SMLOUVA O pořízení nástroje pro řízení PRIVILEGOVANÝCH ÚČTŮ A OPRÁVNĚNÍ

Smluvní strany:

**Česká republika – Ministerstvo práce a sociálních věcí**

se sídlem: Na Poříčním právu 1/376, 128 00 Praha 2

IČO: 005 51 023

bank. spojení: Česká národní banka, pobočka Praha, Na Příkopě 28, 11503 Praha 1,

č. účtu: 2229001/0710

zastoupená: Ing. Karlem Trpkošem, vrchním ředitelem sekce informačních technologií

(dále jen „**Objednatel**“)

a

**NTT Czech Republic s.r.o.**

se sídlem: Milevská 2095/5, 140 00 Praha 4

IČO: 26175738, DIČ: CZ26175738

společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 77064

bank. spojení: *neveřejný údaj*, č. účtu: *neveřejný údaj*

zastoupená: Michaelem Paierem, jednatelem společnosti

(dále jen „**Dodavatel**“)

dnešního dne uzavřely tuto smlouvu o pořízení nástroje na řízení privilegovaných účtů a oprávnění v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“) (dále jen „**Smlouva**“)

Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

1. ÚVODNÍ USTANOVENÍ
   1. Objednatel prohlašuje, že:
      1. je ústředním orgánem státní správy, jehož působnost a zásady činnosti jsou stanoveny zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, a
      2. splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.
   2. Dodavatel prohlašuje, že:
      1. je právnickou osobou řádně založenou a existující podle českého právního řádu,
      2. splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a
      3. ke dni uzavření této Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat.
   3. Objednatel oznámil dne 13. 2. 2024 uveřejněním formuláře Oznámení o zahájení zadávacího řízení ve Věstníku veřejných zakázek svůj záměr zadat veřejnou zakázku s názvem „**Nástroj pro řízení privilegovaných účtů**“, ev. č. Z2024-006897 (dále jen „**Veřejná zakázka**“) dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Na základě tohoto zadávacího řízení byla pro plnění Veřejné zakázky vybrána nabídka Dodavatele v souladu s ustanovením § 122 ZZVZ.
   4. Smluvní strany prohlašují, že mají společnou snahu přispět k férovému a etickému prostředí. S cílem kultivovat prostředí tuzemského trhu tak, aby se přiblížilo vyšším standardům v oblasti obchodní, soutěžní a pracovněprávní etiky, smluvní strany učinily nedílnou součástí této Smlouvy Etický kodex (Příloha 8 této Smlouvy), v souladu, s jehož pravidly se zavazují předmět této Smlouvy plnit.
2. ÚČEL SMLOUVY
   1. Účelem této Smlouvy je zajištění realizace předmětu Veřejné zakázky dle Zadávací dokumentace Veřejné zakázky, tj. implementace nástroje pro řízení privilegovaných účtů do prostředí Objednatele, a to v souladu s požadavky Objednatele definovanými touto Smlouvou a jejími přílohami.
   2. Objednatel uzavírá tuto Smlouvu také s cílem naplnit legislativní požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (zákon i vyhláška dále jen „**Kybernetická legislativa**“).
   3. Dodavatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy aplikuje subsidiárně.
3. PŘEDMĚT SMLOUVY

Dodavatel se zavazuje:

* 1. formou softwarového předplatného (subscription) poskytnout nástroj/-e či technická nebo virtuální zařízení pro řízení privilegovaných účtů a oprávnění. Technické požadavky na funkčnost a kvalitu nástroje a související služby jsou uvedeny v Příloze 1 této Smlouvy,

(dále také jako „**Nástroj PAM**“);

* 1. implementovat Nástroj PAM s fixním počtem účtů a konektorů, který je uveden v odst. 6.1 této Smlouvy. Rozsah implementace je Objednatel upravit pouze postupem v souladu s odst. 6.3 této Smlouvy. Činnosti, které Dodavatel provede v rámci implementace, jsou uvedeny v harmonogramu v Příloze 3 této Smlouvy,

(dále také jako „**Základní implementace**“);

* 1. poskytovat technickou podporu výrobce a technickou podporu Dodavatele pro Nástroj PAM, dle požadavků uvedených v Příloze 1 této Smlouvy,

(dále také jako „**Technická podpora**“);

* 1. na vyžádání a dle potřeb Objednatele poskytovat doplňkové služby pro oblast kybernetické bezpečnosti,

(dále také jako „**Doplňkové služby**“);

* 1. vytvořit exitovou strategii na přechod k jinému dodavateli stejného Nástroje PAM a poskytnutí služeb exitu, které jsou spojené se závěrečným ukončením poskytování podpory Nástroje PAM a spočívající v přípravě a předání novému dodavateli na konci smluvního vztahu podle pokynů Objednatele,

(dále také jako „**Služby exitu**“)

(všechny body předmětu této Smlouvy dle odst. 3.1 až 3.5 společně též jako „**Předmět plnění**“).

