doporučeného dopisu nebo emailem, a zaslání na kontaktní adresu uvedenou v Příloze č. 3 této Smlouvy (ve znění případných pozdějších řádných změn). Řádným doručením tohoto oznámení dojde ke změně doručovací adresy Strany bez nutnosti uzavření dodatku k této Smlouvě.
- 14.4** Nestanoví-li tato Smlouva jinak, bude jakákoliv komunikace v souvislosti s touto Smlouvou považována za doručenu druhé Straně:
- 14.4.1 v případě doporučené pošty třetí (3.) pracovní den po dni, ve kterém byla příslušná zásilka odevzdána k poštovní přepravě, poštovné předplaceno, ve správně nadepsané obálce,
- 14.4.2 v případě elektronické komunikace v okamžiku, kdy byla příslušná e-mailová zpráva doručena na řádně vyplněnou e-mailovou adresu druhé Strany – potvrzení od email serveru adresáta.

## **15. OSTATNÍ UJEDNÁNÍ**

- 15.1** Zhotovitel není oprávněn postoupit tuto Smlouvu ani jakákoli svá práva a povinnosti z této Smlouvy na třetí osobu bez předchozího písemného souhlasu Objednatele, a to ani částečně.
- 15.2** Strany se výslovně dohodly, že:
- 15.2.1 Zhotovitel je oprávněn započíst své splatné i nesplatné pohledávky za Objednatelem výlučně na základě písemné dohody s Objednatelem.
- 15.2.2 Zhotovitel není oprávněn jakkoli zastavit jakékoli své pohledávky za Objednatelem vyplývající z této Smlouvy.
- 15.3** Zhotovitel je povinen nejpozději v den uzavření této Smlouvy prokázat, že má zřízeno pojištění na pojistnou částku ve výši nejméně 1.000.000,- Kč pro případ obecné odpovědnosti za škodu způsobenou při provádění Díla Objednateli nebo třetí osobě. Uzavřením Smlouvy se Zhotovitel též zavazuje, že pojištění bude ve stejném nebo větším rozsahu udržovat až do ukončení platnosti této Smlouvy. Zhotovitel se po tuto dobu zavazuje Objednateli na jeho výzvu do dvou (2) Pracovních dnů předložit doklad o trvání takového pojištění.

## 16. ZÁVĚREČNÁ USTANOVENÍ

- 16.1** Je-li nebo stane-li se některé ustanovení této Smlouvy neplatným, nevymahatelným nebo neúčinným, nedotýká se tato neplatnost, nevymahatelnost či neúčinnost ostatních ustanovení této Smlouvy. Strany se zavazují nahradit do pěti (5) Pracovních dnů po doručení výzvy druhé Strany neplatné, nevymahatelné nebo neúčinné ustanovení ustanovením platným, vymahatelným a účinným, jehož znění bude odpovídat účelu vyjádřenému původním ustanovením a touto Smlouvou jako celkem.
- 16.2** Vyšší moc.
- 16.2.1 Ani jedna ze Stran nebude v prodlení se splněním svých závazků vyplývajících ze Smlouvy z důvodu existence okolnosti vyšší moci, pokud tato okolnost znemožní nebo podstatným způsobem ovlivní plnění závazků takové Strany vyplývajících ze Smlouvy. Bezprostředně předcházející věta tohoto odstavce platí pouze po dobu existence takové okolnosti vyšší moci nebo trvání jejích následků a pouze ve vztahu k závazku nebo závazkům Strany přímo nebo bezprostředně ovlivněných takovou okolností vyšší moci.
- 16.2.2 Za okolnost vyšší moci se pokládají takové události, které Strana nemohla v době uzavření Smlouvy předvídat a které Straně objektivně brání v plnění jejích smluvních závazků vyplývajících z této Smlouvy. Za okolnosti vyšší moci se považují zejména válka, embargo, zásah státu nebo vlády, teroristický čin, živelné události a stávka zaměstnanců Objednatele. Pro vyloučení pochybností se uvádí, že za okolnost vyšší moci se nepovažuje jakékoliv prodlení s plněním závazků kterýchkoli Zhotovitelů či smluvních stran Zhotovitele vůči Zhotoviteli, stávka zaměstnanců Zhotovitele a Zhotovitelů a smluvních partnerů Zhotovitele, jakož i insolvence, předlužení, konkurs, vyrovnání, likvidace či jiná obdobná událost týkající se Zhotovitele nebo jakéhokoliv Zhotovitele či smluvního partnera Zhotovitele a exekuce majetku Zhotovitele nebo jakéhokoliv Zhotovitele či smluvního partnera Zhotovitele.
- 16.2.3 Nastane-li kterákoliv z okolností vyšší moci popsaná v odstavci 16.2.2 této Smlouvy, podnikne Strana, na její straně překážka vznikla, veškeré kroky, které lze po takové Straně rozumně požadovat, jež povedou k obnově normální činnosti v souladu se Smlouvou, a to co nejrychleji s ohledem na okolnosti, které okolnost vyšší moci způsobily. Strana se zavazuje druhou Stranu informovat o tom, že nastala okolnost vyšší moci, bez zbytečného odkladu poté, co bude objektivně možné takovouto komunikaci uskutečnit.
- 16.2.4 Pokud bude okolnost vyšší moci trvat po dobu delší než deset (10) Pracovních dnů, zavazují se Strany na vzájemném jednání najít s využitím úsilí, které lze rozumně po Stranách požadovat, vhodné řešení nastalé situace.
- 16.3** Jestliže kterákoliv ze Stran přehlédne nebo promine jakékoliv neplnění, porušení, prodlení nebo nedodržení nějaké povinnosti vyplývajících z této Smlouvy, pak takové jednání nezakládá vzdání se takové povinnosti s ohledem na její trvajících nebo následné neplnění, porušení nebo nedodržení a žádné takové vzdání se práva nebude považováno za účinné, pokud nebude pro každý jednotlivý případ vyjádřeno písemně.
- 16.4** Práva a povinnosti Stran, které nejsou výslovně upraveny Smlouvou, se řídí ustanoveními Občanského zákoníku a dalšími aplikovatelnými právními předpisy České republiky. Smlouva, vztah mezi Objednatelem a Zhotovitelem a práva a povinnosti smluvních Stran z něj vyplývající se řídí a budou vykládány v souladu s právem České republiky.
- 16.5** Zhotovitel na sebe ve smyslu § 1765 odst. 2 Občanského zákoníku bere nebezpečí podstatné změny okolností, které mohou založit v právech a povinnostech Stran zvláště hrubý nepoměr. Zhotoviteli tak nevznikne právo domáhat se obnovy jednání o Smlouvě v případě takové podstatné změny okolností ve smyslu § 1765 odst. 1 Občanského zákoníku.
- 16.6** Zhotovitel není oprávněn podat v souladu s ustanovením § 1766 Občanského zákoníku návrh soudu na změnu závazku ze Smlouvy.

- 16.7** Tato Smlouva je uzavírána mezi podnikateli v rámci jejich podnikání, z tohoto důvodu se na tuto Smlouvu v souladu s ustanovením § 1797 Občanského zákoníku neuplatní ustanovení § 1793 až 1795 Občanského zákoníku o neúměrném zkrácení ani ustanovení § 1796 o lichvě.
- 16.8** S ohledem na uzavření Smlouvy mezi podnikateli v rámci jejich podnikání se Strany dále v souladu s ustanovením § 1801 Občanského zákoníku dohodly, že pro účely této Smlouvy se nepoužijí ustanovení § 1799 a § 1800 Občanského zákoníku o smlouvách uzavíraných adhezním způsobem.
- 16.9** Strany se dohodly, že zaplacením smluvní pokuty Zhotovitelem není dotčen nárok Objednatele požadovat náhradu škody v plné výši. I v případě, kdy bude smluvní pokuta snižena soudem, zůstává zachováno právo Objednatele na náhradu škody v plné výši. Pokud jakýkoliv právní předpis stanoví pokutu (penále) pro porušení smluvní povinnosti (kdykoliv během trvání této Smlouvy), pak nebude takovým nárokem nijak dotčeno právo Objednatele na náhradu škody v plné výši.
- 16.10** Tato Smlouva obsahuje úplné ujednání o předmětu Smlouvy a všech náležitostech, které Strany měly a chtěly ve Smlouvě ujednat, a které považují za důležité pro závaznost této Smlouvy. Žádný projev vůle Stran učiněný při jednání o této Smlouvě ani projev vůle učiněný po uzavření této Smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními této Smlouvy a nezakládá žádný závazek žádné ze Stran. Tato Smlouva nahrazuje veškeré ostatní písemné či ústní dohody učiněné ve věci předmětu této Smlouvy.
- 16.11** Strany sjednávají, že si nepřejí, aby nad rámec výslovných ustanovení této Smlouvy byla jakákoli práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi Stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu této Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak.
- 16.12** Strany si sdělily všechny skutkové a právní okolnosti, o nichž k datu podpisu této Smlouvy věděly nebo vědět musely, a které jsou relevantní ve vztahu k uzavření této Smlouvy. Kromě ujištění, která si Strany poskytly v této Smlouvě, nebude mít žádná ze Stran žádná další práva a povinnosti v souvislosti s jakýmkoli skutečnostmi, které vyjdou najevo a o kterých neposkytla druhá Strana informace při jednání o této Smlouvě. Výjimkou budou případy, kdy daná Strana úmyslně uvedla druhou Stranu ve skutkový omyl ohledně předmětu této Smlouvy.
- 16.13** Pro vyloučení všech pochybností Strany uvádějí, že žádný závazek dle této Smlouvy není fixním závazkem podle § 1980 Občanského zákoníku.
- 16.14** Odlišně od § 1987 odst. 2 Občanského zákoníku si Strany sjednávají, že nejistá a/nebo neurčitá pohledávka Objednatele je způsobilá k započtení.
- 16.15** Objednatel může namítnout neplatnost Smlouvy a/nebo jejího dodatku z důvodu nedodržení formy kdykoliv, a to i když již bylo započato s plněním.
- 16.16** Pro vyloučení pochybností Strany ujednávají, že ke splnění peněžitého dluhu podle této Smlouvy nelze použít směnku.
- 16.17** Strany se zavazují řešit veškeré spory, které mezi nimi mohou vzniknout v souvislosti s prováděním nebo výkladem této Smlouvy, smírným jednáním a vzájemnou dohodou. Pokud se nepodaří vyřešit předmětný spor do třiceti (30) dnů ode dne jeho vzniku, bude takový spor předložen jednou ze Stran věcně a místně příslušnému soudu. Strany si tímto sjednávají místní příslušnost obecného soudu Objednatele dle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
- 16.18** Objednatel Dodavatele upozorňuje a Dodavatel bere na vědomí, že Objednatel je osobou uvedenou v § 2 odst. 1 písm. n) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
- 16.19** Tato smlouva se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení, které je podepsáno platnými kvalifikovanými elektronickými podpisy smluvních stran.
- 16.20** Zhotovitel jako strana, vůči níž se práva Objednatele jako věřitele ze Smlouvy promlčují, tímto po zralé úvaze výslovným prohlášením prodlužuje délku promlčecí doby práv věřitele (tzn. Objednatele) vyplývajících z této Smlouvy na dobu patnácti (15) let.

