

KUPNÍ SMLOUVA

Smluvní strany:

ALEF NULA, a.s.

se sídlem Pernerova 691/42, 186 00 Praha

IČO: 61858579

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2727

bankovní spojení: Komerční banka

číslo účtu: x

zastoupená Ing. Milanem Zinkem, předsedou představenstva

kontakt pro smluvní účely: e-mail: x et: x (dále jen „**prodávající**“)

a

MERO ČR, a.s.

se sídlem Kralupy nad Vltavou, Veltruská 748, PSČ 278 01

IČO: 60193468

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2334

bankovní spojení: Komerční banka, a.s.

číslo účtu: x

zastoupená Ing. Jaroslavem Pantůčkem, předsedou představenstva a Ing. Marcelem Kalakajem, členem představenstva

kontakt pro smluvní účely: e-mail: x, tel.: x

(dále jen „**kupující**“)

uzavírají v souladu s ustanovením § 2079 a následujících zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**“) tuto kupní smlouvu (dále jen „**smlouva**“):

1. PŘEDMĚT SMLOUVY

1.1 Na základě této smlouvy se prodávající zavazuje dodat kupujícímu software pro řízení a správu privilegovaných účtů – tzv. „**Privileged Access Management**“ (dále jen „**SW**“ nebo „**PAM**“) spolu se všemi součástmi, příslušenstvím a souvisejícími činnostmi v souladu s přílohami č. 1 a č. 2 (dále jen „**předmět koupě**“ nebo „**systém**“) za podmínek stanovených v této smlouvě a za kupní cenu dohodnutou v čl. 2 této smlouvy. Kupující předmět koupě se všemi jeho součástmi a příslušenstvím kupuje a získává časově a místně neomezené právo užít SW za podmínek stanovených touto smlouvou.

Součástí dodávky předmětu koupě ve smyslu této smlouvy jsou (související činnosti):

- analýza stávajícího prostředí prodávajícího a návrh implementace součástí předmětu koupě
- dodávka časově neomezených licencí pro ostatní produkty třetích stran nezbytných pro provoz PAM
- dodávka licencí na databáze a operační systémy nutné pro provoz PAM včetně zajištění jejich podpory na dobu 4 let od předání a převzetí předmětu koupě
- dodávka hardware (nutné hw k provozování řešení pokud je nad rámec prostředí poskytované kupujícím)
- implementace PAM v rozsahu dle přílohy č. 2
- vytvoření Provozní dokumentace PAM
- zajištění komplexního školení v místě sídla kupujícího; termín školení bude určen kupujícím a bude prodávajícímu sdělen (postačuje forma e-mailu) nejpozději 14 dnů předem

Prodávající poskytuje kupujícímu časově a místně neomezené právo (perpetuální licence) užít SW, a to pro minimálně 100 aktiv nebo pro minimálně 150 privilegovaných účtů. Odměna za poskytnutí licence je součástí kupní ceny dle odst. 2.1.

- 1.2 Na základě této smlouvy se prodávající zavazuje poskytnout na svůj náklad a nebezpeční pro kupujícího služby spočívající v **Poskytování technologické podpory výrobce** (tzv. maintenance) předmětu koupě po dobu 4 let od předání a převzetí předmětu koupě (dále jen „služba“ nebo „služby“).

2. KUPNÍ CENA A PLATEBNÍ PODMÍNKY

- 2.1 Smluvní strany se dohodly, že kupní cena za předmět koupě dle čl. 1.1 této smlouvy činí **2.100.000,- Kč** (slovy dvěmilionystotisíc korun českých) plus případná DPH v zákonné výši (dále jen „**kupní cena**“). Kalkulace kupní ceny je uvedena v příloze č. 3 této smlouvy.
- 2.2 Cena za službu dle odst. 1.2 této smlouvy činí **960.000,-** (slovy devětsetšedesát tisíc korun českých) **Kč** bez DPH (dále jen „**cena za službu**“).
- 2.3 Kupní cena a cena za službu se stanovuje jako cena pevná a neměnná.
- 2.4 Kupní cenu uhradí kupující prodávajícímu na základě řádně vystavené a doručené faktury – daňového dokladu. Faktura – daňový doklad musí vždy splňovat náležitosti vyplývající z obecně závazných právních předpisů a náležitosti dle zák. č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění (dále jen „**zákon o DPH**“). Na faktuře – daňovém dokladu musí být uvedeno číslo smlouvy, objednávky a kontaktní osoba. Přílohou faktury bude kopie protokolu o předání a převzetí předmětu koupě.

Cena za službu bude prodávajícím fakturována jednou ročně, a to vždy v měsíci na který připadá výročí poskytování služby. Cena za službu za první rok poskytování služby bude vyfakturována spolu s kupní cenou.

- 2.5 Fakturu – daňový doklad doručí prodávající elektronicky na adresu fakturace@mero.cz, nejpozději pátý (5.) kalendářní den měsíce, který následuje po měsíci, ve kterém byl předmět koupě převzat kupujícím. Nebude-li prodávajícím předložena faktura – daňový doklad obsahovat náležitosti a údaje v souladu s touto smlouvou, bude prodávajícímu kupujícím vrácena do 10 kalendářních dnů po jejím obdržení jako doklad nesplňující předepsané náležitosti k doplnění či opravě. V tomto případě nemá prodávající nárok na zaplacení fakturované částky, úrok z prodlení ani jakoukoliv jinou sankci. Lhůta splatnosti počíná běžet znovu až ode dne doručení jím opravené nebo doplněné faktury – daňového dokladu.
- 2.6 Splatnost faktury – daňového dokladu činí 30 dnů od doručení kupujícím. Kupující uhradí kupní cenu/cenu za službu a DPH prodávajícímu – plátcem DPH pouze na účet, který je správcem daně zveřejněn způsobem umožňujícím dálkový přístup.
- 2.7 Kupující má právo proti kupní ceně/ceně za službu dle odst. 2.2 v souladu s ustanovením § 1982 a násl. občanského zákoníku započítat veškeré své splatné i neplatné pohledávky vůči prodávajícímu, zejména pohledávky z titulu smluvních pokut, které bude prodávající povinen kupujícímu podle této smlouvy uhradit.
- 2.8 Pokud bude DPH ze strany prodávajícího aplikovatelná, vyúčtuje prodávající tuto DPH při fakturaci kupní ceny/ceně za službu a zahrne ji do této faktury. DPH vyúčtovaná v souladu s tímto ustanovením smlouvy se stane součástí kupní ceny/ceny za službu. Pokud DPH nebude v souladu s předpisy upravujícími uplatnění DPH v České republice ze strany prodávajícího aplikovatelná, ke kupní ceně/ceně za službu nebude připočtena žádná DPH.
- 2.9 Pro účely správného uplatnění DPH prodávající prohlašuje, že k datu podpisu této smlouvy je registrovaným plátcem DPH v České republice. Prodávající se zavazuje kupujícímu písemně oznámit skutečnost, že jeho registrace k DPH v České republice byla zrušena, a to do 15 dnů ode dne, kdy tato skutečnost nastala.
- 2.10 Pro účely správného uplatnění DPH kupující prohlašuje, že k datu podpisu této smlouvy je registrovaným plátcem DPH v České republice. Kupující se zavazuje prodávajícímu písemně oznámit skutečnost, že jeho registrace k DPH v České republice byla zrušena, a to do 15 dnů ode dne, kdy tato skutečnost nastala.
- 2.11 Pro účely správného uplatnění DPH prodávající prohlašuje, že k datu podpisu této smlouvy je v souladu s předpisy upravujícími uplatnění DPH v České republice usazen v České republice. Prodávající se zavazuje kupujícímu písemně oznámit skutečnost, že v souladu s předpisy upravujícími uplatnění DPH v České republice přestal být považován za osobu usazenou v České republice, a to nejpozději do 15 dnů ode dne, kdy tato skutečnost nastala.