* 1. Dodavatel dále bere na vědomí, že na základě plnění této Smlouvy získá přístup k osobním údajům a k záznamům, které mohou obsahovat osobní údaje či jejich fragmenty uložené v monitorovaných systémech Objednatele. Dodavatel se zavazuje pro Objednatele jako správce osobních údajů zpracovávat osobní údaje v prostředí ICT Objednatele, a to dle podmínek stanovených v čl. 14 této Smlouvy.
  2. Objednatel se touto Smlouvou zavazuje poskytnout Dodavateli nezbytnou součinnost při poskytování Předmětu plnění Dodavatelem v rozsahu, který je vymezen v této Smlouvě.
  3. Objednatel se zavazuje zaplatit Dodavateli dohodnutou cenu za řádně a včas poskytnutý Předmět plnění nebo jeho část, a to za podmínek touto Smlouvou dále stanovených.
  4. Dodavatel se zavazuje poskytovat Předmět plnění za aktivní účasti členů realizačního týmu uvedeného v Příloze 4 této Smlouvy, jimiž Dodavatel prokázal svou kvalifikaci v zadávacím řízení Veřejné zakázky a jež byli hodnoceni, jejich odpovídajícími náhradníky, jež prokážou minimální kvalifikaci a dosáhnou minimálně stejného počtu bodů v hodnocení jako nahrazovaný člen realizačního týmu nebo dalšími osobami na stejných pozicích (rolích) jako členové realizačního týmu uvedení v Příloze 4 této Smlouvy při rozšíření realizačního týmu, přičemž i tyto osoby musí prokázat minimální kvalifikaci a dosáhnout minimálně stejného počtu bodů v hodnocení jako člen realizačního týmu na stejné pozici (roli). Jakákoliv dodatečná změna členů realizačního týmu či jeho rozšíření o nového člena musí být předem projednána a písemně schválena Objednatelem. Objednatel bezdůvodně neodepře svůj souhlas se změnou člena realizačního týmu či jeho rozšířením, pokud tato osoba bude disponovat požadovanými minimálními znalostmi a odbornou kvalifikací dle požadavků Objednatele uvedených v zadávací dokumentaci Veřejné zakázky a minimálně stejnými zkušenostmi a praxí, které byly předmětem hodnocení dle zadávací dokumentace, tj. Dodavatel se zavazuje doložit, že nový člen realizačního týmu by získal alespoň stejný počet bodů v rámci hodnocení jako člen realizačního týmu, kterého nahrazuje, či jehož pozice (role) je rozšířena o nového člena realizačního týmu. Smluvní strany tímto ujednaly, že v případě dodatečné změny členů realizačního týmu nebude uzavřen dodatek, jímž dojde ke změně Přílohy 4 této Smlouvy.
  5. Dodavatel se dále zavazuje poskytovat Předmět plnění dle této Smlouvy sám, nebo s využitím poddodavatelů uvedených v Příloze 6 této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Dodavatel sám. Dodavatel se zavazuje, že při poskytování Předmětu plnění prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má odpovědnost, jako by Předmět plnění poskytoval sám. Smluvní strany tímto ujednaly, že v případě dodatečné změny poddodavatele nebude uzavřen dodatek, jímž dojde ke změně Přílohy 6 této Smlouvy.
  6. Smluvní strany výslovně uvádějí, že při poskytování Předmětu plnění prostřednictvím jakékoliv třetí osoby má Dodavatel odpovědnost, jako by plnění dle této Smlouvy realizoval sám.
  7. Objednatel se touto Smlouvou zavazuje poskytnout Dodavateli nezbytnou součinnost při poskytování Předmětu plnění Dodavatelem v rozsahu, který je vymezen v této Smlouvě.
  8. Objednatel se zavazuje uhradit Dodavateli dohodnutou cenu za řádně a včas poskytnutý Předmět plnění nebo jeho část, a to za podmínek touto Smlouvou dále stanovených.
  9. Objednatel se zavazuje ve svých datových centrech zajistit HW a SW prostředí pro řádnou implementaci a provoz Nástroje PAM. Maximální možné parametry pro prostředí jsou uvedeny v Příloze 1 této Smlouvy.