**16.21** Tato Smlouva, není-li v ní uvedeno jinak, může být měněna a doplňována pouze prostřednictvím písemných průběžně číslovaných dodatků podepsaných oběma Stranami. Případná změna tohoto ustanovení o změně Smlouvy musí být učiněna také prostřednictvím písemného dodatku podepsaného oběma Stranami. Objednatel je oprávněn namítnout neplatnost Smlouvy a/nebo jejích dodatků z důvodu nedodržení písemné formy kdykoliv, a to i když již bylo započato s plněním.

**16.22** Součástí této Smlouvy je dále níže uvedený dokument Objednatele:

Standardy ICT,

(otisk SHA256: 671b70d1d77d9c21ac00e9e6b101c8e2f47ad40d05b0edd1e3686f046d894e5e) upravující další práva a povinnosti Stran vyplývající z právního vztahu založeného touto Smlouvou (dále též „Standardy“).

Strany prohlašují, že Objednatel zveřejnil Standardy na svém profilu ([https://zakazky.prg.aero/publication\\_display\\_22.html](https://zakazky.prg.aero/publication_display_22.html)), tedy profilu zadavatele, v rámci zadávacího řízení předcházejícího uzavření této Smlouvy spolu s ostatními podklady vztahujícími se k zakázce, na jejíž plnění byla uzavřena tato Smlouva. Zhotovitel prohlašuje a činí nesporným, že Zhotovitel měl možnost si Standardy z profilu zadavatele stáhnout a uložit a uchovat si tak jejich obsah (a že způsob jejich zveřejnění tento postup umožňoval) a že měl dostatek času se se Standardy před podáním nabídky v rámci zadávacího řízení předcházejícího uzavření této Smlouvy, resp. též před uzavřením této Smlouvy, řádně seznámit. Zhotovitel prohlašuje a činí nesporným, že Objednatel poskytl před uzavřením Smlouvy Dodavateli Standardy, Dodavatel se s nimi řádně seznámil, souhlasí s nimi a zavazuje se je dodržovat. Zhotovitel prohlašuje, že rozumí významu toho ustanovení Smlouvy.

**16.23** Nedílnou součástí této Smlouvy jsou následující přílohy:

16.23.1 Příloha č. 1 – Technická specifikace Systému

16.23.2 Příloha č. 2 - Podrobná kalkulace Ceny Díla

16.23.3 Příloha č. 3 – Kontaktní osoby

16.23.4 Příloha č. 4 - Harmonogram Implementace

16.23.5 Příloha č. 5 - Akceptační protokol

16.23.6 Příloha č. 6 - Požadavky informační bezpečnosti

16.23.7 Příloha č. 7 – Požadavky na akceptaci Analýzy

**STRANY TÍMTO PROHLAŠUJÍ, ŽE SI TUTO SMLOUVU PŘEČETLY A ŽE SOUHLASÍ S JEJÍM OBSAHEM,  
NA DŮKAZ ČEHOŽ JI STVRZUJÍ SVÝMI PODPISY:**

Datum:

Za Objednatele:

Podpis: \_\_\_\_\_

Jméno: Ing. Jiří Pos

Funkce: Předseda představenstva

Datum:

Za Zhotovitele

Podpis: \_\_\_\_\_

Jméno: Mgr. Dan Rosendorf

Funkce: Předseda představenstva

Podpis: \_\_\_\_\_

Jméno: Ing. Jiří Kraus

Funkce: Místopředseda představenstva

## Specifikace rozsahu díla, dodávky nástroje pro PAM

### Popis prostředí Letiště Praha, a.s. pro implementaci PAM

Letiště má vysoce segmentovanou síť, kdy jednotlivé infrastrukturní a systémové celky jsou v oddělených VLANs a to za několika úrovněmi firewall ochrany.

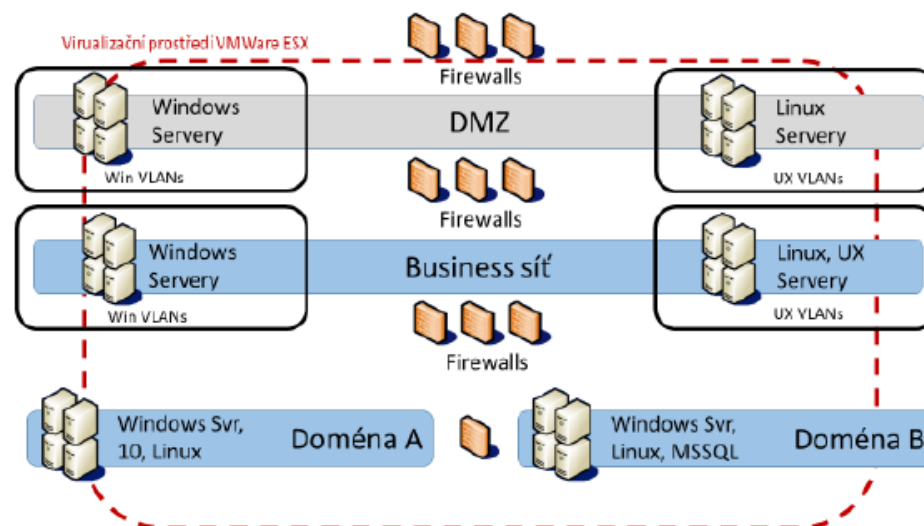
Prostředí Letiště lze rozdělit na základní části:

- DMZ – část, kde jsou Windows a Linux systémy dostupné z internetu. DMZ má minimálně 2 VLANs oddělující typově dle použitého operačního systému.
- Business síť, která zahrnuje velké množství VLANs obsahující Linux/Unix/AIX, Windows systém a síťové systémy a dedikované síťové prvky.
- Interní část Letiště – zde jsou systémy oddělené jak od internetu, tak od business sítě Letiště.
- OT systémy Letiště – představují velkou skupinu systémů, které jsou specifické pro svojí úzce zaměřenou funkčnost a jedná se o systémy oddělené od standardních IT systémů, někdy dokonce zcela offline fungující jako uzavřené „clustery“ mimo hlavní síť Letiště.
- Síťové prvky Letiště jako jsou switche, routery, firewally, proxy apod.
- Cloudové prostředí Letiště provozované v Microsoft Azure/O365.

Z technologického pohledu je možné rozdělení na Windows servery, Linux/Unix/AIX, síťové služby, virtualizační platformy a segmentace dle aplikací, databází a specializovaných systémů.

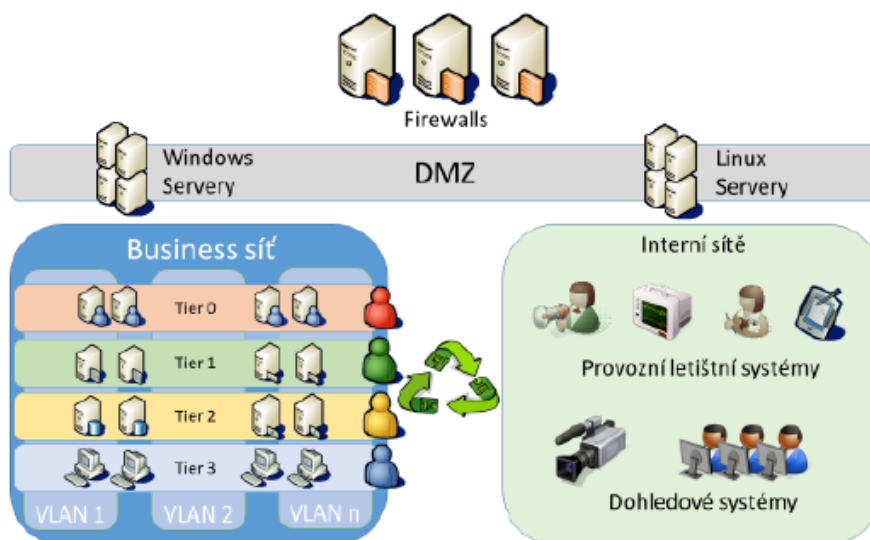
Letiště se skládá ze 4 nasazených domén:

- DMZ – nejméně důvěryhodné prostředí s Windows a Linux servery a aplikacemi otevřenými do internetu. 2 domain controllery.
- Business doména – integruje business systémy a aplikace a infrastrukturní části integrované na úrovni správy identit. Tato obsahuje největší počet serverů a stanic. 4 domain controllery.
- Dvě oddělené domény A a B se 4 domain controllery.

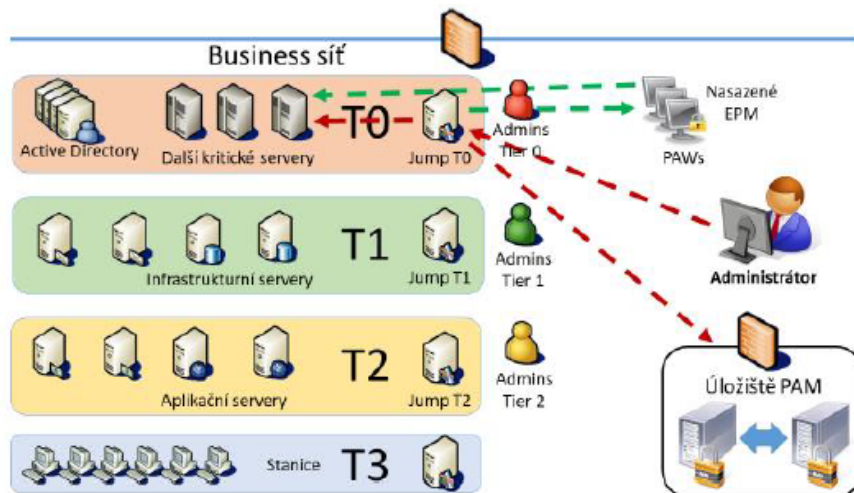


Do budoucna se plánuje s nasazením další oddělené domény pro OT systémy Letiště v rozsahu min. 2 domain controllerů.

Všechny tyto systémy jsou oddělené na úrovni síťové segmentace. Kromě síťové segmentace má Letiště aplikovaný tierový model a to jak na úrovni jmenných účtů, tak na úrovni rozdělení serverů a stanic.



Do jednotlivých systémů se privilegovaní uživatelé dostávají prostřednictvím "jump" serverů nebo PAW stanic. "Jump" servery jsou segmentovány jak na úrovni sítí, tak jsou rozděleny dle tierového modelu a mohou se na ně přihlašovat jen uživatelé s privilegovaným účtem ze stejného tieru a pro daný typ systémů. V případě externích dodavatelů jsou využívány jak "jump" servery, tak přímý přístup ve VPN. Tyto přístupy jsou hlídány poměrně rozsáhlou množinou vlastních SIEM pravidel určených k dohledu nad privilegovanými uživateli.



Pro implementaci PAM se předpokládají následující kroky, které budou revidovány a specifikovány na základě detailní analýzy s vybraným Dodavatelem.

Základní rozdělení implementace PAM je na fázi 1 a fázi 2, kdy fáze 1 je určena pro infrastrukturní správce, servery a vybrané kritické systémy.