- 2.12 Prodávající se zavazuje vrátit bez zbytečného odkladu veškerou neoprávněně vyúčtovanou DPH, kterou kupující prodávajícímu uhradil. Dále se prodávající zavazuje uhradit kupujícímu škodu, která kupujícímu v důsledku nesprávně vyúčtované DPH prodávajícím vznikla.
- 2.13 V případě, že se prodávající stane nespolehlivým plátcem ve smyslu zákona o DPH, popř. obecně závazného právního předpisu nahrazujícího zákon o DPH, uhradí kupující DPH z přijatého zdanitelného plnění přímo příslušnému správci daně.
- 2.14 Kupující není povinen hradit jakékoliv finanční částky podle této smlouvy na jiný bankovní účet, než ten, který je zřízen bankou ve prospěch prodávajícího, a současně, který je správcem daně zveřejněn způsobem umožňujícím dálkový přístup, a současně, který není veden poskytovatelem platebních služeb mimo Českou republiku.

3. DODÁNÍ PŘEDMĚTU KOUPE

- 3.1 Prodávající je povinen dodat předmět koupě včetně uskutečnění souvisejících činností, vyjma zajištění školení, nejpozději do 30 dnů od účinnosti smlouvy. Místem dodání předmětu koupě je sídlo kupujícího. O dodání a převzetí předmětu koupě smluvní strany sepíší protokol.

4. ODPOVĚDNOST ZA VADY, PRÁVA Z VADNÉHO PLNĚNÍ, ZÁRUKA ZA JAKOST

- 4.1 Prodávající tímto poskytuje na předmět koupě záruku za jakost ve smyslu ustanovení § 2113 a násl. občanského zákoníku v trvání 12 měsíců od předání a převzetí předmětu koupě.
- 4.2 V případě, že budou kupujícím po převzetí předmětu koupě na tomto zjištěny vady, má kupující právo uplatnit vůči prodávajícímu nároky v souladu s ustanovením § 2099 a násl. občanského zákoníku. Prodávající je povinen zahájit odstraňování oznámené vady a vady odstranit bez zbytečného odkladu od oznámení, nejpozději však do 14 dnů od oznámení. Smluvní strany výslovně sjednávají, že kupující není povinen oznámit prodávajícímu vady předmětu koupě bez zbytečného odkladu poté, kdy je zjistil nebo při náležité pozornosti zjistit měl. Smluvní strany tímto výslovně vylučují aplikaci ustanovení § 2111 a § 2112 občanského zákoníku na právní vztah založený touto smlouvou.
- 4.3 Ve smyslu ustanovení § 2106 občanského zákoníku považují smluvní strany vadné plnění za podstatné porušení smlouvy s tím vyplývajícími důsledky.
- 4.4 Nesplní-li prodávající svůj závazek dodat předmět koupě kupujícímu řádně a včas, je kupující oprávněn vyúčtovat smluvní pokutu ve výši 3 000,- Kč za každý započatý den prodlení.
- 4.5 V případě prodlení prodávajícího s odstraněním reklamované vady je kupující oprávněn vyúčtovat prodávajícímu smluvní pokutu ve výši 2 000,- Kč za každý započatý den prodlení a každou vadu.
- 4.6 Další nároky kupujícího, zejména nároky na náhradu škody, nejsou ujednáním o smluvní pokutě a/nebo úroků z prodlení dotčeny. Ustanovení § 1971 a § 2050 občanského zákoníku se, je-li věřitelem kupující, nepoužijí.
- 4.7 Záruční doba se prodlužuje o dobu uplynulou od oznámení reklamované vady prodávajícímu do řádného odstranění vady.

5. DŮVĚRNOST INFORMACÍ

- 5.1 Smluvní strany se dohodly, že prodávající není oprávněn uveřejnit, či jakýmkoliv způsobem sdělit či zpřístupnit třetí osobě jakékoliv informace či skutečnosti, a to bez ohledu na formu, v jaké byly prodávajícímu předány či zpřístupněny, s nimiž přišel do styku v rámci plnění této smlouvy (dále jen „**Důvěrné informace**“) s výjimkou případů, kdy k takovému jednání či úkonu obdrží předchozí písemný pokyn či souhlas kupujícího. Důvěrné informace se mohou týkat zejména skutečností výrobní, obchodní, technické, ekonomické, organizační či jiné povahy a mohou zahrnovat obchodní tajemství.
- 5.2 Důvěrné informace je prodávající oprávněn použít pouze pro účely plnění této smlouvy.
- 5.3 Prodávající omezí počet zaměstnanců pro styk s Důvěrnými informacemi a se zaměstnanci, kteří přijdou s Důvěrnými informacemi do styku, uzavře obdobnou smlouvu o mlčenlivosti nebo tyto zaměstnanci podepíší jednostranný závazek mlčenlivosti ve vztahu k Důvěrným informacím.

- 5.4 Prodávající se zavazuje, že veškeré nosiče obsahující Důvěrné informace budou vráceny kupujícímu, a to do 7 dnů od výzvy kupujícího. Pokud jsou nosiče ve vlastnictví prodávajícího, budou tyto na výzvu kupujícího zničeny, resp. budou z nich nenávratně odstraněny veškeré Důvěrné informace a prodávající podepíše čestné prohlášení o zničení veškerých nosičů obsahujících Důvěrné informace/o nenávratném odstranění veškerých Důvěrných informací, a to vše do 7 dnů od výzvy kupujícího.
- 5.5 Povinnost mlčenlivosti dle této smlouvy se nevztahuje na informace:
- a) které prodávajícímu byly již dříve známy, aniž by přijal závazek důvěrnosti ke druhé smluvní straně,
 - b) které prodávající řádně získal od třetí osoby, která podle jeho vědomostí není vázána důvěrností ve vztahu k této informaci, nebo
 - c) které jsou, nebo se stanou veřejně dostupnými nikoli v důsledku porušení této smlouvy nebo právního předpisu,
 - d) pokud povinnost poskytnout Důvěrné informace vyplývá z právního předpisu a prodávající byl k jejich poskytnutí příslušným orgánem vyzván.
- 5.6 Povinnost uchovat v tajnosti Důvěrné informace trvá také po zániku této smlouvy.
- 5.7 V případě porušení závazku uvedeného v čl. 5 odst. 5.1 nebo odst. 5.2 této smlouvy je kupující oprávněn požadovat smluvní pokutu ve výši 1.000.000,- Kč za každý jednotlivý případ porušení.
- 5.8 Ujednáním o smluvní pokutě není dotčeno právo kupujícího na náhradu škody.
- 5.9 Splatnost smluvní pokuty se sjednává na dobu 15 dnů od doručení jejího vyúčtování.
- 5.10 Ujednání obsažená v tomto článku zůstávají v platnosti i v případě zániku/ukončení této smlouvy.