1. MÍSTO, TERMÍNY A ZPŮSOB PLNĚNÍ
   1. Dodavatel se zavazuje realizovat Předmět plnění v následujících termínech:
      1. poskytovat Nástroj PAM dle odst. 3.1 průběžně po dobu 48 měsíců od termínu *Fakturační milník 1*, který je uvedený v Příloze 3 této Smlouvy;
      2. Realizovat Základní implementaci dle odst. 3.2 této Smlouvy v souladu s harmonogramem uvedeným v Příloze 3 této Smlouvy;
      3. Poskytovat Technickou podporu dle odst. 3.3 této Smlouvy průběžně po celou dobu účinnosti této Smlouvy od termínu dokončení Základní implementace *(Fakturační milník 2 uvedený v Příloze 3 této Smlouvy)*;
      4. Poskytovat Doplňkové služby dle odst. 3.4 této Smlouvy dle potřeby Objednatele po celou dobu účinnosti Smlouvy;
      5. Poskytovat Služby exitu dle odst. 3.2 této Smlouvy v souladu s termíny uvedenými v čl. 7 této Smlouvy.
   2. V případě potřeby o poskytnutí Doplňkových služeb dle odst. 3.4 této Smlouvy zašle Objednatel podle odst. 13.1.2i) této Smlouvy Dodavateli písemnou objednávku obsahující detailní specifikaci zamýšleného obsahu a rozsahu prací. Specifikace bude obsahovat popis zadání, očekávanou pracnost v ČD (1 ČD = 8 pracovních hodin), termín dodání a fakturační milník. Objednávka musí být před započetím předmětných prací písemně odsouhlasena Dodavatelem.
   3. Veškeré písemné výstupy ze své činnosti bude Dodavatel předávat v sídle Objednatele, nebude-li v konkrétním případě Smluvními stranami sjednáno jinak.
   4. Místem plnění jsou datová centra Objednatele v lokalitách Sokolovská 855/225 a Na Poříčním právu 376/1 (obojí Praha), dále cloudové prostředí Microsoft Azure ve správě Objednatele a cloudová prostředí Dodavatele a výrobce Nástroje PAM. Základní implementace nebo poskytnutí Doplňkových služeb a Služeb exitu může zahrnovat i činnosti provádění v sídle Objednatele a dále jakékoliv místo v České republice, k němuž se vztahuje či by se mohlo vztahovat poskytování Předmětu plnění.
2. CENA A PLATEBNÍ PODMÍNKY
   1. Cena za poskytnutí Nástroje PAM dle odst. 3.1 této Smlouvy a její hrazení:
      1. Cena za poskytnutí Nástroje PAM je stanovena jako součin účtů či konektorů a jednotkové ceny uvedené v Příloze 7 této Smlouvy.
      2. Objednatel se zavazuje objednat služby poskytování Nástroje PAM v rozsahu Základní implementace dle odst. 6.1. této Smlouvy na období 48 měsíců. Cena za poskytování Nástroje PAM bude Objednatelem uhrazena na základě faktury vystavené Dodavatelem do 5 pracovních dnů ode dne Akceptace dle harmonogramu plnění uvedeného v Příloze 3 této Smlouvy (Fakturační milník 1).
      3. Zúčtovací období za poskytnutí Nástroje PAM je jeden rok počínaje termínem *Fakturační milník 1*, který je uveden v Příloze 3 této Smlouvy.
      4. Cena za poskytnutí Nástroje PAM je splatná vždy na začátku zúčtovacího období, počínaje termínem *Fakturační milník 1*, který je uveden v Příloze 3 této Smlouvy.
      5. Objednatel může kdykoli v průběhu účinnosti Smlouvy upravit počet účtů a konektorů. Vždy však musí být zachován minimální počet v rozsahu Základní implementace dle odst. 6.1 této Smlouvy.
      6. V případě navýšení počtu účtů a konektorů bude cena stanovena jako alikvótní část součinu účtů a konektorů a jednotkových cen, a to k datu konce zúčtovacího období s přesností na měsíc. Pokud dojde k navýšení počtu účtů a konektorů méně než rok před ukončením účinnosti Smlouvy, je cena stanovena jako alikvótní část do doby ukončení účinnosti Smlouvy. Cena SW licencí Nástroje PAM související s tímto navýšením je splatná k datu předání těchto licencí do užívaní Objednateli.
      7. Snížení počtu účtů a konektorů nemá vliv na cenu v rámci probíhajícího zúčtovacího období. Pro navazující zúčtovací období je cena stanovena podle skutečného počtu účtů a konektorů dle požadavků Objednatele.
      8. Snížení počtu účtů a konektorů může probíhat každoročně, a to ke konci zúčtovacího období. Objednatel je zavazuje, 3 měsíce před tímto datem, definovat požadované množství účtů a konektorů na následující období, a k obnově tohoto množství se zavázat na další zúčtovací období.
   2. Cena za poskytnutí Technické podpory dle odst. 3.3 této Smlouvy a její hrazení:
      1. Cena Technické podpory je uvedena v Příloze 7 této Smlouvy.
      2. Cena je pevná po celou dobu účinnosti Smlouvy a není závislá na aktuálním počtu účtů ani konektorů Nástroje PAM.
      3. Zúčtovací období za poskytnutí Technické podpory je jeden rok.
      4. Cena za poskytnutí Technické podpory je splatná vždy na začátku zúčtovacího období, počínaje termínem *Fakturační milník 2*, který je uveden v Příloze 3 této Smlouvy.