V této fázi musí být pokryté minimálně týmy administrátorů:

- Windows
- Linux/UX/AIX
- Síťové prvky
- DBA
- Oddělení kybernetické bezpečnosti
- Vybraní aplikační správci (bude určeno v analýze do naplnění celkové kapacity do 50 uživatelů ve fázi 1)
- Vybraní externí uživatelé (dodavatelé) - budou specifikováni během analýzy

Fáze 2 pokrývá především aplikační část Letiště, zbývající aplikační správce, OT systémy, zbývající dodavatele Letiště, cloud a zbývající systémové části Letiště, které nebyly řešeny ve fázi 1. Implementace a rozsah fáze 2 bude vycházet z fáze 1, efektivity nasazení PAM, dokončení k fázi 2 vázaných interních projektů a dle celkového stavu letecké dopravy a z toho vyplývajících požadavků na Letiště v následujících letech. Fáze 2 je pro zadavatele nepovinná a realizuje se formou dodatečné objednávky maximálně až do poptávaného rozsahu dle přílohy „Cenová kalkulace“.

Následující prostředí Letiště budou během obou fází projektu integrovány do PAM nebo minimálně analyzovány (OT systémy):

- První oddělená doména A
  - Doména má 2 domain controllery.
  - V doméně je do 20 Windows serverů a do 1400 koncových zařízení s Windows 10.
  - Doména A má nasazený tierový model pro jmenné účty a má plochou síťovou strukturu.

- 
- Použité systémy: Windows Server 2016, 2019, Windows 10.
    - Ve fázi 1 projektu PAM je požadována integrace serverů a všech koncových zařízení. Tato doména je navrhována jako první pro zavedení do PAM kvůli jednoduché struktuře vhodné k úvodní instalaci a konfiguraci základních komponent PAM prostředí.
  - Druhá oddělená doména B, kde jsou systémy základní služby provozující dohledové systémy oddělené od ostatních částí Letiště.
    - Doména má 2 domain controllery.
    - Doména B má nasazený tierový model pro jmenné účty se střední mírou síťové segmentace mezi servery a stanicemi.
    - V doméně je do 100 Linux/Windows serverů a cca 2000 specializovaných dohledových zařízení.
    - Použité systémy: Windows Server 2016, 2019, Windows 7, 10, SQL Server v doméně, Debian, RedHat.
    - Ve fázi 1 je požadována integrace serverů. Ve fázi 2 budou integrovaná dohledová zařízení alespoň pro základní přístupy administrátorů, při jejich vzdálené správě. Při analýze bude určeno, která specializovaná zařízení jsou typově vhodná pro zařazení do PAM.
  - Business část sítě Letiště, která je tvořena jak doménovými tak nedoménovými zařízeními.
    - Business síť má 4 domain controllery.
    - Doména má cca 500 Windows serverů a 2500 standardních stanic s Windows 10, PAW stanice s Windows 10.
    - V síti je cca 400 Linux/AIX serverů mimo doménu bez zavedení LDAP.
    - V této síti dochází k výrazným změnám počtu zařízení.
    - Pro Linux servery je možné využít Ansible.
    - Business síť má nasazený tierový model pro jmenné účty a vysokou míru síťové segmentace.
    - Použité systémy: Windows Server 2012, 2016, 2019, Windows 7, 10, Debian, RedHat, Oracle Linux, AIX, Microsoft Exchange, SCOM, SQL Server, Oracle, Sybase, MySQL, Maria DB, VMWare ESX.
    - Ve fázi 1 je požadována kompletní integrace serverů business sítě a stanic.
  - Správa síťové infrastruktury.
    - Použité systémy: F5, Juniper, Baracuda, Cisco, Checkpoint, Pulse Secure.
    - Integrace do PAM bude provedena ve fázi 1.
    - Koncových zařízení pro integraci ve fázi 1 cca 1000.
  - Webové aplikace určené pro privilegované uživatele viz. Technická specifikace bod „Webové aplikace - management konzole“. Vše integrováno do PAM během fáze 1.
  - Databázové systémy v business části sítě.
    - Jde o cca 10 instancí MySQL/Maria DB v DMZ, dále cca 70 instancí Oracle, SQL Server, Sybase, Maria Db.
    - Je požadována integrace všech databázových systémů pro DBA během fáze 1.
  - DMZ část je tvořena Windows a Linux servery.
    - Doména s Windows servery a Linux servery mimo LDAP.
    - Koncových zařízení do 150.
    - DMZ má nasazený tierový model pro jmenné účty a střední míru síťové segmentace.
    - Použité systémy: Windows Server 2012, 2016, 2019 v doméně, Linux RedHat, Debian, Ubuntu, RedHat, MySQL, Maria DB.
-

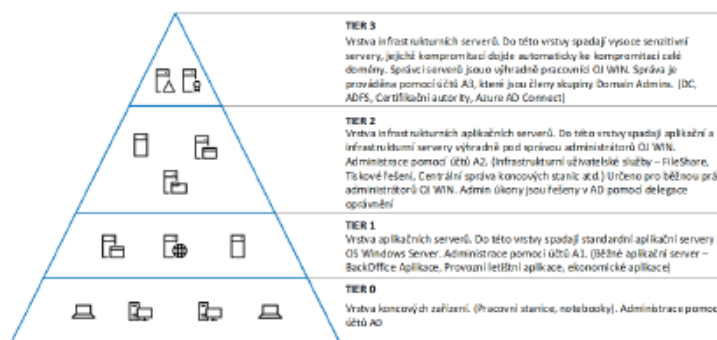


- Z DMZ VLANs nebude povolený přímý přístup na úložiště dat ve vnitřní síti Letiště. Způsob nasazení bude předmětem detailní analýzy a dle typu vybrané PAM technologie.
  - Je požadována integrace všech serverů během fáze 1.
- OT systémy.
  - Jedná se o značně rozsáhlé a různorodé prostředí v počtu 100+ tisíc zařízení, kde aktuálně dochází ke konsolidaci asset managementu v rámci interního OT/CAFM projektu.
  - V OT systémech dochází k výrazným změnám počtu zařízení.
  - OT systémy nejsou řízeny doménou, ale je plánováno její nasazení v následujících letech v rozsahu 2 DC.
  - Předpokládá se vzorová implementace některých systémů jako Rockwell, SCADA atd. v jednotkách typových zařízení během fáze 2.
  - Z pohledu PAM se předpokládá vytvoření dedikovaných „jump“ serverů především pro externí dodavatele přistupující na OT zařízení a do řídicích OT systémů jako úvodní proces zavedení PAM pro OT prostředí.
  - Vzhledem k obrovskému rozsahu OT prostředí bude plně nasazení PAM pro OT řešené v samostatném projektu a to v závislosti na konsolidaci OT, zavedení PERA architektury a rozhodnutí, které systémy budou v PAM.
  - Dodavatelé nebudou v rámci stávajícího projektu počítat s výše uvedeným rozsahem všech OT zařízení, ale budou realizovat pouze analýzu OT a instalaci „jump“ serveru pro dodavatele během fáze 1. Vzorové integrace OT zařízení budou realizované ve fázi 2 na základě analýzy OT z fáze 1 a čerpaní MD ve fázi 2 samostatnou objednávkou.
- Přihlašování do Azure pro privilegované uživatele.
  - Ve fázi 1 je požadována integrace pro privilegované uživatele přistupující na Azure portál, O365 a nasazené cloudové projekty s počtem do 100 hostů.
  - Aktuálně je v cloudu do 1700 zařízení, které nejsou určeny pro fázi 1. Jejich případná integrace bude realizována na základě rozhodnutí jejich začlenění do PAM a samostatné objednávky ve fázi 2.
  - Celkový počet zařízení v cloudu se bude v následujících letech pravděpodobně výrazně měnit.
- Externí uživatelé.
  - Aktuálně se jedná až do 200 externích privilegovaných uživatelů. V případě obnovy letecké dopravy v rozsahu před pandemií je možné očekávat výrazný nárůst.
  - Pro fázi 1 je požadována implementace minimálně 50 externistů.
  - Maximální celkový počet přihlášených externích uživatelů do sítě Letiště je 58 za den za poslední rok.
  - Tito uživatelé využívají jak dedikované „jump“ servery, tak přímý přístup na koncová zařízení v rámci VPN.
  - Přístup externích uživatelů bude sjednocený do PAM se zadokumentovaným postupem, který bude replikovatelný zaměstnanci Letiště, aby zaměstnanci Letiště byli schopni autonomně vytvářet přístupy pro externí uživatele.
- Ve fázi 2 dojde k integraci zbývajících systémů pro aplikační správce. Naprostá většina těchto systémů běží v business síti a DMZ, kde se předpokládá nasazení specializovaných „jump“ serverů pro OT správce a externí dodavatele. Detailní popis bude uvedený v analýze.

## Základní rozdělení Tierového modelu Letiště Praha

Microsoft prostředí je rozděleno do 4 úrovní na základě posouzení bezpečnostních dopadů při kompromitaci objektů v jednotlivých vrstvách. Tier model Letiště vychází z modelu publikovaného na <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>. S tím rozdílem, že model na Letišti je číslován obráceně oproti modelu Microsoftu (Microsoft označuje jako nejkritičtější vrstvu 0 vs. na Letišti je nejkritičtější vrstva 3 viz. dále).

Pro každou vrstvu je administrátorovi vytvořen jmenný účet pro administraci konkrétní vrstvy. Hlavní snahou je zabránění vertikálního pohybu šíření kompromitace, tzn. zabránit kompromitaci zařízení nebo uživatelských účtů ve vyšších vrstvách tierového modelu.



Do Tieru 0 spadají veškerá uživatelská koncová zařízení a uživatelské Terminálové servery. U této kategorie vycházíme z předpokladu, že nemáme pod kontrolou fyzickou ochranu zařízení, tzn. nejsme schopni např. kontrolovat připojení Keyloggeru apod. Laterální pohyb v rámci této vrstvy je potom omezován použitím technologií Lokální Firewall, LAPS, Bitlocker, Credential Guard, BitDefender atd.

Prefix administrátorských účtů pro tier 0: a0[e / i / u] - e – externista, i - zaměstnanec LP ICT, u - zaměstnanec LP mimo ICT.

V Tieru 1 jsou umístěné běžné aplikační servery. Pro tyto aplikační servery platí, že správci serveru jsou administrátoři z oddělení aplikačních správců mimo infrastrukturní správce. Omezení laterálního pohybu je dále řešeno síťovou segmentací pro vybrané systémy, nasazením technologií LAPS a lokálních Firewallů.

Prefix administrátorských účtů pro tier 1: a1[e / i / u]

Tier 2 a Tier 3 jsou určeny pro servery výhradní správě infrastrukturních administrátorů. Do Tieru 2 patří servery pro aplikace a standardní infrastrukturní služby, které spravují WIN administrátoři. Typicky do této vrstvy spadají – FileShare, licenční servery, Exchange, WSUS servery, monitoring. Administrátorské účty v této vrstvě jsou určeny pro běžnou/každodenní práci administrátora. Spadají sem tak veškeré úkony, které není potřeba vykonávat s oprávněním „Domain Admin“. Specifické činnosti v Active Directory (vytváření běžných uživatelských účtů, editace aplikačních GPO apod.) jsou potom řešeny delegací přímo pro konkrétní účel. Hlavním účelem této vrstvy je zajistit, aby běžná činnost administrátorů nebyla vykonávána účtem s oprávněním „Domain Admin“.