6. OSTATNÍ UJEDNÁNÍ

- 6.1 Prodávající se zavazuje dodržovat pravidla závazná pro dodavatele obsažená v etickém kodexu kupujícího. Prodávající podpisem této smlouvy stvrzuje, že se s etickým kodexem kupujícího, zejména s ustanoveními zavazujícími dodavatele a možnostmi dodavatele, jak oznámit případné neetické či protiprávní jednání zástupců kupujícího, řádně seznámil. Etický kodex je dostupný na webových stránkách <http://www.mero.cz/o-spolecnosti/eticky-kodex/>.
- 6.2 Prodávající na sebe tímto přebírá nebezpečí změny okolností ve smyslu ustanovení § 1765 odst. 2 občanského zákoníku.
- 6.3 Kupující upozorňuje prodávajícího, že je subjektem podléhajícím režimu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění, a prováděcím právním předpisům. V této souvislosti bere prodávající na vědomí, že je kupující povinen dostát povinnostem vyplývajícím z uvedených právních předpisů.
- 6.4 Prodávající je povinen neprodleně informovat kupujícího o bezpečnostních incidentech nebo jiných mimořádných událostech, které se staly v jeho informačních systémech a přímo souvisí se službami pro kupujícího dle této smlouvy, a které by mohly ve svém důsledku vést k narušení bezpečnosti informací kupujícího a/nebo k jejich ohrožení ochrany, a to následujícím způsobem:
- a) Primárním komunikačním kanálem pro nahlášení kybernetického bezpečnostního incidentu (KBI) je e-mail x
 - b) Předmět zprávy by měl obsahovat typ incidentu (např. DDoS, hacking, phishing, ransomware, atd.) pro snadnější třídění incidentů. Zpráva by měla obsahovat například části logů obsahující záznamy o útoku, časové známky včetně časové zóny, zdrojové a cílové IP adresy a porty. Nezbytnou součástí jsou i základní kontaktní informace, tedy jméno osoby, která KBI zasílá a jméno společnosti,
 - c) V případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, je **nutné** kontaktovat kupujícího na čísle +x.
- 6.5 Kupující má oprávnění k provedení kontroly opatření bezpečnosti informací, které jsou realizovány ze strany prodávajícího.
- 6.6 Každá smluvní strana má právo:

- a) vést, zpracovávat a auditovat kontrolní záznamy (logy) související s předmětem plnění této smlouvy,
 - b) vyžádat od druhé smluvní strany písemné vyhodnocení plnění určitých ustanovení nebo aspektů této smlouvy, nebo celkové vyhodnocení plnění této smlouvy, a to jedenkrát za tři po sobě následující měsíce.
- 6.7 Prodávající je povinen předat kupujícímu seznam osob (obsahující jméno, příjmení, e-mail a kontaktní telefonní číslo příslušné osoby) osob, kterým bude umožněn přístup do informačních systémů kupujícího, a to do 5 dnů od uzavření smlouvy. Tento seznam musí být opatřen souhlasem na něm uvedených osob se zpracováním osobních údajů ze strany společnosti MERO ČR, a.s. pro účely plnění této smlouvy. Prodávající je dále povinen neprodleně informovat kupujícího o změně osob, které mají přístup do informačních systémů kupujícího. Zároveň je prodávající povinen poskytnout součinnost při kontrole těchto přístupů, a to minimálně jednou za 6 měsíců.
- 6.8 Kupující tímto upozorňuje prodávajícího, že je ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění, osobou povinnou k uveřejnění smlouvy v registru smluv, resp. že je ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, jakožto veřejný zadavatel povinen ke zveřejnění uzavřené smlouvy včetně jejích změn a dodatků, výše skutečně uhrazené ceny za plnění veřejné zakázky a seznamu subdodavatelů dodavatele veřejné zakázky.
- 6.9 Smluvní strany jsou oprávněny odstoupit od této smlouvy v souladu s příslušnými ustanoveními občanského zákoníku.
- 6.10 Kupující je oprávněn odstoupit od této smlouvy zejména v těchto případech:
- a) prodlení prodávajícího s dodáním předmětu koupě o více než 15 dnů
 - b) prodlení prodávajícího s odstraněním reklamované vady o více než 15 dnů
 - c) opakovaný výskyt téže vady předmětu koupě

Kupující je rovněž oprávněn odstoupit od této smlouvy, budou-li se na prodávajícího vztahovat mezinárodní sankce podle právního předpisu účinného po uzavření této smlouvy.

7. ZÁVĚREČNÁ USTANOVENÍ

- 7.1 Tato smlouva byla uzavřena v souladu s českým právem a řídí se platnými právními předpisy České republiky.
- 7.2 V případě, že se jakékoli ustanovení stane zcela či z části neplatným, zdánlivým, neúčinným nebo nevymahatelným, ale bylo by platné, účinné a vymahatelné, kdyby byla jeho část vymazána, bude toto ustanovení nebo jeho část, považováno za vymazané v rozsahu, který je potřebný pro platnost, účinnost a vymahatelnost této smlouvy jako celku, při zachování co možná největšího původního ekonomického významu daného ustanovení. V takovém případě smluvní strany nahradí do patnácti dnů od výzvy kterékoliv ze smluvních stran takovéto neplatné, zdánlivé, neúčinné nebo nevymahatelné ustanovení ustanovením, které bude nejlépe splňovat smysl takového neplatného, zdánlivého, neúčinného nebo nevymahatelného ustanovení.
- 7.3 Smluvní strany tímto v souladu s ustanovení § 1895 odst. 1 občanského zákoníku vylučují možnost postoupení práv a povinností prodávajícího z této smlouvy nebo její části na třetí osobu bez předchozího písemného souhlasu kupujícího.
- 7.4 Prodávající není oprávněn bez předchozího písemného souhlasu kupujícího postoupit pohledávky vzniklé z této smlouvy anebo v souvislosti s ní na třetí osobu, ani není oprávněn tyto pohledávky bez předchozího písemného souhlasu kupujícího zastavit či je započítat.
- 7.5 Smluvní strany tímto v nejvýše povoleném rozsahu ustanovení § 1801 občanského zákoníku vylučují použití ustanovení § 1799 a § 1800 občanského zákoníku na tuto smlouvu a jejich vzájemné právní vztahy z této smlouvy vyplývající.
- 7.6 Změny a doplňky této smlouvy lze činit pouze písemně, vzestupně číslovanými dodatky podepsanými oběma smluvními stranami.

- 7.7 Jakékoli spory vzniklé z této smlouvy nebo v souvislosti s ní budou s konečnou platností rozhodovány příslušnými českými soudy.
- 7.8 Tato smlouva nabývá platnosti podpisem oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.
- 7.9 Smluvní strany se dohodly, že při výkladu ustanovení této smlouvy nebudou přihlížet k praxi mezi nimi zavedené, k obchodním zvyklostem, ani k jednání, která předcházela uzavření této smlouvy. Smluvní strany jsou vázány ve svých právech a povinnostech pouze obsahem této smlouvy.
- 7.10 Smluvní strany jako správci osobních údajů ve smyslu Obecného nařízení o zpracování osobních údajů (EU) 2016/679 („GDPR“) budou zpracovávat osobní údaje získané od druhé smluvní strany a jejich zástupců v rámci jednání o uzavření a plnění této smlouvy v souladu s pravidly stanovenými v GDPR. Předmětem zpracování osobních údajů jsou osobní údaje druhé smluvní strany, jejich zástupců, zaměstnanců, spolupracovníků nebo členů statutárních orgánů („Subjekty údajů“), a to zejména: (i) identifikační údaje (zejména jméno a příjmení, pozice) a (ii) kontaktní údaje (zejména e-mailová adresa a tel. spojení). Osobní údaje Subjektů údajů budou smluvní strany zpracovávat v rozsahu nezbytném pro plnění svých povinností dle této smlouvy, výkon svých práv, plnění zákonných povinností a související obchodní komunikace. V souvislosti se zpracováním osobních údajů Subjektů údajů smluvní strany prohlašují, že (i) budou zpracovávat osobní údaje v souladu s požadavky GDPR; (ii) umožní Subjektům údajů výkon jejich práv dle GDPR; a (iii) zajistí mlčenlivost osob zpracovávajících osobní údaje. Bližší informace o zpracování osobních údajů ze strany kupujícího jsou uvedeny na stránkách <https://mero.cz/o-spolecnosti/ochrana-osobnich-udaju/>.
- 7.11 Tato smlouva je vyhotovena v listinné podobě s vlastnoručními podpisy anebo v elektronické podobě s platnými zaručenými elektronickými podpisy založenými na kvalifikovaných certifikátech, kdy každá ze smluvních stran obdrží vyhotovení smlouvy s elektronickými podpisy. Je-li smlouva vyhotovena v listinné podobě, je sepsána ve dvou vyhotoveních, z nichž po jednom obdrží každá smluvní strana.
- 7.12 Přílohy této smlouvy tvoří její nedílnou součást.
- Příloha č. 1: Technická specifikace
Příloha č. 2: Rozsah implementace
Příloha č. 3: Cenová kalkulace
Příloha č. 4: Oprávněné osoby a kontaktní údaje
Příloha č. 5: Pojmy a zkratky

V případě rozporu mezi ustanoveními vlastní smlouvy (bez příloh) a ustanoveními obsaženými v příloze, mají přednost ustanovení obsažená ve smlouvě.