   3. Cena za realizaci Základní implementace dle odst. 3.2 této Smlouvy stanovena smluvními stranami ve výši, která je detailně specifikována v Příloze 7 této Smlouvy. Tato cena je pevná a úplná, tj. zahrnuje veškerá plnění dle této Smlouvy v rámci realizace Základní implementace. Cena za realizaci Základní implementace bude Objednatelem uhrazena na základě faktury vystavené Dodavatelem do 5 pracovních dnů ode dne Akceptace dle harmonogramu plnění uvedeného v Příloze 3 této Smlouvy *(Fakturační milník 2)*.
   4. Cena Doplňkových služeb:
      1. Cena Doplňkových služeb dle odst. 3.4 této Smlouvy je stanovena Smluvními stranami sazbou za 1 ČD (1 ČD = 8 pracovních hodin), která je detailně specifikována v Příloze 7 této Smlouvy. Tato jednotková cena je pevná a úplná, tj. zahrnuje veškerá plnění dle této Smlouvy v rámci poskytování Doplňkových služeb za 1 ČD.
      2. Cena za Doplňkové služby bude Objednatelem uhrazena vždy po akceptaci dílčího plnění Doplňkových služeb způsobem dle čl. 9 této Smlouvy, a to na základě faktury vystavené Dodavatelem, a bude stanovena jako součin rozsahu Dodavatelem poskytnutého plnění Doplňkových služeb vyjádřeného v ČD nebo jejich částech, a příslušné sazby za toto plnění dle odst. 5.4.1 této Smlouvy.
      3. Objednatel uhradí cenu pouze za skutečně řádně provedené Doplňkové služby. Objednatel není zavazuje vyčerpat Doplňkové služby dle odst. 3.4 této Smlouvy v rozsahu, který byl uveden v Zadávací dokumentaci Veřejné zakázky. Objednatel je oprávněn, nikoli však zavazuje, čerpat Doplňkové služby nad rozsah uvedený v Příloze 7 této Smlouvy, a to za sazbu dle odst. 5.4.1 této Smlouvy.
   5. Cena za poskytnutí Služeb exitu dle odst. 3.5 této Smlouvy je stanovena smluvními stranami ve výši, která je detailně specifikována v Příloze 7 této Smlouvy. Tato cena je pevná a úplná, tj. zahrnuje veškerá plnění dle této Smlouvy v rámci poskytování Služeb exitu. Cena za Služby exitu bude Objednatelem uhrazena na základě faktury vystavené Dodavatelem do 30 kalendářních dnů ode dne akceptace dílčího plnění nebo řádného ukončení poskytování Služeb exitu podle této Smlouvy.
   6. Celková cena za Předmět plnění může být za celou dobu účinnosti této Smlouvy nejvýše taková, aby součet všech cen za jednotlivé části Předmětu plnění dle této Smlouvy nepřekročil celkovou předpokládanou hodnotu Veřejné zakázky (bez výhrady rozšíření předmětu plnění dle čl. 22 této Smlouvy) ve výši 74 804 000,- Kč bez DPH. To neplatí v případě využití výhrady dle čl. 22 Smlouvy.
   7. V případě, že index růstu spotřebitelských cen (míra inflace vyjádřená přírůstkem indexu spotřebitelských cen ke stejnému měsíci předchozího roku oznamovaná Českým statistickým úřadem ve Veřejné databázi ČSÚ; dále jen „index“) bude ke dni 30. 6. kalendářního roku trvání této Smlouvy představovat procentuální nárůst, je Dodavatel oprávněn svým jednostranným oznámením zaslaným nejpozději do 15. 8. aktuálního kalendářního roku zvýšit cenu jakékoliv položky uvedené v Příloze 7 této Smlouvy o procentuální výši odpovídající procentuálnímu nárůstu indexu, avšak maximálně o 3,00 % zvýšení ročně. Příklad: Pokud by v prvním roce trvání Smlouvy byl k 30. 6. zjištěn narůst hodnoty indexu o 2,40 %, ke zvýšení cen všech služeb poskytovaných Dodavatelem na základě této Smlouvy na další rok dojde právě o 2,40 %. Pokud by ve druhém roce trvání této Smlouvy byl k témuž datu zjištěn nárůst hodnoty indexu o 3,80 %, potom je Dodavatel oprávněn navýšit ceny všech poskytovaných služeb na základě této Smlouvy o 3,00 % oproti cenám předchozího roku, tzn. růst spotřebitelských cen vyjádřený hodnotou indexu nad 3,00 % za rok jde k tíži Dodavatele. Posuzován bude vždy nárůst cen oproti stejnému měsíci předchozího roku, delší období se nezohledňuje. Zvýšení ceny je účinné od 1. 1. následujícího kalendářního roku po doručení písemného oznámení o takovémto zvýšení Objednateli.
   8. Platební podmínky
      1. Splatnost jednotlivých plateb dle této Smlouvy je stanovena na 30 kalendářních dnů od doručení faktury Objednateli. Dodavatel odešle fakturu Objednateli na emailovou adresu osoby Objednatele oprávněné jednat ve věcech technických a osobu Objednatele oprávněné jednat ve věcech bezpečnostních, které jsou uvedeny v Příloze 5 této Smlouvy, nejpozději následující pracovní den po vystavení faktury.
      2. Všechny faktury musí splňovat všechny náležitosti daňového dokladu požadované zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“), avšak výslovně vždy musí obsahovat následující údaje: označení smluvních stran a jejich adresy, IČO, DIČ, údaj o tom, že vystavovatel faktury je zapsán v obchodním rejstříku včetně spisové značky, označení této Smlouvy, označení poskytnutého Předmětu plnění, číslo faktury, den vystavení a lhůta splatnosti faktury, označení peněžního ústavu a číslo účtu, na který má být částka uhrazena, fakturovanou částku, razítko a podpis oprávněné osoby Dodavatele fakturu vystavit.