Prefix administrátorských účtů pro tier 2: a2i

---

V Tieru 3 jsou umístěny servery, jejichž kompromitací automaticky dochází ke kompromitaci celé Active Directory.

Primárně jsou zde zařazené tyto systémy/servery:

- Domain Controllers
- Certifikační Autority
- ADFS Servery, Azure AD Connect

Prefix administrátorských účtů pro tier 3: a3i

V Tieru 3 jsou administrátorské účty zařazené do skupiny „Domain Admins“.

#### Tier model v UX prostředí

Tierový model je postupně aplikován do dalších prostředí jako Linux/Unix/AIX, kde jsou zachovávány stejné principy jako pro technologie Microsoft. Ale pouze s tím rozdílem, že prefix privilegovaných účtů je x např. x1i.jméno pro privilegovaného uživatele ze zaměstnanců Letiště oddělení Linux správců.

#### Tier model v cloudovém prostředí

V cloudovém prostředí je nasazený tierový model se stejnými principy, jaké platí pro Windows prostředí. Naming účtů je vytvářen identicky neboli jsou zde vytvořené účty s a[tier n][e/i/u] prefixem. Nejedná se ale o analogické účty vytvořené v on-premise prostředí v Active Directory, ale jsou to samostatné privilegované cloudové účty vytvářené jen v Azure Active Directory bez jakékoliv propagace do on-premise.

#### Jump servery

Jedná se o jiné servery než standardní Terminal Server (na TS je povoleno instalovat standardní aplikace pro vzdálenou práci).

Jump servery slouží výhradně pro přihlašování administrátorů a pro přístup na další systémy v daném tier. Někdy může docházet ke kombinovanému nasazení jump a terminál serverů.

Uživatelé se k Jump serveru hlásí vždy administrátorským účtem dle Tieru ve kterém je Jump server zařazený. Uživatelé jump serveru nejsou standardně zařazení do skupiny lokálních administrátorů serveru. V lokálních administrátorech jsou pouze vybraní uživatelé, kteří mají oprávnění instalovat na Jump servery aplikace potřebné pro administraci ICT systémů.

Jump server má nastavené FW prostupy odpovídající dané tier, ve které se nachází a jen na členské servery povoluje vstup a vice versa tyto servery povolují vstup z daného tier jump serveru.

Standardní uživatelé ani jiné než A[num]i účty nemají povoleno instalovat aplikace na jump servery. Pokud by k tomu došlo, bude to znamenat bezpečnostní incident v SIEM.

#### Konsolidace Jump serverů

V rámci projektu PAM se požaduje konsolidace „jump serverů“ na jednotnou technologii a jasně nastavenými pravidly pro instalaci a hardening těchto „jump serverů“ s důrazem na maximální izolaci session a zároveň uživatelskou přívětivost. Zabezpečení musí být na úrovni nedovolující neautorizované osobě (nebo malware kódu) přístup do kritických systémů Letiště

Cílem je také efektivní zabezpečení PAW stanic používanými administrátory, kde jsou instalace podřízené potřebám administrátorů při zachování maximální bezpečnosti. Předpokládá se, že bude

potřeba zachovat specifické přístupy, které nepůjde pokrýt konsolidovanými „jump“ servery avšak s nasazením maximální možné ochrany i pro tyto přístupy.

## VPN přístupy do sítě Letiště

Připojování uživatelů do vnitřních sítí Letiště probíhá přes technologie:

- Pulse Secure klient
- F5 klient
- F5 portál

Přihlašování do VPN probíhá multifaktorově s využitím SMS jako druhého faktoru. Po autentizaci mají uživatelé přidělené profily s povolenými prostory na firewallech a dle toho mohou přistupovat na koncové systémy a aplikace.

Přes klienta Pulse Secure nebo F5 vzniká plnohodnotná VPN, která spojuje zařízení uživatele s vnitřní sítí Letiště, kdy dochází k aktualizaci politik zařízení a dostupnosti síťových prvků Letiště dle oprávnění uživatele. Připojení přes F5 portál je možné pro vytvořený profil uživatele, které mu dovolí RDP spojení na dedikované koncové systémy jako je pracovní stanice a koncový serverový bod, obvykle terminal server nebo „jump“ server, ale stanice nemá vytvořený VPN tunel do sítě Letiště.

Privilegovaní uživatelé se aktuálně mohou připojit jak přímo tak nepřímo pomocí „jump“ serverů na koncové systémy, stanice a PAW, pokud to mají povolené prostory na firewallech. Záměrem PAM projektu je změnit současný model, aby privilegovaní uživatelé museli přistupovat do serverového prostředí pouze prostřednictvím PAM systému a to včetně PAW stanic, na které je bude PAM přesměrovávat. Pro běžné uživatele zůstane současný VPN model zachován.

## Nasazení EPM technologie

EPM technologie představují velmi silný nástroj s dopadem na mnoho systémových funkcí a jejich nasazení je plánováno pro vybrané části Letiště.

Implicitně není povolena instalace EPM agentů na servery, dokud nedojde k otestování instalovaných EPM komponent a jejich dopad na provoz (pro domain controllery to platí striktně viz. kapitola „Agenti na domain controllerech“).

Často jsou servery pod kombinovanou správou Letiště a dodavatelů a není možné libovolně instalovat komponenty třetích stran. Pro běžné servery není ve fázi 1 plánováno nasazení EPM, ale je plánováno pro PAW stanice a „jump“ servery.

Pro nasazení EPM je navrhován scénář, kdy např. skriptovací technologie jako Powershell nebudou povolené z „jump serverů“, ale bude možné je použít z PAW stanic. Na nich budou nainstalovány EPM agenti, kteří budou řídit elevace oprávnění uživatelů, kontrolovat spouštěné aplikace, skripty a jejich podepisování apod. a oproti standardním „jump“ serverům poskytnou administrátorům možnost nadstandardního zásahu při vysokém zabezpečení.

V některých doménách a tierech může být vyžadováno povolení skriptovacích nástrojů také na „jump“ serverech, protože pro určité domény nemusí být povolený přístup z PAW stanic nebo někteří administrátoři nemají PAW stanice (např. dodavatelé). V takovém případě je navrhováno použít EPM na „jump“ serverech. Konečný scénář bude určen po analýze s Dodavatelem, se kterým bude specifikována vhodná architektura a nasazení EPM.

## Agenti na domain controllerech

Jak bylo uvedeno v kapitole „Nasazení EPM technologie“ není implicitně povoleno instalovat agenty na DC a to jak EPM agenty, tak případně další. Instalace agentů na klíčové prvky infrastruktury podléhá otestování a schválení ze strany Letiště.

**Pokud by případný dodavatel PAM vyžadoval pro základní funkčnost instalaci agentů na DC, tak Letiště si vyhrazuje právo posoudit míru rizika a dopadu na DC a případně takové řešení vyloučit.**

Povinnost testování platí také pro volitelné agenty, jako jsou agenty pro ochranu DC před Kerberos útoky. Pro fázi 1 se předpokládá nasazení agentů na DC v testovacím prostředí Letiště a po úvodním testování jejich nasazení do domény A se dvěma DC a to na testovací období až 1 rok. Zbývajících 8 produkčních DC +2 plánované pro OT systémy je uvedeno v příloze „Cenová kalkulace“ ve fázi 2 jako opce a o jejich nasazení bude rozhodnuto dle výsledků testování.

## PAW stanice

Letiště má nasazený model PAW stanic, který není využíván napříč všemi administrátory, ale je aplikován jen na některé organizační jednotky.

V rámci dodávky bude od vybraného Dodavatele požadována konfigurace EPM politik pro PAW stanice a to jak s ohledem na elevaci privilegií, tak na povolené aplikace především se zaměřením na programové a skriptovací nástroje.

Na PAW stanice přistupují privilegovaní uživatelé pod jejich jmennými tierovými účty, které odpovídají rozsahu jejich přístupu a to tak, že tierový účet na PAW stanici je buď roven nebo o jednu úroveň níž, než je jejich maximální oprávnění přístupu v serverovém tieru. Např. pokud uživatel může přistupovat jen na servery v nejnižším tier 2, tak se na PAW stanici hlásí svým tier 2 jmenným účtem. Ale pokud uživatel může přistupovat až na nejvyšší tier 0, tak na PAW stanici se hlásí o jednu úroveň tieru nižším účtem tedy jmenným účtem pro tier 1.

Na PAW stanicích je zakázáno používat běžné uživatelské a doménové účty, případně aplikační účty a mohou zde být použité jen jmenné tierové účty privilegovaných uživatelů.

PAW stanice jsou fyzické počítače umístěné v zabezpečených prostorách Letiště.

Na PAW stanice se privilegovaní uživatelé mohou připojit přes VPN. Do VPN se uživatelé hlásí ze svých běžných stanic přes VPN klienta (F5 nebo Pulse Secure) a pak se RDP protokolem připojí na PAW stanici pod svým tierovým účtem. Případně se administrátoři mohou na PAW stanice připojit z vybraných terminal/jump serverů, které jsou umístěné v dedikovaných VLAN. Pro RDP připojení jsou nastaveny restriktivní politiky jako omezení kopírování souborů apod. Tento model by se měl změnit nasazením „jump“ serverů PAM, přes které by administrátoři přistupovali na svoje PAW stanice a jejich relace budou nahrávané.

Od Dodavatele je minimálně požadováno ve vztahu k PAW stanicím a nabídkám řešení:

- Rámcový návrh na nasazení EPM na PAW (jaké scénáře Dodavatel doporučuje a je možné řešit nabízenou technologií PAM).
  - Způsob ochrany PAW stanic (zamykání a odemykání, při výše popsaném modelu použití privilegovaných účtů na PAW a nasazení PAM).
  - Doporučená rozšíření autentizačních prvků pro PAW kompatibilních s PAM technologií (např. autentizační tokeny apod.). Dodávka rozšiřujících prvků není předmětem tohoto projektu.
  - Doporučení na případnou virtualizaci PAW a vhodnou konfiguraci ve vztahu k PAM.
-

Detailní rozpis s návrhem řešení bude proveden během analýzy.

## Disaster recovery a break-glass scénáře

Součástí nabídky bude rámcový popis pro řešení disaster recovery a break-glass scénářů, který bude detailně rozpracován při analýze s vybraným dodavatelem.

Letiště má vytvořený základní model pro break-glass účty, který bude revidován na základě PAM projektu.

Aktuálně jsou "break-glass" účty uchovávány dvěma způsoby:

- KeePass pro vysoce privilegované zásahové účty. Typicky je tento scénář používán síťovými administrátory, kteří potřebují přistupovat pod root oprávněním k odpojeným síťovým zařízením. Tyto KeePass soubory jsou uloženy v zašifrované podobě na zásahových zařízeních administrátorů (jejich pracovní notebooky) a chráněné heslem dle Bezpečnostních standardů Letiště.
- Účty uloženy v trezoru na Helpdesk Letiště.