Obě smluvní strany shodně prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně, nikoliv v tísní a za nápadně nevýhodných podmínek.

V Praze dne

V Kralupech nad Vltavou dne

ALEF NULA, a.s.
Ing. Milan Zínek
předseda představenstva

MERO ČR, a.s.
Ing. Jaroslav Pantůček
předseda představenstva

MERO ČR, a.s.
Ing. Marcel Kalakaj
člen představenstva

Příloha č. 2 – Rozsah implementace

- Analýza stávajícího prostředí kupujícího a návrh implementace součástí předmětu koupě
- Instalace a konfigurace řešení v IT prostředí kupujícího včetně systémů, které kupující technologicky provozuje.
- Implementace vysoké dostupnosti řešení přes 2 lokality, v případě nedostupnosti řešení v primární lokalitě nahradí výpadek plnohodnotně záložní řešení, přepnutí proběhne automaticky v reálném čase;
- Implementace automatické správy hesel a SSH klíčů na jednotlivá aktiva
- Napojení na infrastrukturu kupujícího:
 - Integrace na systém logování;
 - Napojení na email bránu (SMTP);
 - Napojení na synchronizaci času (NTP); a
 - Doménové servery.
- Nastavení pravidelného zálohování řešení, umožnění obnovu řešení a virtuálních serverů ze záloh do 30ti minut;
- Nastavení skupin a oprávnění uživatelů a administrátorů PAM;
- Nastavení a přiřazení přístupových politik skupinám uživatelů;
- Nastavení politik hesel podle skupin zařízení;
- Automatizace vyhledávání zařízení a jejich automatické členění do skupin dle sítí a účelu zařízení;
- Automatizace vyhledávání účtů na serverech a v doméně a jejich automatické členění do skupin dle zařízení a účelu;
- Automatizované navázání administrátorských účtů z domény k administraci jednotlivých skupin zařízení;
- Automatizované navázání osobních administrátorských účtů z domény a ze zařízení běžným účtům administrátorů tak, aby každý administrátor používal jen svůj osobní privilegovaný účet a neviděl v žádném případě jiné osobní administrátorské účty;
- Přiřazení automaticky vytvářených skupin účtů skupinám uživatelů;
- Spuštění automatické rotace řízených účtů (přihlašovacích údajů); a
- Zajištění automatického reportování změny hesel a aktivit s účty.
- Nastavení reportingu o stavu koncových zařízení.

Software (počet licencí na koncové aktivum/administrátora)	Uživatelské licence pro správu a použití PAM systému uživateli/systémy kupujícího.	licence na aktivum/uživatele	Password Safe per Asset license - perpetualni licence na aktivum v počtu 100ks	PS-LIC	100	x	xKč
Software (počet serverových licencí)	Všechny licence appliance + licence nutné pro provoz systému v HA režimu.	serverové licence	BeyondTrust Appliance U Series-VM 2x virtuální appliance obsahující všechny licence nutné pro provoz nástroje	BT-APP-U-VM	2	x	x Kč
Ostatní licence nutné k provozu řešení	Všechny licence (jak výrobce technologie, tak třetích stran), které není možné zařadit do specializovaných licenčních položek. Prodávající doplní jednotlivé položky licence a rozepíše typ, počet a cenu.	ostatní licence	Provoz nabízeného řešení nevyžaduje další licence.	/	0	0	0 Kč
Hardware (nutné hw k provozování řešení pokud je nad rámec prostředí poskytované kupujícím)	Kompletní HW náklady nad rámec poskytované infrastruktury kupujícího, pro provoz bezpečného úložiště v HA režimu, HW pro zátěž vyplývající ze součtu zátěže. Prodávající uvede přesnou konfiguraci nabízeného HW.	ks	Poskytované prostředí je dostatečné pro nasazení a provoz nástroje dle specifikace ZD	/	0	0	0 Kč
Analýza*	Analýza prostředí, návrh prováděcí dokumentace dle "technické specifikace" a "Přívodní popis k technickému zadání".	člověkodenní (MD)	Analýza prostředí, systému Analýza privilegovanych účtů a oprávnění Návrh jmenových konvencí	/	7	x	x Kč
*Maximální cena za Analýzu byla stanovena částkou 300.000,- Kč bez DPH. Částka 300.000,- Kč bez DPH je nepřekročitelná. Nesplnění této podmínky je důvodem k vyloučení účastníka zadávacího řízení.							
Instalace hardware	Základní instalace a konfigurace hardware, OS a dalších prerekvizit PAM.	člověkodenní (MD)	/	/	4	x	xKč
Instalace software	Instalace softwarových částí PAM do prostředí kupujícího.	člověkodenní (MD)	/	/	10	x	x Kč
Implementace a integrace do stávajícího prostředí	Nápojení na všechny požadované platformy a integrace a dalšími klíčovými prvky infrastruktury dle "Technické specifikace" a "Rozsah implementace".	člověkodenní (MD)	/	/	8	x	xKč
Zkušební provoz	Ověření provozu včetně napojení na klíčové infrastrukturní prvky.	člověkodenní (MD)	/	/	3	x	x Kč
Dokumentace	Dokumentace skutečného stavu a nasazení PAM.	člověkodenní (MD)	/	/	3	x	x Kč
Akceptační testy	Provedení akceptačních testů dle specifikace určené v analýze.	člověkodenní (MD)	/	/	3	x	xKč
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 3 zaměstnanci kupujícího.	člověkodenní (MD)	/	/	2	x	xKč
Bod 1.2 Předmětu smlouvy - Maintenance							
Maintenance a servisní podpora 24x7	Maintenance a 24 x 7 support formou e-mailu a telefonické hotline v českém nebo anglickém jazyce, s garantovanou dobou odezvy a zahájením řešení problému.	měsíc	/	/	48	x	xKč

Příloha č. 4 – Oprávněné osoby a kontaktní údaje

Seznam oprávněných osob strany kupující

Jméno	Telefon	e-mail	Pověření ve výše uvedeném rozsahu
Bc. Petr Stádník			Ve věcech smluvních a technických, ve věcech kybernetické bezpečnosti, hlášení závad a reklamací, akceptace měsíčních zpráv o realizaci služby
Václav Urbánek			Ve věcech smluvních a technických, hlášení závad a reklamací, akceptace měsíčních zpráv o realizaci služby
Ing. David Plecháč			Ve věcech technických, hlášení závad a reklamací, akceptace měsíčních zpráv o realizaci služby
Alexander Tóth			Ve věcech technických, hlášení závad a reklamací
Martin Dekastello			Ve věcech technických, hlášení závad a reklamací