      3. Nebude-li faktura obsahovat stanovené náležitosti dle předchozího bodu či přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn ji vrátit ve lhůtě její splatnosti Dodavateli. V takovém případě se ruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury.
      4. Platby se provádí bankovním převodem na účet druhé smluvní strany uvedený ve faktuře.
      5. V případě prodlení kterékoliv smluvní strany s uhrazením peněžité částky vzniká oprávněné smluvní straně nárok na úrok z prodlení ve výši 0,01 % z dlužné částky za každý i započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé škody či jiné újmy.
      6. Objednatel bude hradit přijaté faktury pouze na bankovní účty Dodavatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH. V případě, že Dodavatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po zveřejnění příslušného účtu Dodavatele v registru plátců a identifikovaných osob Dodavatelem.
      7. Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátce**“). V případě, že správce daně rozhodne o tom, že Dodavatel je nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do 2 pracovních dnů. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.
   9. Bankovní záruka za řádné poskytování Předmětu plnění
      1. Dodavatel se zavazuje na vlastní náklady obstarat a odevzdat Objednateli před podpisem této Smlouvy originální bankovní záruku za řádné poskytování Předmětu plnění ve výši 1.000.000,- Kč. Bankovní záruka nesmí vypršet dříve, než uplyne 12 kalendářních měsíců po zbytí účinnosti této Smlouvy. Objednatel jako oprávněná osoba bude mít originál bankovní záruky v držení po celou dobu dle předchozí věty.
      2. Bankovní záruka za řádné poskytování Předmětu plnění bude vydána bankou, která byla zřízena a provozuje činnost podle zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů.
      3. Bankovní záruka za řádné poskytování Předmětu plnění musí být sjednána jako bezpodmínečná, znějící na první vyžádání Objednatele a bez námitek. Banka se v této bankovní záruce musí zavázat k uhrazení celé částky na první výzvu Objednatele, pokud Objednatel v této výzvě uvede, že Dodavatel nesplnil závazky vyplývající z této Smlouvy. Banka není oprávněna zkoumat, je-li výzva Objednatele důvodná. Objednatel je oprávněn nechat si předanou bankovní záruku přezkoumat a schválit od své banky. V případě výhrad banky Objednatele k předložené bankovní záruce se Dodavatel zavazuj předložit v dodatečné lhůtě 2 týdnů novou řádnou bankovní záruku za řádné poskytování Předmětu plnění.
      4. Povinnost obstarat bankovní záruku za řádné poskytování Předmětu plnění má Dodavatel. Veškeré náklady spojené s touto bankovní zárukou za řádné poskytování Předmětu plnění a jejím obstaráním jsou zahrnuty ve smluvní ceně dle této Smlouvy a hradí je Dodavatel.
      5. Bankovní záruka za řádné poskytování Předmětu plnění slouží k zajištění řádného splnění všech závazků Dodavatele dle této Smlouvy nebo s touto Smlouvou související, včetně nároků Objednatele na smluvní pokuty, náhradu škody nebo nároků, vzniklých jako důsledek odstoupení od této Smlouvy. Objednatel je oprávněn požadovat plnění z bankovní záruky za řádné poskytování Předmětu plnění jen na základě písemného oznámení bance, že Dodavatel nesplnil určitý závazek dle této Smlouvy nebo s touto Smlouvou související a není zavazuje překládat bance žádné další dokumenty, které by takovéto nesplnění potvrzovaly.
      6. V případě, že Objednatel uplatní nárok na uhrazení konkrétní částky, bude čerpat plnění z bankovní záruky za řádné poskytování Předmětu plnění do výše požadované částky. Před uplatněním plnění z bankovní záruky za řádné poskytování Předmětu plnění oznámí Dodavateli písemně důvod a výši požadovaného plnění z titulu bankovní záruky za řádné poskytování Předmětu plnění. V případě jejího čerpání se Dodavatel zavazuje poskytnout Objednateli novou bankovní záruku – předložit novou záruční listinu ve znění shodném s předcházející záruční listinou (na původní výši záruky) tak, aby splnil povinnost udržovat bankovní záruku za řádné poskytování Předmětu plnění v souladu s jejími parametry v této Smlouvě, a to nejpozději do 14 dnů ode dne uplatnění práva Objednatelem.
      7. Objednatel se zavazuje odškodnit Dodavatele a zabezpečit, aby mu nevznikla žádná újma v důsledku uplatnění nároků z bankovní záruky za řádné poskytování Předmětu plnění v rozsahu, na který Objednatel neměl nárok.
      8. Strany dohody se dohodly, že v případě nepředložení bankovní záruky za řádné poskytování Předmětu plnění ve stanovených lhůtách, nebo v případě jejich předložení ve formě a s obsahem, který bude v rozporu s podmínkami uvedenými v odst. 5.9 této Smlouvy, půjde o podstatné porušení této Smlouvy.
3. ROZSAH ZÁKLADNÍ IMPLEMENTACE A JEJÍ NAVÝŠENÍ
   1. Rozsah Základní implementace je stanoven podle počtu privilegovaných účtů a konektorů ke cloudovým službám:

|  |  |  |
| --- | --- | --- |
| ZÁKLADNÍ IMPLEMENTACE | Jednotka | Počet |
| Privilegovaný účet standard - interní admin | Uživatel v AD | 50 |
| Privilegovaný účet remote - externí admin (dodavatel) | Uživatel v AD | 100 |
| Cloudový účet | Uživatel v AD | 5 |
| Správce hesel | Uživatel v AD | 20 |
| Privilegovaný účet pro správu koncových zařízení | Uživatel v AD | 20 |
| Aplikační účet pro automatizované operace | Technický účet | 5 |
| Správa aplikačních účtů v Azure | Konektor do Azure | 1 |
| Správa aplikačních účtů v DevOps prostředí | Konektor do Azure | 1 |

* 1. V rámci Základní implementace provede Dodavatel všechny činnosti, které jsou uvedeny v harmonogramu v Příloze 3 této Smlouvy, a to s počtem účtů (jednotek) uvedených v odst. 6.1 této Smlouvy. Přesný výčet konkrétních aktiv bude výstupem činnosti „Návrh architektury Nástroje PAM a úprav v prostředí MPSV“, kterou Dodavatel provede a Objednatel akceptuje dle harmonogramu uvedeného v Příloze 3 této Smlouvy.
  2. Na vyžádání a dle potřeb Objednatele rozšíří Dodavatel Nástroj PAM na další aktiva (zařízení ICT, systémy, aplikace a podobné zdroje) Objednatele.
     1. Objednatel může počty účtů a konektorů navýšit tak, aby bylo dodrženo ustanovení v odst. 5.6 této Smlouvy.
     2. V případě zájmu o navýšení počty účtů a konektorů zašle Objednatel podle odst. 13.1.2i) této Smlouvy Dodavateli písemnou objednávku obsahující počet nových účtů a konektorů. V případě, že Objednatel bude v rámci rozšíření Nástroje PAM požadovat také Doplňkové služby, může být objednávka spojena s objednávkou vystavenou dle odst. 4.2 této Smlouvy. Objednávka musí být před započetím předmětných prací odsouhlasena Dodavatelem.
  3. Smluvní strany se dohodly, že Objednatel je oprávněn v rámci Doplňkových služeb dle odst. 3.4 této Smlouvy požádat Dodavatele o posouzení Objednatelem zamýšlených změn v prostředí ICT, které mohou mít dopad na poskytování Nástroje PAM a Technické podpory. Dodavatel se v takovém případě zavazuje bez zbytečného odkladu posoudit zamýšlenou změnu z hlediska zachování řádného poskytování Nástroje PAM a Technické podpory a Objednatel se zavazuje uhradit Dodavateli prokázané účelně vynaložené náklady takovéhoto posouzení, které bude poskytnuto jako v rámci Doplňkových služeb. Pokud provede Objednatel změnu ve svém prostředí ICT nad rámec posuzovaný Dodavatelem, v rozporu s instrukcemi Dodavatele a/nebo bez předchozího posouzení změny Dodavatelem, je Dodavatel oprávněn omezit poskytování Nástroje PAM a Technické podpory, pokud by taková změna měla poskytování Nástroje PAM a Technické podpory omezovat či narušovat.