Postup vyzvedávání "break-glass" účtů není v tuto chvíli sjednocen.

Scénáře dodavatelů pro DR a "break-glass" musí minimálně zahrnovat:

- Kompletní výpadek celého PAM systému.
- Výpadek některého ze základních systémů Letiště např. virtualizační platforma.
- Výpadek konektivity na některé ze základních prvků PAM.
- Selhání některého z prvků PAM a doporučený postup pro jeho zálohování a obnovu.
- Výpadek bezpečného úložiště dat včetně fatálního výpadku jak primárního tak sekundárního nodu.
- Výpadek webového portálu a scénáře pro přístup k úložišti dat.
- Doporučené postupy na zajištění dostupnosti webového portálu a jeho redundance.
- Výpadek konektivity v prostředí Letiště a řešení přihlašování privilegovaných uživatelů.
- Doporučené postupy pro nasazení "break-glass" účtů, způsob úschovy, periodicitu změn, nakládání s nimi apod.

Speciální pozornost bude Dodavatel 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.

S vybraným Dodavatelem bude vydefinována testovací matice DR a "break-glass" scénářů a ta bude testována při akceptaci řešení.

## Vysvětlení k dodávce hardware

V rámci dodávky PAM je poptáván hardware pro bezpečné úložiště dat a pro webovou konzoli.

Všechn hardware musí splňovat všechny body uvedené v „Obecné požadavky na HW“ v příloze „Technická specifikace“.

Pro úložiště je požadována dodávka hardware pro dva samostatné servery určené pro primární a sekundární DR node, které budou ve stejné hardware konfiguraci. Jejich konfigurace bude odpovídat požadavkům:

- Kapacita a rychlost zápisu dat do úložného prostoru musí být schopná pokrýt minimálně 200 souběžně připojených privilegovaných uživatelů
- Počet paralelních spojení otevřených jedním administrátorem a nahrávané relace uložit po dobu minimálně 365 dní.
- Minimální počet jader na jeden server bezpečného úložiště je 32 případně vyšší dle doporučení výrobce pro danou zátěž.
- Minimální velikost RAM na jeden server je 128GB případně vyšší dle doporučení výrobce pro danou zátěž.
- Disky musí být hot-swap řízené RAID řadičem s minimální kapacitou 4 TB případně vyšší dle doporučení výrobce pro danou zátěž.
- Dvouportová (dual port) HBA karta Fibre Channel s rychlostí každého portu min. 16Gbs, včetně optických SFP+ modulů
- Minimálně 4 ethernet portů 100/1000 Mb/s (100BASE-TX,1000BASE-T).
- Server musí mít alespoň jeden volný PCIe slot pro rozšiřující karty.
- Dvojice nezávislých napájecích zdrojů.
- Výkon dle PassMark CPU Mark ([www.cpubenchmark.net](http://www.cpubenchmark.net)) nejméně 28000 bodů.
- Servery pro bezpečné úložiště jsou dodávány jako celek včetně licence operačního systému a všech PAM licencí nutných pro provoz úložiště. Dodavatel za tento celek ručí jak během implementace, tak následně během správy dle Servisní smlouvy.

Hardware pro webovou konzoli je poptáván jako jeden ze serverů, na kterých poběží webové rozhraní. Tento server nebude zařazený do virtualizačního prostředí Letiště, ale je plánován pro případ výpadku virtualizačního prostředí a redundantní zajištění dostupnosti služeb PAM přes webové rozhraní. (jedná se o řešení jednoho z DR scénářů viz. kapitola Letiště, má nasazený model PAW stanic, který není využíván napříč všemi administrátory, ale je aplikován jen na některé organizační jednotky.

V rámci dodávky bude od vybraného Dodavatele požadována konfigurace EPM politik pro PAW stanice a to jak s ohledem na elevaci privilegií, tak na povolené aplikace především se zaměřením na programové a skriptovací nástroje.

Na PAW stanice přistupují privilegovaní uživatelé pod jejich jmennými tierovými účty, které odpovídají rozsahu jejich přístupu a to tak, že tierový účet na PAW stanici je buď roven nebo o jednu úroveň níž, než je jejich maximální oprávnění přístupu v serverovém tieru. Např. pokud uživatel může přistupovat jen na servery v nejnižším tier 2, tak se na PAW stanici hlásí svým tier 2 jmenným účtem. Ale pokud uživatel může přistupovat až na nejvyšší tier 0, tak na PAW stanici se hlásí o jednu úroveň tieru nižším účtem tedy jmenným účtem pro tier 1.

Na PAW stanicích je zakázáno používat běžné uživatelské a doménové účty, případně aplikační účty a mohou zde být použité jen jmenné tierové účty privilegovaných uživatelů.

PAW stanice jsou fyzické počítače umístěné v zabezpečených prostorách Letiště.

Na PAW stanice se privilegovaní uživatelé mohou připojit přes VPN. Do VPN se uživatelé hlásí ze svých běžných stanic přes VPN klienta (F5 nebo Pulse Secure) a pak se RDP protokolem připojí na PAW stanici pod svým tierovým účtem. Případně se administrátoři mohou na PAW stanice připojit z vybraných terminal/jump serverů, které jsou umístěné v dedikovaných VLAN. Pro RDP připojení jsou nastaveny restriktivní politiky jako omezení kopírování souborů apod. Tento model by se měl změnit

---

nasazením „jump“ serverů PAM, přes které by administrátoři přistupovali na svoje PAW stanice a jejich relace budou nahrávány.

Od Dodavatele je minimálně požadováno ve vztahu k PAW stanicím a nabídkám řešení:

- Rámcový návrh na nasazení EPM na PAW (jaké scénáře Dodavatel doporučuje a je možné řešit nabízenou technologií PAM).
- Způsob ochrany PAW stanic (zamykání a odemykání, při výše popsaném modelu použití privilegovaných účtů na PAW a nasazení PAM).
- Doporučená rozšíření autentizačních prvků pro PAW kompatibilních s PAM technologií (např. autentizační tokeny apod.). Dodávka rozšiřujících prvků není předmětem tohoto projektu.
- Doporučení na případnou virtualizaci PAW a vhodnou konfiguraci ve vztahu k PAM.

Detailní rozpis s návrhem řešení bude proveden během analýzy.

Disaster recovery a break-glass scénáře“).

Letiště plánuje k tomuto samostatnému hardware s webovou konzolí provozovat druhý server ve virtualizaci, který bude zajišťovat vysokou dostupnost webového rozhraní PAM pro privilegované uživatele.

Licence operačního systému pro hardware s webovou konzolí zajistí Letiště, pokud se bude jednat o Windows Server.

Požadavky na hw pro webovou konzoli:

- Minimální počet jader je 16 případně vyšší dle doporučení výrobce pro danou zátěž.
- Minimální velikost RAM je 128GB případně vyšší dle doporučení výrobce pro danou zátěž.
- Disky musí být hot-swap řízené RAID řadičem s minimální kapacitou 4 TB případně vyšší dle doporučení výrobce pro danou zátěž.
- Minimálně 4 ethernet portů 100/1000 Mb/s (100BASE-TX,1000BASE-T).
- Server musí mít alespoň jeden volný PCIe slot pro rozšiřující karty.
- Dvojice nezávislých napájecích zdrojů.
- Výkon dle PassMark CPU Mark ([www.cpubenchmark.net](http://www.cpubenchmark.net)) nejméně 22000 bodů.

Výše uvedený popis má informativní charakter pro přípravu nabídek.

## Fáze projektu implementace PAM

Pro dodávku PAM řešení je požadováno, aby se skládala z minimálně následujících fází:

- Vstupní analýza – provedení vstupní analýzy s výstupním dokumentem s minimálním pokrytím bodů dle popisu níže,,
  - Instalace – instalace řešení na prostředky dodané při realizaci řešení a na vlastní prostředky Letiště,
  - Implementace – provedení nastavení, konfigurace, vč. všech provozních nastavení dle požadavků Letiště,
  - Testování – testování funkčnosti dodávaného řešení před akceptací díla,
  - Dokumentace,
  - Zaškolení – odborné zaškolení správců a administrátorů dodávaného řešení a dalších specialistů řešení využívající,
-



- 
- Akceptace – provedení akceptačních procedur a předání do ostrého provozu.

#### Vstupní analýza

Dodavatel provede 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 se Zadavatelem, kdy dojde k vysvětlení aktuálních procesů nakládání s privilegovanými účty ze strany Letiště a vysvětlení technologického zázemí Letiště. Zadavatel předpokládá využití know-how a zkušeností Dodavatele, který v rámci analýzy navrhne nejvhodnější způsob, jak odhalené typy účtů vhodně řídit a spravovat a toto řešení udržovat efektivní v čase. Tato aktivita může probíhat paralelně s aktivitou analýzy existujících privilegovaných účtů a bude realizována na základě organizační dohody mezi zástupci Dodavatele a Letiště.

Výstupem těchto činností bude dokument (viz. dále), obsahující popis budoucího stavu řízení všech typů privilegovaných účtů.

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.

Dodavatel na základě vstupní analýzy vytvoří finální dokument nazvaný „*Implementační plán projektu PAM*“ pro následnou realizaci díla, který bude popisovat minimálně tyto body:

- Základní popis řešení, technologií a technických konceptů.
  - Obecné technické předpoklady a požadavky na realizaci řešení.
  - Architektura řešení s jejím vysvětlením.
  - Procesy a služby systému s jejich rozpisem a vysvětlením jejich účelu v rámci řešení.
  - Popis systémů třetích stran a jejich integrace.
  - Integrovaná architektura se systémy Letiště (SIEM, AD/LDAP, SMTP, NTP atd.).
  - Popis nakládání s daty, jejich uložení, zabezpečení, ochrana.
  - Detailní síťový a komunikační model řešení včetně interní komunikace mezi vnitřními prvky řešení.
  - Návrh politik PAM řešení detailně specifikovaných během analýzy a vycházející z „best practice“ doporučení výrobce technologie.
  - Technologické požadavky na zajištění provozu.
  - Popis konfigurace komponent PAM řešení.
  - Uživatelská příručka PAM řešení a popis rozhraní z pohledu uživatele (z pohledu majitelů privilegovaných účtů uživatelsky přístupujících k PAM).
  - Uživatelská příručka PAM řešení z pohledu administrátorů a popis primárních úkonů, které administrátoři PAM budou vykonávat (může být formou odkazů na ostatní kapitoly detailně se věnující konkrétním bodům např. Zálohování apod.).
  - Detailní popis instalačních postupů a to včetně testovacího prostředí.
  - 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).
  - Návrh metodiky nakládání s “break-glass” účty a scénáře na jejich otestování (bude součástí akceptačních testů).
  - Popis způsobů aktualizace PAM řešení (všechny části PAM).
  - Bezpečnostní zajištění řešení včetně souladu se ZoKB.
  - Soulad s GDPR.
-

- Monitoring PAM řešení.
- Návrh harmonogramu projektu a procesních kroků pro implementaci řešení včetně návrhu konfigurace řešení v jednotlivých fázích implementace a definice finální podoby dodávaného řešení. Harmonogram bude vycházet z navrženého harmonogramu od Zadavatele uvedeného v zadávací dokumentaci.
- Popis náběhu systému (popis pilotní/testovací fáze až do doby akceptace).
- Postup testování a testovacích scénářů.
- Akceptační kritéria včetně postupu akceptace.
- Požadavky na součinnost.
- Detailní specifikace lokální podpory Dodavatele potažmo Výrobce a definování postupů pro její využití.
- Specifikace požadavků a rozsahu na školení zástupců Letiště (bude v rozsahu standardizovaných školení administrátorů od Výrobce technologie).
- Návrh maximálně automatizovaného discovery procesu privilegovaných účtů po zavedení PAM.
- Návrh na provádění assesment analýz PAM systému zaměstnanci Letiště (četnost, rozsah, hlavní oblasti assesmentu, automatizace assesment procesu, scoring apod.).
- Návrh procesu technické profylaxe PAM řešení (musí probíhat minimálně jednou ročně) ze strany Dodavatele, případně za součinnosti s Výrobce.