Seznam oprávněných osob strany prodávající

Jméno	Telefon	e-mail	Pověření ve výše uvedeném rozsahu
Radek Švadlenka			Ve věcech obchodních a smluvních
Petra Sedláčková			Ve věcech technických, hlášení závad a reklamací, akceptace měsíčních zpráv o realizaci služby
David Horák			Ve věcech technických, Implementačních a konzultačních
Martin Hubínek			Ve věcech technických, Implementačních a konzultačních

Příloha č. 5 – Pojmy a zkratky

Pojem / zkratka	Význam
Access management/control	Kontrola přístupů privilegovaných účtů na úrovni členitějšího řízení autorizace, vyšší a sofistikovanější forma detekce a ochrany na základě definovaných politik
Active - Passive režim	Princip/metoda realizace vysoké dostupnosti prostřednictvím dvou aktivně pracujících zařízení/appliance. Architektura takového IT řešení nebo IT komponenty je natolik redundantně nebo jinak zabezpečena, že v případě neplánovaného výpadku funkčnosti některé ze SW funkcionalit nebo infrastrukturní části není žádným způsobem negativně ovlivněn provoz navrhovaného řešení PAM.
Active/Standby	Aktivní/pohotovostní provozování dostupnosti 2 pracujících serverů/zařízení
Administrátor aplikace/systému, nebo také správce aplikace/systému	Uživatel přistupující do SW prostředí navrhovaného řešení PAM s autorizací umožňující administraci nebo správu aplikace/systému.
Adresářový server	Serverová instance SW aplikace umožňující správu datových informací ve stromové struktuře odpovídající protokolu LDAP
Akceptační test	Test pro akceptaci díla nebo dílčí části
API	Application Programming Interface – rozhraní pro programování aplikací.
Aplikace, nebo také IT systém, nebo také systém	Soubor funkčních a nefunkčních parametrů tvořících dohromady fungující SW celek provozovaný v IT prostředí k naplnění funkčních a nefunkčních požadavků uživatele.
Appliance/HW Appliance	HW / SW zařízení se specifickou funkcí a omezenou možností konfigurace připravenou výrobcem dodávaného řešení, existující v produktové řadě s produktovým číslem.
AS	Aplikační server.
ASCII	Kódová tabulka, která definuje znaky anglické abecedy a jiné znaky používané v informatice
Asynchronní komunikace	Nesoučasná komunikace - mezi předáním a převzetím zprávy je časová prodleva, např. e-mail.
Auditní log	Chronologický záznam všech aktivit v systému. Auditní logy zpravidla obsahují minimálně následující údaje: kdy, kdo změnu provedl, změněný atribut, starou hodnotu, novou hodnotu.
Auditor IKB	Uživatel (zpravidla z oddělení IKB), který má přístup k auditním informacím a nahrávkám v navrhovaném řešení PAM.
Autentizace	Proces ověření proklamované identity subjektu. Autentizace je bezpečnostním opatřením k zajištění ochrany před falšováním identity, kdy se subjekt vydává za někoho, kým není. Rozlišujeme autentizaci entity (osoby, programu) a autentizaci emailové zprávy. Po dokončení autentizace obvykle následuje autorizace.
Autorizace	Proces získávání souhlasu s provedením nějaké operace, povolení přístupu, někomu nebo něčemu (nejen ve smyslu přístupu do konkrétních prostor nebo k nějaké osobě, ale také přístup k informačním systémům, funkcím, programovým objektům a podobně)
Autorizační koncept	Popis principu/způsobu přidělování uživatelských oprávnění do systémů ICT/ICS.
Bezpečnostní incident	(dále též incident) jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace procesů/činností zadavatele a ohrožení bezpečnosti informací.
Bezpečnostní opatření	Proces, procedura nebo technický prostředek navržený za účelem zmírnění působení nebo eliminaci hrozby; snížení míry nebo odstranění zranitelnosti; nebo dopadu hrozby. Slouží pro účely

	prevence, snížení nebo eliminace informačních rizik tak, aby míra rizika odpovídala schopnosti zadavatele riziko akceptovat a tolerovat.
Bezpečnostní událost	(dále též událost) možné porušení bezpečnostní politiky nebo na selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá. Může být příčinou nebo mít vliv na vznik bezpečnostního incidentu.
Běžný uživatel	Uživatel přistupující do SW prostředí navrhovaného řešení PAM s autorizací umožňující pouze čtení informací, nebo čtení informací společně s vykazováním.
Business Impact Analysis (BIA)	Hodnocení prováděné na manažerské úrovni ve vztahu k informačnímu aktivu využívanému pro podporu příslušného business procesu, oblasti řízení, logickému, technologickému nebo technickému celku z pohledu dostupnosti, důvěrnosti a integrity. Prostřednictvím BIA garant aktiv (zadavatele) kvantitativně (např. finanční ztráta, úroveň poskytovaných služeb) a kvalitativně (např. provozní, renomé, právní, regulační) zhodnotí největší újmu (ztrátu), která může nastat v důsledku možné realizace hrozeb (bezpečnostní události/incidentu). Na základě výstupů z BIA jsou stanoveny minimální zdroje potřebné pro obnovení kritických činností po závažném incidentu a jsou vytvářeny strategie a plány zajištění kontinuity činností podnikatele.
CAPTCHA	Turingův test, který se na webu používá ve snaze automaticky odlišit skutečné uživatele od robotů. CAPTCHA je akronym pro „completely automated public Turing test to tell computers and humans apart“, tedy „plně automatický veřejný Turingův test k odlišení počítačů a lidí“.
CD	Kompaktní disk
CISA	Certified Information Systems Auditor
CISA	Certified Information Systems Security Professional
CISM	Certified Information Security Manager
Citlivé programové vybavení	Programové vybavení, jež obsahuje chráněná data společnosti. Jejich vyzrazením, zneužitím, neautorizovanou změnou nebo nedostupností by vznikla organizaci škoda, případně by organizace nemohla řádně plnit svoje poslání.
CK	Cílový koncept.
CLI	CLI – command line interface
CRUD	Zkratka vyjádření akcí prováděných uživatelem nad datovými objekty v IT prostředí s využitím aplikačních funkcionalit. (C)reate – založení, (R)ead – čtení, (U)pdate – změna, (D)elete – výmaz.
CSV	Comma-separated values, neboli hodnoty oddělené čárkami, je jednoduchý souborový formát určený pro výměnu tabulkových dat. Soubor ve formátu CSV se sestává z řádků, ve kterých jsou jednotlivé položky odděleny znakem čárka.
Customizace	Úprava aplikace (SW prostředí navrhovaného řešení PAM) podle požadavku zákazníka = objednatele. Vývoj na zakázku - zákaznický vývoj v řešení pouze pro potřeby objednatele.
DB	Databáze.
DBS	Databázový server.
DCOM (RPC)	Microsoft technologie pro komunikaci mezi komponenty software a počítači přes síť
Deployment	Nasazení aplikace do prostředí (ať už produkčního, tak i testovacího) s možností zpětných úprav bez vyšších nákladů.
Disponibilní kapacita	Časová dostupnost zdroje nebo role pro práci na projektech, poměr z plánované dostupnosti zaměstnance.
DR	Disaster Recovery.