1. ZPŮSOB POSKYTOVÁNÍ SLUŽEB EXITU
   1. Dodavatel se zavazuje dle pokynů Objednatele poskytnout veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s poskytováním Nástroje PAM a Technické podpory na Objednatele a/nebo nového poskytovatele, ke kterému dojde po pozbytí účinnosti této Smlouvy, tedy poskytnout Služby exitu dle odst. 3.5 této Smlouvy, které zahrnují:
      1. vypracování strategie a plánu exitu a poskytnutí nezbytné součinnosti k jeho realizaci,
      2. poskytnutí potřebné součinnosti podle pokynů Objednatele novému poskytovateli,
      3. předání veškeré dokumentace a potřebných informací,
      4. předání všech uložených dat,
   2. Za účelem dle předchozího bodu se Dodavatel zavazuje ve lhůtách dle odst. 7.3 této Smlouvy vypracovat na základě pokynu Objednatele dokumentaci vymezující postup provedení Služeb exitu (dále jen „**Exitový plán**“), a poskytnout plnění nezbytná k realizaci tohoto Exitového plánu za přiměřeného použití vhodných ustanovení této Smlouvy. Závazek dle tohoto ustanovení platí nejméně 1 rok od ukončení smluvního vztahu založeného touto Smlouvou.
   3. Objednatel je oprávněn požádat o vypracování Exitového plánu nejdříve 1 rok před řádným pozbytím účinnosti této Smlouvy, dále kdykoli spolu s odstoupením/výpovědí Objednatele od této Smlouvy, nebo i po odstoupení/výpovědi Dodavatele od této Smlouvy. Dodavatel se zavazuje vypracovat Exitový plán a po akceptaci Objednatelem poskytnout plnění nezbytná k jeho realizaci do 1 měsíce od doručení takového požadavku Objednatele, nestanoví-li Objednatel jinak.
   4. V případě, že dojde k uzavření nové smlouvy týkající se Předmětu plnění nebo jakékoli jeho části s novým poskytovatelem odlišným od Dodavatele, zavazuje se Dodavatel po pozbytí účinnosti této Smlouvy poskytovat Objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely řádného provedení Služeb exitu. Dodavatel se zavazuje zajistit předání Nástroje PAM a souvisejících služeb novému poskytovateli, a to i nad rámec svých povinností dle čl. 7 této Smlouvy. Dodavatel se zavazuje tuto součinnost poskytovat s odbornou péčí, bez zbytečného odkladu a zodpovědně, a to minimálně po dobu 2 let od ukončení smluvního vztahu založeného touto Smlouvou. Smluvní strany se dohodly, že rozsah tohoto plnění je zahrnut v ceně plnění podle této Smlouvy. Pro vyloučení pochybností se stanoví, že v této souvislosti nevznikne Dodavateli nárok na dodatečné finanční plnění ze strany Objednatele.
2. ZMĚNOVÉ ŘÍZENÍ
   1. Kterákoliv ze smluvních stran je oprávněna písemně navrhnout změny technické specifikace uvedené v Příloze 1 této Smlouvy. Objednatel není zavazuje navrhovanou změnu akceptovat. Dodavatel se zavazuje vynaložit veškeré úsilí, které po něm lze spravedlivě požadovat, aby změnu požadovanou Objednatelem akceptoval.
   2. Dodavatel se zavazuje provést hodnocení dopadů kteroukoliv smluvní stranou navrhovaných změn na termíny plnění, cenu a součinnost Objednatele. Dodavatel se zavazuje toto hodnocení provést bez zbytečného odkladu, nejpozději do 5 pracovních dnů ode dne doručení návrhu kterékoliv smluvní strany druhé smluvní straně.
   3. Jakékoliv změny technické specifikace uvedené v Příloze 1 této Smlouvy musí být písemně sjednány v souladu s příslušnými ustanoveními ZZVZ, a to zejména v souladu s ustanovením § 222 ZZVZ.
   4. Kterákoli ze smluvních stran je rovněž oprávněna navrhnout změnu poskytování Předmětu plnění, a to při přiměřené aplikaci odst. 8.1 až 8.3 této Smlouvy.
3. AKCEPTACE