Kromě výše uvedených základních bodů musí Dodavatel v rámci Analýzy vytvořit návrh konkrétních kroků včetně stanovení odpovědností pro tyto body:

- a. 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).
- b. Zrušení uživatele PAM – Zrušení účtu na úrovni PAM řešení v případě, že účet není nadále používán (např. v případě odchodu zaměstnance ze Společnosti, odebrání účtu externího dodavatele apod.).
- c. 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.
- d. Přidělení/odebrání role uživateli PAM – Přidělení/odebrání role (např. správce PAM, uživatel, auditor) uživateli PAM.
- e. 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).
- f. Použití privilegovaného účtu – Poskytnutí přístupu uživatele PAM (interního/externího administrátora) k privilegovanému účtu prostřednictvím PAM řešení (tj. v případě že má uživatel přístup schválen).
- g. 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.

- h. **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 viz. kapitola “Disaster recovery a break-glass scénáře” v Detailní technické specifikaci.
- i. **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) viz. kapitola “Disaster recovery a break-glass scénáře” v Detailní technické specifikaci.
- j. **Žádost o změnu konfigurace** – Zpracování žádosti o změnu konfigurace PAM (např. vytvoření nové/změna stávající politiky).
- k. **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).
- l. **Sledování či ukončení relace** – Sledování aktivní relace nebo její předčasné ukončení odpovědnou osobou (např. člen dohledového týmu).
- m. **Žádost o nahrávání relace** – Zpracování žádosti o nahrávání relací pro konkrétního uživatele (na vyžádání, pokud PAM systém není nastaven k nahrávání všech relací).
- n. **Žádost o zpřístupnění nahrávky** – Zpracování žádosti o zpřístupnění nahrávky relace pořízené pomocí PAM řešení.

Některé z bodů analýzy budou vzhledem ke svojí specifické povaze vázané na způsob implementace PAM řešení a během fáze Analýzy bude specifikováno, o které se jedná. Tyto body budou dále doplňovány v rámci implementační fáze a jejich naplnění bude vyhodnoceno při akceptaci řešení. Příkladem takového bodu je Disaster recovery proces nebo použití “break-glass” účtů, který bude mít základní specifikaci během Analýzy, ale jeho finální podoba bude stanovena a zadokumentována až po otestování a případných úpravách, které mohou vyplynout až v testovací fázi.

#### Instalace

- Dodavatel realizuje dodávané řešení PAM v prostředí Letiště ve shodě s Implementačním plánem projektu,
- veškeré náklady související s dopravou a instalací jdou na vrub Dodavatele,
- instalace řešení PAM bude provedena do vyhrazené infrastruktury Zadavatele nebo do dodaného hardware, který je součástí dodávky a je dedikovaný pro běh řešení.
- Technici Dodavatele splňují veškeré podmínky dané výrobcem PAM pro jeho instalaci.

#### Implementace

Dodavatel provede potřebnou konfiguraci a nastavení systému PAM a všech komponent dle níže uvedených požadavků. Implementace bude zahrnovat, zejména:

- vytvoření produkčního a testovacího prostředí PAM odpovídajícího detailní analýze,
- nastavení politik pro PAM,
- nastavení a zabezpečení úložiště hesel a nahrávek privilegovaných uživatelů,
- nastavení nahrávání privilegovaných relací a jejich optimalizace s ohledem na přenosovou rychlost a úložný prostor,,
- integrace koncových zařízení a pro systémy uvedené v Příloze C bude provedena integrace řízení hesel privilegovaných účtů včetně bezheslového přihlášení se na integrované

zařízení/systém (SSO), pokud to vybraná PAM technologie bude přímo podporovat nebo pokud bude nutné v rámci implementace provést proprietární napojení,

- zachování neovlivněného hesla nejvyšší úrovně oprávnění a dalších "break-glass" účtů (v obálce do trezoru),
- integrace na SIEM IBM QRadar,
- integrace s monitorovacími systémy Letiště,
- za součást implementace je považována také součinnost při konfiguraci sítě a bezpečnostního monitoringu.

#### Produkční a testovací prostředí

Při implementaci PAM řešení bude vytvořeno jak produkční, tak testovací prostředí, kdy obě prostředí se budou vzájemně zrcadlit z pohledu základních konfiguračních parametrů. Testovací prostředí musí zajistit vždy alespoň jednu z částí PAM systému, které budou implementovány v produkčním prostředí a to v obdobné konfiguraci.

Cílem je, aby testovací prostředí sloužilo jak v době implementace PAM systému, tak následně po jeho zavedení a to především pro činnosti:

- vývoj a testování napojení na systémy integrované do PAM,
- testování konfigurací PAM, které se budou následně promítat do produkčního prostředí,
- testování aktualizací komponent PAM před jejich nasazením do produkčního prostředí,
- zaškolení administrátorů a uživatelů do PAM.

Testovací prostředí bude realizováno na virtualizační platformě Letiště a Dodavatel musí zajistit všechny potřebné licence PAM systému pro testovací prostředí. Letiště zajistí licence pro CAL, RDS a prostředí operačních systémů (např. Windows Server).

Rámcové požadavky na testovací prostředí uvede Dodavatel v nabídce. Licence PAM software na testovací prostředí musí být součástí standardní licence PAM dle přílohy C zadávací dokumentace.

#### Testování

Dodavatel zajistí řádné otestování řešení PAM dle navržených testovacích a akceptačních scénářů v implementačním plánu projektu. Zejména budou provedeny následující testy:

- funkční testy - ověří, že implementované PAM řešení poskytuje bezchybně všechny požadované funkcionality detailně vydefinované během fáze Analýzy a odpovídající technickým požadavkům vycházejícím z přílohy C zadávací dokumentace,
- bezpečnostní testy zahrnující penetrační testy - ověří, že jsou všechny komponenty zabezpečeny dle požadavků vydefinovaných během fáze Analýzy, že odpovídají doporučeným postupům Výrobce, především pak maximální zabezpečení bezpečného úložiště, zabezpečení a šifrování dat, správná konfigurace oprávnění přístupů a jejich segmentace apod.,
- DR testy - ověří, že v případě výpadku jednotlivých částí PAM řešení nebo dokonce totálního výpadku existují navržené postupy na obnovu včetně postupů pro obnovu databáze hesel a přístupu k ní při naprostém výpadku PAM systému.

Dodavatel k realizaci testů zajistí:

- Návrh testování a k tomu potřebné nástroje, testovacích scénářů a hodnotících kritérií,
- Přípravu prostředí a testovacích dat v součinnosti se Zadavatelem (testovací data musí odpovídat prostředí Letiště),
- Testovací protokoly s výstupy z testů,

Detailní popis testů bude specifikován v analýze řešení PAM.

## Dokumentace

Součástí dodávky musí být dokumentace minimálně v následujícím rozsahu:

- Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace.
- Produktová dokumentace výrobce ke všem dodávaným modulům PAM,
- Instalační dokumentace (předpis pro prvotní instalaci a instalační postupy pro údržbu a rozvoj systému PAM) a dokumentace k integrovaným systémům
- Administrátorské a uživatelské příručky (manuály),
- Popis havarijních plánů pro obnovu služeb PAM systému,
- Dokumentace ke všem logům – hlavně popis struktury logů, seznam událostí s jejich významem a vazbou na jednotlivé operace.

Uvedená dokumentace je požadována v českém jazyce. Produktová dokumentace výrobce, včetně dokumentace výrobce popisující strukturu a význam logů, je akceptovatelná v anglickém nebo českém jazyce.

Pravidelná aktualizace dokumentace bude prováděna v rámci služeb servisní podpory, a to pravidelně při jakékoliv změně, např. aktualizacích (patchování, upgrade) realizovaného PAM řešení, pokud nebude dohodnuto jinak.