Dvoufaktorová autentizace	Proces ověření identifikačních a autentizačních údajů subjektu. Je to kombinace dvou ze tří faktorů možné autentizace – subjekt něco „ví“ (např. heslo), něco „má“ (např. mobilní telefon s příchozí sms) a něco „je“ (např. otisk prstu).
DWH/BI nástroj	Data Warehouse a Business Intelligence – SW řešení datového skladu pro analytický a statistický reporting dat. Řešení využívá ETL datové pumpy a zpravidla je využíváno OLAP ukládání dat nebo kombinace s OLTP.
ERP	Enterprise Resources Planning.
ETL	ETL je zkratka pro Extract-Transform-Load, tři databázové funkce, které jsou sloučeny do jednoho nástroje, který vytáhne údaje z jedné databáze a umístí je do jiné databáze. - Extract je proces čtení dat z databáze. - Transform je proces konverze získaných dat z jejich původní podoby do podoby, ve které musí být, aby se mohly umístit do jiné databáze. - Load je proces zápisu dat do cílové databáze.
Event log	Záznam události (často i s časovým razítkem), která nastala v systému ICT/ICS.
Export, Export dat, Export souboru, Export reportu	Export vybraných dat z navrhovaného řešení PAM do jiného SW řešení, na sdílený datový prostor nebo do lokálního datového úložiště.
Failover DB	Označení pro pojištění v případě výpadku, kdy dochází k přepnutí na redundantní DB server (či obecně redundantní komponenta DB).
FIPS	Federal Information Processing Standards (Federální standardy zpracování informací)
FW	Firewall
Fyzická ochrana	Systém technických a organizačních opatření zabraňujících neoprávněným činnostem s majetkem (neoprávněné užívání, poškození, zničení nebo zcizení hmotného a nehmotného majetku), nebo která mají za cíl zajistit bezpečnost osob.
GDPR	General Data Protection Regulation.
GIT	Systém pro správu a verzování zdrojových programů.
Go Live	Termín předání řešení do produktivního provozu. V IT terminologii může řešení nabývat významu SW nebo HW komponenty/prostředí/aplikace/systému/ucelené funkcionality.
HA	High Availability.
HADR	High Availability and Disaster Recovery
Hardening	Hardening systémů a platform je základním bezpečnostním opatřením, kterým se lze účinně bránit před zneužitím informačních systémů nebo aplikací.
Hardeningová politika (systémová bezpečnostní politika)	Dokumenty popisují požadavky na nastavení systémů ICT/ICS za účelem snížení rizik spojených s jejich provozováním. Zahrnuje požadavky na odstranění zbytečného software, zablokování nepotřebných funkcionalit a služeb, povinný obsah konfiguračních souborů aj.
Hrozba	Příčina (osoba nebo událost), která může svým působením poškodit aktiva zadavatele. Hrozba zneužívá zranitelnosti aktiva.
HSM/HSM modul/HSM box	Datové úložiště pro bezpečné uchování šifrovacích klíčů, elektronických podpisů a certifikátů
HTTP	Internetový protokol, původně určený k výměně hypertextových dokumentů mezi serverem a prohlížečem (tzv. služba WWW). Současná verze HTTP však již dokáže přenášet jakékoliv soubory a používá se i k mnoha jiným funkcím (např. spouštění vzdálených aplikací).
HW	Hardware.
Check-in hesla	Změna hesla a odznačení účtu od statusu "používaný uživatelem"

Check-out hesla	Změna hesla a následné poskytnutí hesla uživateli spolu s označením účtu jako používaného daným uživatelem
ICS	Industrial Control System (průmyslový řídicí systém). Systém pro řízení technologických celků (například: SCADA, PLC řadiče atd.).
ICT	Informační a komunikační technologie, zkráceně ICT (z anglického Information and Communication Technologies).
ID	Identifikační číslo
Identita	Virtuální entita, která reprezentuje atributy, role a účty fyzického uživatele (osoby) v koncových systémech.
IKB	Informační Kybernetická Bezpečnost
IMEI	International Mobile Equipment Identity - nikátní 15 místné číslo přidělené každému mobilnímu zařízení
Import, Import dat, Import souboru	Import vybraných dat do navrhovaného řešení PAM z jiného SW řešení, ze sdílený datového prostoru nebo z lokálního datového úložiště.
Informační a kybernetická bezpečnost	Systém právních, technických, administrativních, organizačních a režimových prostředků zajišťujících ochranu důvěrnosti, integritu a dostupnost informačních aktiv a systém opatření, jehož předmětem je ochrana informačního aktiva v elektronické podobě a systému ICT/ICS, který ho zpracovává – v majetku nebo užívání společnost,
Informační aktiva	Data, informace, znalosti, aplikace, systém nebo služba, která má hodnotu pro společnost, podporuje procesy společnosti. Vše, co se snažíme chránit proti existujícím rizikům, včetně Primárních aktiv
IP adresa	je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti,
ISKII	Informační systém kritické informační infrastruktury
ISO	International Organization for Standardization (mezinárodní organizace pro normalizaci)
ISZS	Informační systém základní služby
IT	Informační technologie
JAVA	Objektově orientovaný programovací jazyk
JDBC	Java Database Connectivity - aplikační programové rozhraní (API) pro programovací jazyk Java, které definuje, jak může klient přistupovat k databázi.
JOB	Plánovaná jednoduchá nebo dávková úloha zahrnující jednu nebo několik aplikačních funkcionalit spouštěných mimo aplikační dialogový proces (většinou v aplikačním pozadí).
KDI	Kategorie dat a informací
Klíčová událost (pro logování)	Událost, která je odpovědnou osobou definována jako důležitá pro potřeby logování.
Koncové zařízení	Pracovní stanice typu osobní počítač nebo notebook
Koncový systém nebo IT zařízení	Ve smyslu projektové dokumentace se jedná o IT systém/SW aplikaci/IT zařízení, které je integrováno na navrhované řešení PAM. Privilegované účty nebo hesla integrovaného IT systému/SW aplikace/IT zařízení jsou spravované v rámci navrhovaného řešení PAM.
KPJM	Korporátní přihlašovací jméno uživatele (tento přihlašovací účet je logickou reprezentací identity uživatele v IS).
Kritické systémy	Systémy ICT/ICS a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost společnosti.
KZ/KS	Koncové zařízení typu PC nebo NB
LDAP	Lightweight Directory Access Protocol je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře).

Load Balancing	Rozdělení pracovní zátěže v infrastrukturním IT prostředí na více fyzických nebo virtuálních HW zdrojů. Zejména se jedná o aplikační servery, databázové servery, síťovou infrastrukturu a diskové (a) úložiště. Na úrovni infrastrukturní architektury dochází využitím load balancingu k optimalizaci infrastrukturních zdrojů.
MAC adresa	„Media Access Control“ - je jednoznačný identifikátor síťového zařízení
Master	V souvislosti s IT se jedná o autoritativní zdroj dat, zdrojových kódů, knihoven nebo postupů pro vybudování aplikace.
MFA	Multi-factor authentication
MKZ	Mobilní koncové zařízení typu mobilní telefon nebo tablet
Monitoring	(fault/performance/provozní) – proces dohledu nad funkcí systému ICT/ICS s cílem identifikovat změny nebo odchylky od požadovaných hodnot.
MS	Microsoft
MS AD	SW produkt Microsoft Active Directory.
MS Excel	SW řešení od výrobce Microsoft.
MS Exchange	SW řešení od výrobce Microsoft.
MS Office	Sada kancelářských SW řešení od výrobce Microsoft obsahující SW nástroj MS Word, MS Excel, MS PowerPoint, MS OneNote, MS Project, MS Outlook a MS Publisher.
MTDL	Určuje nepřekročitelný interval ztráty dat. Definiuje, jak rozsáhlou historii dat je možné v případě incidentu „obětovat“, tzn., za jak dlouhé období bude nutné data znovu pořízovat, aby pro organizaci nenastaly neakceptovatelné dopady. Jde o hranici netolerovatelných dopadů.(Maximum Tolerable Data Loss)
MTPD	Nejdelší časový úsek, ve kterém musí být obnovena dostupnost funkcí informačního systému (dat) tak, aby nedošlo k neakceptovatelným dopadům pro organizaci. Jde o hranici netolerovatelných dopadů. Vztahuje se na všechny typy závad včetně komplexní obnovy systému (tzv. Disaster Recovery).(Maximum Tolerable Period of Disruption)
Multi-tenant	Logické oddělení dat v SW řešení s pomocí funkcionalit databázové nebo aplikační vrstvy.
Nativní report	Nativní report je prezentovaný ve formě obrazovky, který je zabudován přímo v dodaném SW prostředí navrhovaného řešení PAM a v tomto prostředí zobrazuje data o objektech.
NDA	Non-Disclosure Agreement (dohoda o mlčenlivosti, dohoda o důvěrnosti). Dohoda, která je uzavírána mezi zadavatelem a externím subjektem, kdykoli se předpokládá sdělování interních informací zadavatele externímu subjektu. NDA stanovuje podmínky ochrany předávaných nebo získaných informací a je uzavírána ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník.
Neautorizovaný přístup / úprava	Pokus o přístup nebo provedení úprav bez potřebných oprávnění.
Notifikace	Upozornění zaslané automaticky nebo manuálně pomocí funkcionality navrhovaného řešení PAM. Zasilání notifikací probíhá převážně pomocí emailové komunikace.
OLAP	Online Analytical Processing je technologie uložení dat v databázi, která umožňuje uspořádat velké objemy dat tak, aby byla data přístupná a srozumitelná uživatelům zabývajícím se analýzou obchodních trendů a výsledků (Business Intelligence).
OLTP	Online Transaction Processing je technologie uložení dat v databázi, která umožňuje jejich co nejsnadnější a nejbezpečnější modifikaci v mnohauživatelském prostředí.
on-line režim/on-line	Aktivita nebo činnost probíhající v reálném čase/právě teď
on-premise	On-premises software je takový software, který lze instalovat a provozovat v prostorách zákazníka.