## Použité zkratky

DC – Domain Controller

DMZ – Demilitarized Zone

DR – Disaster Recovery DWH – Data Warehouse

EPM – Endpoint Privilege Management

GPO – Group Policy Object

MD – Man Day, člověkodenní

OT – Operational Technology

PAM – Privilege Access Management

PAW – Privilege Access Workstation

VLAN – Virtual Local Area Network

Příloha č. 2 – Podrobná kalkulace Ceny díla

Kalkulace Nabídkové ceny - PIM/PAM		Fáze 1/4 roky				Fáze 2 / **			
Položka	Popis položky	Množstevní jednotka (MJ)	Fixní počet MJ	Cena za MJ v Kč bez DPH	Cena celkem v Kč bez DPH	Množstevní jednotka (MJ)	Předpokládaný Počet MJ*	Cena za MJ v Kč bez DPH	Cena celkem v Kč bez DPH
Software (počet primárních uživatelských licencí)***	Uživatelské licence pro správu a použití PAM systému uživateli Zadavatele.	licence na uživatele	50	52108,8	2 605 440 Kč	licence na uživatele	110	44641	4 910 510 Kč
Software (počet externích uživatelských licencí)***	Uživatelské licence pro externí uživatele, kteří nejsou v přímém vztahu vůči Zadavateli.	licence na uživatele	50	11949	597 450 Kč	licence na uživatele	250	10396	2 599 000 Kč
Software (počet serverových licencí)	Všechny serverové licence nutné pro provoz systému v HA režimu.	serverové licence	0	0	0 Kč	serverové licence	0	0	0 Kč
EPM licence stanice	Licence pro Endpoint Protection Management na PAW stanicích.	desktop licence	10	3978	39 780 Kč	desktop licence	150	3670	550 500 Kč
EPM licence servery	Licence pro Endpoint Protection Management na serverech.	serverové licence	5	9282	46 410 Kč	serverové licence	95	8562	813 390 Kč
Počet domain controllerů	Licence vztahující se k nasazení PAM systému na domain controllery.	serverové licence	2	87516	175 032 Kč	serverové licence	10	76877	768 770 Kč
Ostatní licence nutné k provozu řešení	Všechny licence jak výrobce technologie tak třetích stran, které není možné zařadit do specializovaných licenčních položek. Dodavatel doplní jednotlivé položky licence a rozeplíše typ, počet a cenu.	APP-STATIC-SUBS - Secret management for homegrown static applications including C3 Credential Provider integrations	5	40112	200 560 Kč	ostatní licence	0	0	0 Kč
Hardware (nutné hw k provozování řešení) - bezpečné úložiště	Kompletní HW náklady pro provoz bezpečného úložiště v HA režimu. HW pro zátěž vyplývající ze součtu zátěže Základní fáze a Fáze 2. Dodavatel uvede přesnou konfiguraci nabízeného HW.	ks	2	277667	555 334 Kč				
Hardware (nutné hw k provozování řešení) - webová konzole	Kompletní HW náklady pro provoz webové konzole. HW pro zátěž vyplývající ze součtu zátěže Základní fáze a Fáze 2. Dodavatel uvede přesnou konfiguraci nabízeného HW.	ks	1	219324	219 324 Kč				
Analýza*	Analýza prostředí, návrh prováděcí dokumentace dle "technické specifikace" a "Průvodní popis k technickému zadání".	člověkoden	36	19000	684 000 Kč				
Instalace hardware	Základní instalace a konfigurace hardware, OS a dalších previzit PAM.	člověkoden	3	17000	51 000 Kč				
Instalace software	Instalace softwarových částí PAM do prostředí Letiště	člověkoden	3	17000	51 000 Kč				
Implementace a integrace do stávajícího prostředí	Napojení na všechny požadované platformy a integrace s dalšími klíčovými prvky infrastruktury dle "Technické specifikace" a "Průvodního popisu k technickému zadání".	člověkoden	12	17000	204 000 Kč				
Zkušební provoz	Ověření provozu včetně napojení na klíčové infrastrukturní prvky.	člověkoden	2	17000	34 000 Kč				
Dokumentace	Dokumentace skutečného stavu a nasazení PAM.	člověkoden	2	17000	34 000 Kč				
Akceptační testy	Provedení akceptačních testů dle specifikace popsané v analýze.	člověkoden	4	17000	68 000 Kč				
Zaškolení	Zaškolení do administrace řešení, způsobu použití, popisu a ukázky scénářů pro údržbu a obnovu, doporučené "best practice" při využití PAM řešení. Školení se budou účastnit pouze zaměstnanci Zadavatele.	člověkoden	10	17000	170 000 Kč				

### Příloha č. 3 Kontaktní osoby

#### Adresa pro doručování.

(a) Adresa pro doručování Objednatele:

**Letiště Praha, a. s.**

Jana Kašpara č.p. 1069/1, Praha 6, 160 08

Česká republika

K rukám: výkonného ředitele ICT

(b) Adresa pro doručování Zhotovitele:

**ICZ a.s.**

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

Česká republika

K rukám: .....

#### Odpovědné osoby:

Odpovědným zástupcem k zastupování **smluvní strany Zhotovitele ve smluvních záležitostech** souvisejících s plněním této Smlouvy je:

.....

Odpovědným zástupcem k zastupování **smluvní strany Zhotovitele v technických záležitostech** souvisejících s plněním této Smlouvy je:

.....

Odpovědným zástupcem k zastupování **smluvní strany Objednatele v technických záležitostech** souvisejících s plněním této Smlouvy je:

.....

Odpovědným zástupcem k zastupování **smluvní strany Objednatele ve smluvních záležitostech** souvisejících s plněním této Smlouvy je:

.....

#### Příloha č. 4 – Harmonogram Implementace

*	Popis aktivity	Termín	Trvání
<b>1.</b>	<b>Podpisy smluv</b>	T0	<b>1PD</b>
<b>2.</b>	Realizace projektu 1. fáze (kick off)	T1+10	<b>10PD</b>
<b>3.</b>	<b>Analýza</b>	T2+60	<b>60PD</b>
<b>4.</b>	Posouzení a vyhodnocení analýzy	T3+15	<b>15PD</b>
<b>5.</b>	Instalace HW	T4+10	<b>10PD</b>
<b>6.</b>	Instalace SW - instalace PAM (7+3+10) - základní systémy + testovací prostředí	T5+30	<b>30PD</b>
<b>7.</b>	Integrace SW do 3. systémů LP	T6+60	<b>60PD</b>
<b>8.</b>	Školení pro LP - úvodní seznámení	T7+5	<b>5PD</b>
<b>9.</b>	Testovací provoz I - Pilotní provoz s privilegovanými uživateli Letiště	T8+44	<b>44PD</b>
<b>10.</b>	Testovací provoz II - PEN testy 1. fáze a vyhodnocení bezpečnostních parametrů	T9+42	<b>42PD</b>
<b>11.</b>	Kompletace a odevzdání dokumentace stavu PAM	T11+5	<b>5PD</b>
<b>12.</b>	Akceptace dokumentace ze strany LP	T12+5	<b>5PD</b>
<b>13.</b>	Školení pro LP - pokročilé školení	T13+5	<b>5PD</b>
<b>14.</b>	Akceptace/dokončení 1. fáze	T14+5	<b>5PD</b>

Harmonogram počítá s ideálním průběhem projektu bez započítání možného větvení, které může vzniknout např. opravnými termíny definovanými Smlouvou o dílo.

PD - pracovní dny

\*v závislosti na aplikaci čl. 5.4 Smlouvy může dojít k prodloužení tohoto termínu.



---

---

---

---

---

---

## Příloha č. 5 Předávací protokol

---

**Smlouva (objednávka) Letiště Praha, a.s. č. / Contract Nr.:**

**Dodavatel/Strana:**

**Předmět akceptace:**

**Datum akceptace:**

---

### VYJÁDŘENÍ K AKCEPTACI

Předmět plnění je akceptován

"bez výhrad/s výhradami"

---

### VÝHRADY K AKCEPTACI

<b>ID</b>	<b>Závažnost</b>	<b>Popis</b>	<b>Datum odstranění</b>

\* Klasifikace typu/závažnosti výhrady dle příslušného smluvního vztahu. Např.: A/B/C, 1/2/3/4, apod.

---

### SEZNAM PŘÍLOH

---

### SCHVALOVACÍ DOLOŽKA

<b>Datum / Date</b>	<b>Jméno / Name</b>	<b>Funkce / Position</b>	<b>Podpis / Signature</b>

## **Příloha č. 6 Požadavky informační bezpečnosti**

### **1. ÚVOD**

Účelem tohoto dokumentu je definovat závazné bezpečnostní, organizační a technické požadavky pro poskytovatele, jejichž předmětem plnění pro objednatele je (výhradně či jako součást předmětu plnění jiné služby) vývoj, implementace a/nebo servis software či hardware (dále také jen „SW“ či „HW“), nebo kteří v souvislosti s plněním pro objednatele přistupují do informačního systému objednatele (dále také „IS LP“) a/nebo kteří v rámci poskytovaného plnění pro objednatele zpracovávají, a/nebo přenášejí a/nebo ukládají a/nebo archivují jakákoli data a informace objednatele a/nebo jeho zákazníků (dále také jen „Bezpečnostní požadavky“).

### **2. OBECNÉ POŽADAVKY**

#### **2.1** Poskytovatel bere na vědomí, že

- 2.1.1 informační systém Objednatele je certifikován v souladu s normou ČSN ISO/IEC 27001:2013.
- 2.1.2 část informačního systému Objednatele je součástí informačního systému základní služby v souladu se Zákonem č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

#### **2.2** Poskytovatel se při poskytování plnění pro objednatele zavazuje plnit následující povinnosti:

- 2.2.1 pokud poskytovatel využívá při poskytování plnění poddodavatele, poskytovatel se zavazuje zajistit dodržování Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se poskytovatel zavazuje doložit objednateli na vyžádání předložením příslušného smluvního vztahu uzavřeného s tímto poddodavatelem, případně předložením čestného prohlášení o řádném naplňování této povinnosti;
- 2.2.2 nestanoví-li dohoda stran jinak, poskytovatel jmenuje nejpozději do 3 dnů po uzavření Smlouvy zodpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních požadavků a související komunikace mezi smluvními stranami (dále také jen „Kontaktní osoba“).
- 2.2.3 Pokud při plnění předmětu Smlouvy dochází ke zpracování osobních údajů, poskytovatel se zavazuje zajistit uzavření samostatné přílohy ve smyslu příslušných ustanovení nařízení GDPR;
- 2.2.4 dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů společnosti objednatele resp., platné řídicí dokumentace objednatele či její části, pokud byl s takovými dokumenty nebo jejich částmi seznámen.

### **3. BEZPEČNOSTNÍ POŽADAVKY NA VÝVOJ SW**

#### **3.1** Poskytovatel se při poskytování plnění pro objednatele zavazuje:

- 3.1.1 poskytovat objednateli v termínech stanovených objednatel, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje SW či po jeho předání;
- 3.1.2 k dodání systémové a provozní bezpečnostní dokumentace nejpozději do doby předání a převzetí SW způsobem uvedeným ve Smlouvě,
- 3.1.3 že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování SW a/nebo které jsou specifikovány výslovně ve Smlouvě (zejména, že SW nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky, nepotřebný SW třetích stran apod.);
- 3.1.4 že pokud součástí plnění je i instalace operačního systému případně SW třetích stran, v průběhu jeho instalace budou použity nejnovější aktualizované verze těchto produktů;

- 3.1.5 že veškeré důvěrné informace<sup>1</sup> poskytnuté objednateli při realizaci plnění nebudou uchovávány v nešifrovaném tvaru a budou chráněna vůči neautorizovanému přístupu, pokud nebude mezi smluvními stranami v konkrétním případě dohodnuto jinak;
- 3.1.6 že v rámci poskytovaného plnění bude instalovat SW nebo jejich upgrade podle hardeningových bezpečnostních politik, kterými je standard CIS (<https://www.cisecurity.org>) level (group) 1 a v souladu s bezpečnostními standardy Objednatele (platí pro poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen);
- 3.1.7 že v produkčním prostředí systému ICT bude obsažen jen kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování systému ICT;
- 3.1.8 že pokud součástí plnění je implementace SW v produkčním prostředí IS LP provede, před jeho spuštěním kontrolu souladu daného SW s bezpečnostními požadavky hardeningových bezpečnostních politik a v případě zjištění nesouladu zajistí bez zbytečného odkladu soulad dodávaného SW s bezpečnostními požadavky hardeningových politik (platí pro poskytovatele, pokud byl s takovými bezpečnostními standardy seznámen).
- 3.1.9 že pokud součástí plnění je implementace SW v produkčním prostředí IS LP bude instalovat nový SW nebo nové verze SW pouze na základě objednatel předem schválených migračních postupů<sup>2</sup>;

#### **4. FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ**

- 4.1 Poskytovatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT anebo datové nosiče,
- 4.2 Poskytovatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému ICT, který je předmětem plnění dle této Smlouvy.