Organizační jednotka	Organizační jednotka (nebo též Organizační útvar, Organizational Unit) je po pracovním místě druhým základním stavebním prvkem formální organizační struktury. Využívá se v rámci organizace nebo logické datové struktury organizačního managementu (organizační struktury) sloužící pro členění, správu a evidenci zaměstnanců v rámci společnosti.
Organizační struktura	Organizační struktura je oficiálně kodifikované hierarchické uspořádání vztahů mezi jednotlivými pracovními místy v rámci organizačních útvarů a vztahů mezi útvary v rámci organizace. Zahrnuje vztahy nadřízenosti a podřízenosti a řeší vzájemné pravomoci (kompetence), vazby a odpovědnost.
OS	Operační systém
OSI	Open Systems Interconnection
Osobní údaje	Veškeré informace o identifikované nebo identifikovatelné fyzické osobě (například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby).
Out-of-the-box	Pojem, který se používá pro označení vlastnosti nebo funkce softwaru, jež jsou součástí instalace SW, pracují bezprostředně po instalaci bez nutnosti jakékoli konfigurace nebo úpravy a jsou k dispozici ve výchozím nastavení SW.
OVIS sondy HP BSM	HP BSM je SW nástroj pro sledování End-to-End procesů, přístupu a výkonu aplikační vrstvy s využitím syntetického nebo reálného uživatele. BAC nebo OVIS sonda umožňuje uskladnění a spuštění programového skriptu volajícího spuštění aplikace nebo systému, popřípadě některou z aplikačních funkcionalit.
PAM	Privileged Access Management
Passphrase	Sekvence znaků či slov sloužící k ověření přístupu do systému ICT/ICS. Je obvykle delší a komplexnější než běžné heslo.
Password management	Centrální správa privilegovaných účtů se zabezpečeným úložištěm hesel, klíčů a správou přístupů k těmto účtům
PDF	Zkratka anglického názvu Portable Document Format – Přenosný formát dokumentů - je souborový formát vyvinutý firmou Adobe pro ukládání dokumentů nezávisle na softwaru i hardwaru, na kterém byly pořízen
PIM	Privileged Identity Management
PKI	Public Key Infrastructure (infrastruktura veřejných klíčů)
PM	Projektový manažer.
POST	POST je v informatice jedna z dotazovacích metod HTTP protokolu, kterou webový prohlížeč (klient) získá webovou stránku (nebo jiný objekt – například obrázek) z webového serveru a zároveň umožňuje předat serveru metaproměnné z webového formuláře na webový server, kde mohou být zpracovány (například PHP skriptem). Alternativní metodou je GET.
PPT	Formát souboru typu MS Power Point. Účelem využití souboru typu PPT je většinou forma prezentace.
Princip nezbytného minima	Principle of Least Privilege) – princip při přidělování přístupových oprávnění – přidělit subjektu co nejnižší možná privilegia, která budou umožňovat správnou funkci pro daný subjekt.
Privilegovaný účet	Uživatelský účet IT systému/aplikace s množinou autorizačních oprávnění vyšších, než běžný uživatel, nebo administrátorských oprávnění, který může být nepersonalizovaný a sdílený mezi vícero uživateli. Jedná se o privilegované účty typu root, Administrator, Enable, system/sys, účty třídy KPJM typu QS, účty třídy KPJM typu QR, účty třídy KPJM typu QP s vysokým oprávněním a další by default privilegované účty zabudované do systému/aplikace ze strany výrobce.

Produkční prostředí	prostředí systému ICT/ICS, kde jsou provozovány aplikace a poskytovány služby, se kterými mají pracovat koncoví uživatelé a zákazníci. Jedná se o prostředí odlišné od testovacího a vývojového.
PUM	Privileged User management
RDP/Windows RDP	Remote Desktop Protocol - síťový protokol pro ovládání vzdáleného počítače pomocí sítě. Pracuje na principu klient -server
Rebranding	V terminologii IT umožňuje systém nebo aplikaci vizuálně přizpůsobit požadavkům zákazníka. Jedná se zejména o změnu barevného schématu, loga, rozsahu využitých znakových sad a fontů, vložení bannerů, produktového názvu aplikace apod.
Relační databáze	Databáze složená z datových tabulek vázaných pomocí relačních vazeb (klíčů). Mezinárodní zkratka je OLTP databáze.
Report	Funkčnost, pomocí které lze vyhledat data evidovaná v aplikaci na základě uživatelem zadaného výběrového kritéria a zobrazit do předem definovaného layoutu. V reportu je možné data získat kombinací z více objektů (data entit, úkolů, rizik, kapacity zdrojů, apod.).
REST	Representational State Transfer - alternativa k protokolu SOAP. Slouží k popisu architektury. Komunikuje pomocí protokolu HTTP. Zahrnuje čtení a design web stránek obsahujících XML soubory.
Retenční doba anonymizace osobních údajů identity uživatele	jedná se o správcem osobních údajů definovanou dobu, po které pomine oprávněný účel zpracování těchto údajů a tyto musí být anonymizovány.
RPA/RPA robot	Robotic process automation - forma technologie automatizace podnikových procesů založená na pracovníků metaforických softwarových robotů (robotů) nebo umělých inteligencí (AI)
RPO	Akceptovatelná ztráta dat po havárii systému definovaná časem (Recovery Point Objectives). Technický parametr provozu aplikace/systému. Udává maximální reálně možnou ztrátu dat, je v zásadě frekvencí zálohování dat, resp. frekvencí zálohování transakčních logů. Platí zásada $RPO \leq MTDL$.
RTO	Doba nutná k obnově dat po havárii systému (Recovery Time Objectives). Technický parametr provozu aplikace/systému. Udává skutečný čas, za jaký jsme schopni obnovit hlavní funkce aplikace/systému v případě havárie. Platí zásada $RTO \leq MTPD$.
Řešitel	Uživatel přistupující do SW prostředí navrhovaného řešení PAM s autorizací umožňující datové operace typu CRUD.
SEČ	Středoevropský čas
Session	Session (v překladu relace, méně častěji sezení nebo seance) v informatice představuje permanentní síťové spojení mezi klientem a serverem, zahrnující výměnu paketů.
Session recording	Zaznamenávání aktivit privilegovaných účtů včetně nahrávek obrazovek a stisků kláves (key-logging)
SIEM	(Security Information and Event Management) je management bezpečnostních informací a událostí. Současně řeší dříve různorodé kategorie: SIM (Security Information Management) - zabývá se dlouhodobým ukládáním událostí, jejich analýzou a hlášením problémů.
Síťová infrastruktura	Souhrn hardwaru, softwaru a síťových služeb celé sítě, který umožňuje komunikaci, připojení k jiným sítím, provoz a řízení sítě.
SLA	Service Level Agreement - smlouva sjednaná mezi poskytovatelem služby a jejím uživatelem
SMTP protokol	Simple Mail Transfer Protocol. Komunikační protokol pro zasílání elektronické e-mailové komunikace.
SMTP server	Poštovní server je prostředkem komunikace s okolním světem. Poštovní servery jsou zároveň vstupní branou pro data, která přicházejí do IT sítě.

SNMP protokol	Simple Network Management Protocol (SNMP) je součástí sady internetových protokolů. Standardně využívá port 161. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování.
SOAP	Simple Object Access Protocol - protokol pro výměnu strukturovaných informací v rámci webových služeb v IT síti. Využívá XML pro formát zpráv a běží na aplikační vrstvě HTTP nebo SMTP.
SoD	Segregation of Duties (oddělení odpovědnosti)
SQL Injection	SQL injection je technika napadení databázové vrstvy programu vsunutím (odtud „injection“) kódu přes neošetřený vstup a vykonání vlastního pozměňujícího poškozujícího SQL příkazu (dotazu DELETE, UPDATE, ALTER atp.).
SRM	Supplier Relationship Management.
SSH	Secure Shell, program a zároveň zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet
SSL	Kryptografický protokol (Secure Sockets Layer) používaný pro zabezpečenou komunikaci v prostředí internetu - předchůdce TLS.
SSL certifikát	Prostředek potřebný k sestavení bezpečného spojení (obvykle mezi klientem a serverem).
SSO	Single Sign On – systém jednotného přihlášení.
Strategie obnovy	plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.
SW	Software.
Switch	Sítový aktivní prvek pro směrování provozu
Synchronní komunikace	Komunikace v reálném čase - komunikace při předávání zpráv, kdy předání a převzetí zprávy probíhá v reálném čase - není žádná časová prodleva.
Syslog server	Prostředek pro shromažďování logů, které vznikají v systémech ICT/ICS.
Systém PIM/PAM/PUM, nebo také řešení PAM, nebo také Navrhované řešení PAM, nebo také Informační systém PAM	Vysoce zabezpečené, centralizované a konfigurovatelné SW řešení PIM/PAM/PUM pro řízení životního cyklu, správy a monitoring privilegovaných účtů včetně efektivní a bezpečné správy hesel, PKI a SSH klíčů a oprávnění pro personifikované i nepersonifikované privilegované účty v prostředí OS, síťových prvků, databází, aplikačních serverů, virtuálních serverů, kontejnerů, infrastrukturních a bezpečnostních prvků, LDAPů, uživatelských KZ, aplikací a aplikačních skriptů umístěných v IT prostředí typu on-premise, nebo v prostředí hybridním, nebo i v prostředí cloudovém. Navrhované řešení PAM obsahuje funkcionality: <ul style="list-style-type: none"> - centrální správa privilegovaných účtů se zabezpečeným úložištěm hesel, klíčů a správou přístupů k těmto účtům - zaznamenávání aktivit privilegovaných účtů včetně nahrávek obrazovek a stisků kláves (key-logging) - kontrola přístupů privilegovaných účtů, včetně členitějšího řízení autorizace, vyšší a sofistikovanější forma detekce, ochrana na základě definovaných politik)
Tenký klient	Tenký klient (překlad anglického thin client) je počítač nebo počítačový program, který při plnění svého úkolu silně závisí na jiném počítači (na svém serveru).
Tiering model/Tier Administrative Model	Active Directory Administrative Tier Model od společnosti Microsoft. Tier0 (nejvyšší úroveň a zahrnuje administrativní účty a skupiny, řadiče domény a domény, které mají přímou nebo

	nepřímou administrativní kontrolu doménové struktury AD), Tier1 (pro servery a aplikace členských domén)a Tier2 (koncové uživatelské zařízení)
TLS	Transport Layer Security - nástupce SSL. Kryptografický protokol využívaný pro zabezpečenou komunikaci v prostředí internetu. Umožňuje výměnu PKI.
Tlustý klient/Tlustá klientská aplikace/TK	Tlustý klient je počítač, který nepotřebuje další přístroj pro vykonávání předem stanovených úloh, příkazy zpracovává sám.
Transakční data	Data vytvořená a uložená v rámci transakčního zpracování ze strany uživatele nebo automatické aplikační funkcionality.
Trezor hesel/Repository (trezor/úložiště)/Úložiště hesel	Úložiště privilegovaných účtů s hesly a klíči, které je šifrováno a dostatečně chráněno před všemi hrozbami, které by jej mohly kompromitovat nebo poškodit
Třída KPJM typu QP	Programový uživatel. KPJM třídy QP je nepersonifikovaný privilegovaný účet.
Třída KPJM typu QR	Správce - externí uživatel s oprávněním vyšším než běžný uživatel. KPJM třídy QR je personifikovaný privilegovaný účet.
Třída KPJM typu QS	Správce - interní uživatel s oprávněním vyšším než běžný uživatel. KPJM třídy QS je personifikovaný privilegovaný účet.
UI	User Interface - uživatelské rozhraní.
UNICODE	Technická norma pro oblast výpočetní techniky definující konzistentní kódování pro reprezentaci a zpracovávání textů použitelné pro většinu písem používaných v současnosti na Zemi. Unicode je vyvíjen v součinnosti s ISO/IEC 10646 a je publikován elektronicky jako The Unicode Standard.
URL	URL (Uniform Resource Locator) je soubor znaků, který slouží k identifikaci přesného umístění informací na internetu. URL definuje doménovou adresu serveru, umístění zdroje na server a protokol.
UTF-8	Zkratka pro UCS/Unicode Transformation Format. Je to způsob kódování řetězců znaků Unicode/ISO/IEC 10646 do sekvencí bajtů.
Uživatel	Fyzická osoba v podobě zaměstnance zadavatele, externího dodavatele, subdodavatele nebo smluvního partnera, která má úmysl používat informační nebo technologický systém zadavatele nebo vstupovat do chráněných prostor zadavatele.
VPN	Virtual Private Network (virtuální privátní síť)
W3C.ORG	World Wide Web Consortium.
WAN	Wide Area Network. Rozsáhlá internetová síť, která je zpravidla směřována mimo lokální perimetr. V porovnání s LAN se jedná o obdobné srovnávání, jako internet a intranet.
WF / workflow	Posloupnost kroků, mezi kterými se definovným způsobem posouvají data nebo dokumenty. Jsou to postupné kroky v pracovním postupu (události, komunikace, části), které ovlivňují 2 a více osob. Na jednotlivé kroky většinou navazují notifikace, schvalující potvrzení nebo vyplnění datových informací ze strany příslušných osob.
WinRM	WinRM (Windows Remote Management) je Microsoft implemtace standardu WS-Management pro vzdálenou správu
WS	Webová služba.
xaaS	Obecné řešení dodávané formou externí služby. Používají se například formy SaaS, IaaS, PaaS, BPaaS.
XSS	Cross-site scripting (XSS) je metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).