#### **5. ŘÍZENÍ PŘÍSTUPU**

- 5.1 V případě, že součástí plnění je přístup zaměstnanců LP k externím webovým službám, musí být dodrženy následující požadavky:
  - 5.1.1 Přihlašovací údaje nesmí být uloženy v čitelné podobě, ale musí být chráněny dostatečně silnými kryptografickými prostředky.
  - 5.1.2 Systém, ke kterému zaměstnanci LP přistupují, musí být pravidelně testován, aktualizován a být dostatečně odolný tak, aby byla zajištěna bezpečnost informací a dat.
  - 5.1.3 Objednatel si vyhrazuje možnost provedení penetračního testování, předmětu plnění, v průběhu trvání smlouvy. Náklady na penetrační testy, které provádí Objednatel na základě svých rozhodnutí, jsou hrazeny z jeho finančních prostředků.
  - 5.1.4 V případě, že výsledkem penetračního testování jsou kritická zjištění je Poskytovatel povinen neprodleně informovat LP o těchto skutečnostech a přijmout dostatečná a účinná nápravná opatření.
  - 5.1.5 Přístupová hesla musí být dostatečně silná, tzn. minimálně 12 znaků, komplexnost hesla (heslo musí obsahovat znaky z minimálně 3 typů), maximální a minimální doba používání hesla a možnost opakování hesel musí být nastavitelná.
- 5.2 V případě, že součástí plnění je přístup k produkčnímu prostředí IS LP musí být dodrženy následující požadavky:
  - 5.2.1 Poskytovatel bere na vědomí, že přístup k systémům IS LP je možné povolit pouze fyzické identitě zaměstnance poskytovatele nebo poddodavatele zaevidované v registru identit objednatel, a to na základě požadavku poskytovatele na přístup.

<sup>1</sup> Za důvěrné informace se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, konfigurační soubory, systémové programy, kritické knihovny, obnovovací procedury apod.

<sup>2</sup> Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více systémy ICT.

- 5.2.2 Přístupová hesla musí být dostatečně silná, tzn. minimálně 12 znaků, komplexnost hesla (heslo musí obsahovat znaky z minimálně 3 typů), maximální a minimální doba používání hesla a možnost opakování hesel musí být nastavitelná.
- 5.2.3 Poskytovatel bere na vědomí, že zaměstnanec poskytovatele musí prokazatelně souhlasit se zpracováním osobních údajů potřebných pro zřízení přístupu, v opačném případě objednatel není povinen přístup k systému ICT zaměstnanci poskytovatele povolit. Zaměstnanec poskytovatele s přiděleným přístupem (fyzickým, logickým) k systému ICT musí prokazatelně souhlasit se zpracováním osobních údajů zpracovávaných během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách objednatele (např.: monitoring pomocí řešení Security Incident and Event Monitoring), přičemž takový souhlas musí být proveden souhlasem písemným nebo digitálním formou emailu, není-li smluvními stranami dohodnuto jinak.
- 5.2.4 Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele musí být řízeno principem nezbytného minima a není nárokové.
- 5.2.5 Poskytovatel se zavazuje, že udělený přístup nebude sdílen více zaměstnanci poskytovatele nebo poddodavatele.
- 5.2.6 Poskytovatel se zavazuje, že přístup do systému ICT prostřednictvím mobilní aplikace bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN.
- 5.2.7 Poskytovatel se zavazuje, že před připojením koncového zařízení, mobilní koncového zařízení nebo aktivního síťového prvku jako síťové switche, WiFi access pointy, routery či huby do počítačové sítě požádá o schválení připojení Kontaktní osobu na straně objednatele
- 5.2.8 Poskytovatel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.
- 5.2.9 Poskytovatel se zavazuje, že nebude instalovat a používat tyto typy nástrojů:
- Keylogger,
  - Sniffer,
  - Analyzátor zranitelností a Port Scanner,
- 5.2.10 Backdoor, rootkit a trojský kůň nebo jinou podobu malware.
- 5.2.11 Poskytovatel se zavazuje, že všechny ICT systémy poskytovatele, které se připojují do síťové infrastruktury objednatele, jsou a budou chráněny proti malware.
- 5.2.12 Poskytovatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému ICT programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému ICT nebo nelegální získání dat a informací.
- 5.2.13 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, ze zařízení, připojeného k IS LP:
- nenavštěvovali internetové stránky s eticky nevhodným obsahem<sup>3</sup>;
  - neukládali a/nebo nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno objednatele;
  - nestahovali, nesdíleli, neukládali, nearchivovali a/nebo neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
  - neukládali a/nebo nesdíleli data a informace společnosti na nepovolených datových úložištích nebo médiích;
  - nezasílali řetězové emaily.
- 5.2.14 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, kteří přistupují do interní sítě a/nebo systému ICT objednatele, respektovali a dodržovali následující omezení. Zařízení typu notebook/počítač musí mít aplikovány bezpečnostní záplaty (operačního

---

<sup>3</sup> Data a informace obsahující prvky extrémismu, terorismu, pornografie anebo podněcování k nesnášenlivosti a společenským předsudkům vztahujícím se ke společenské skupině identifikované na základě rasy, náboženství nebo víry, pohlaví, sexuální orientace, národnosti a etnické příslušnosti či jiné odlišnosti.

systému, internetového prohlížeče a Javy) a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

- 5.2.15 Poskytovatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění objednateli, kteří přistupují do interní sítě a/nebo systému ICT objednatele chránili autentizační prostředky a údaje k systémům ICT objednatele. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídicí dokumentace a mohou být uplatněny příslušné postupy zvládnání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Poskytovatel bere na vědomí, že postup zvládnání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany objednatele.

## **6. MONITOROVÁNÍ**

- 6.1** Dodavatel bere na vědomí, že veškerá jeho aktivita realizovaná v informačním systému Objednatele, může být Objednatelem průběžně a pravidelně monitorována.
- 6.2** Předmět plnění musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, v rozsahu stanoveném Vyhláškou, které umožní jednoznačně určit uživatele, čas a provedenu činnost.
- 6.3** Dodavatel se zavazuje, že umožní přístup k auditním údajům Objednateli v takové podobě, aby je bylo možné zpracovávat nástrojem IBM QRadar SIEM

## **7. PŘEDÁNÍ A PŘEVZETÍ PLNĚNÍ**

- 7.1** Poskytovatel bere na vědomí, že nedodržení Bezpečnostních požadavků včetně požadavku na předání kompletní systémové a provozní dokumentace je Vadou bránící převzetí předmětu Smlouvy (je Vadou kategorie A), přičemž objednatel není do doby odstranění příslušné Vady plnění povinen plnění převzít.
- 7.2** Poskytovatel odpovídá za to, že systémy ICT budou obsahovat nejnovější, stabilní a ověřené bezpečnostní aktualizace (patche)<sup>4</sup>.

## **8. OPRÁVNĚNÍ UŽÍVAT DATA**

- 8.1** Poskytovatel je při poskytování plnění pro Objednatele oprávněn užívat data předaná Poskytovateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
- 8.2** Poskytovatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB a Vyhláškou a dalšími souvisejícími právními předpisy.

## **9. VÝMĚNA INFORMACÍ**

- 9.1** Pokud je předmětem Smlouvy výměna informací mezi smluvními stranami, musí být zajištěna jejich ochrana, zejména při jejich výměně, uložení, archivaci a ukončení Smlouvy.
- 9.2** Poskytovatel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen z pohledu bezpečnostní klasifikace Objednavatele a tedy požadavků na důvěrnost, integritu a dostupnost dat a informací.

---

<sup>4</sup> Aktualizace software na vyšší vývojovou verzi.

- 9.3** Poskytovatel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

## **10. ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ**

- 10.1** Poskytovatel se při poskytování plnění pro objednatele zavazuje, že v případě kdy dojde k narušení bezpečnosti informací:

- 10.1.1 neprodleně nahlásí tuto skutečnost Kontaktní osobě objednatele uvedenou ve Smlouvě nebo
- 10.1.2 telefonicky oznámí na linku +420 220 111 155 a písemně na csoc@prg.aero
- 10.1.3 v případě vzniku bezpečnostní události a následného zvládnání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident, poskytne objednateli požadovanou součinnost (např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení zaměstnance poskytovatele nebo zaměstnance poddodavatele podílející se na realizaci plnění, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná objednatelem). Provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

## **11. ŘÍZENÍ KONTINUITY ČINNOSTÍ**

- 11.1** Objednatel má oprávnění zapojit Poskytovatele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Poskytovatele do plánu kontinuity činností, který souvisí s IS LP a souvisejících služeb a/nebo zahrnutí Poskytovatele do havarijního plánu Objednatele.
- 11.2** Objednatel má povinnost informovat Poskytovatele o způsobu zapojení dle předcházejícího odstavce
- 11.3** Poskytovatel předloží Objednateli metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována. Poskytovatel jako součást dodávky dále dodá a nasadí odpovídající technologické řešení, na kterém bude záloha a obnova dat prováděna.

## **12. LIKVIDACE DAT**

- 12.1** Pokud v rámci plnění předmětu Smlouvy má Dodavatel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pokyny Objednatele. V případě, že Objednatel nepožaduje specifickou likvidaci, je Dodavatel povinen při likvidaci postupovat v souladu s "best practice" (např. DIN 66399 atp.).

## Příloha č. 7 – Požadavky na akceptaci Analýzy

Zhotovitel provede v rámci realizace díla vstupní analýzu a vytvoření „*Implementačního plánu projektu*“ pro následnou realizaci díla, který bude popisovat minimálně tyto body:

- Základní popis řešení, technologií a technických konceptů.
- Obecné technické předpoklady a požadavky na realizaci řešení.
- Architektura řešení s jejím vysvětlením.
- Procesy a služby systému s jejich rozpisem a vysvětlením jejich účelu v rámci řešení.
- Popis systémů třetích stran a jejich integrace.
- Integrovaná architektura se systémy Letiště (SIEM, AD, SMTP, NTP atd.).
- Popis nakládání s daty, jejich uložení, zabezpečení, ochrana.
- Detailní síťový komunikační model řešení včetně interní komunikace mezi vnitřními prvky řešení.
- Technologické požadavky na zajištění provozu.
- Bezpečnostní zajištění řešení včetně souladu se ZKB.
- Soulad s GDPR.
- Monitoring řešení.
- Záloha a obnova dat včetně detailního popisu řešení DR scénářů.
- Návrh politik PAM řešení detailně specifikovaných během analýzy a vycházející z „best practice“ doporučení výrobce technologie.
- Návrh harmonogramu projektu a procesních kroků pro implementaci řešení včetně návrhu konfigurace řešení v jednotlivých fázích implementace a definice finální podoby dodávaného řešení.
- Detailní popis instalačních postupů.
- Postup testování a testovacích scénářů.
- Detailní popis a návrh na testování DR scénářů včetně totálního výpadku PAM.
- Metodika nakládání s break-glass účty.
- Akceptační kritéria včetně postupu akceptace.
- Popis náběhu systému.
- Návrh aktualizace a údržby řešení.
- Požadavky na součinnost.
- Detailní specifikace lokální podpory.
- Specifikace požadavků a rozsahu na školení zástupců Letiště.

Minimálně tyto body budou vyspecifikovány ve fázi detailní analýzy.