   1. Každý výstup Doplňkových služeb, který představuje samostatný předmět způsobilý převzetí (dále jen „**dílčí plnění**“), bude Objednatelem akceptován na základě akceptační procedury. Akceptační procedura zahrnuje ověření, zda Dodavatelem poskytnuté dílčí plnění je výsledkem, ke kterému se Dodavatel zavázal, a to porovnáním skutečných vlastností jednotlivých dílčích plnění Dodavatele s jejich závaznou specifikací stanovenou touto Smlouvou či dohodnutým závazným dokumentem za využití akceptačních kritérií v dokumentu stanovených nebo později pro tento účel dohodnutých smluvními stranami.
   2. **Akceptace dokumentů**
      1. Dokumenty, které mají být podle této Smlouvy vypracované Dodavatelem a předané Objednateli, budou Objednatelem akceptovány v souladu s akceptační procedurou definovanou v tomto odst. 9.2 Smlouvy.
      2. Dodavatel se zavazuje průběžně konzultovat průběh zpracování dokumentů dle odst. 9.2 této Smlouvy s Objednatelem. Dodavatel se zavazuje předat dokumenty k akceptaci včas tak, aby mohly být dodrženy navazující termíny.
      3. Objednatel se zavazuje vznést své výhrady nebo připomínky k dokumentu do 10 pracovních dnů ode dne jeho předání Objednateli Dodavatelem k akceptaci. Vznese-li Objednatel výhrady nebo připomínky k dokumentu, zavazuje se Dodavatel do 10 pracovních dnů provést veškeré potřebné úpravy dokumentu dle výhrad a připomínek Objednatele a takto upravený dokument předat Objednateli k akceptaci. Pokud výhrady a připomínky Objednatele přetrvávají nebo Objednatel identifikuje výhrady a připomínky nové, je Objednatel oprávněn postupovat podle tohoto odst. 9.2.3 Smlouvy i opakovaně.
      4. V případě, že Objednatel nemá k dokumentu připomínky ani výhrady, zavazuje se ve lhůtě 10 pracovních dnů od jeho předání Objednateli Dodavatelem k akceptaci tento dokument akceptovat a potvrdit jeho převzetí formou písemného předávacího protokolu.
      5. Bude-li trvání akceptační procedury ovlivněné vznesením výhrad nebo připomínek Objednatele k dokumentu a potřebou jejich vyřešení, nebude to mít vliv na dohodnuté termíny pro akceptaci dokumentu.
   3. **Akceptace jiných dílčích plnění než dokumentů**
      1. Umožňuje-li to povaha plnění Dodavatele a nestanoví‑li tato Smlouva jinak, bude akceptace jednotlivých dílčích plnění jiných než dokumentů provedena v souladu s akceptační procedurou definovanou v tomto odst. 9.3 této Smlouvy.
      2. Předání a převzetí Objednatelem objednaného a Dodavatelem řádně provedeného dílčího plnění bude probíhat postupně akceptací jednotlivých částí dílčích plnění, a to v termínech uvedených v této Smlouvě nebo stanovených v souladu s touto Smlouvou.
      3. Akceptační procedura zahrnuje ověření řádného provedení jednotlivých dílčích plnění porovnáním jejich skutečných vlastností s jejich specifikací stanovenou touto Smlouvou či dohodnutým závazným dokumentem za využití akceptačních kritérií v dokumentu stanovených nebo později pro tento účel dohodnutých smluvními stranami.
      4. Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů připravené Dodavatelem. Nedohodnou-li se smluvní strany jinak, přípravu scénářů, příkladů a dat pro potřeby akceptačního testu zajistí Dodavatel za přiměřené součinnosti Objednatele, a to s ohledem na účel akceptační procedury dle odst. 9.3.3 této Smlouvy. Objednatel má právo vyjadřovat se a požadovat zapracování svých odůvodněných připomínek ke specifikaci akceptačních testů a dalším parametrům testování.
      5. Jestliže jednotlivé dílčí plnění splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních testů umožnit Objednateli toto dílčí plnění převzít a Objednatel se zavazuje k jeho převzetí nejpozději do 5-ti pracovních dnů. Smluvní strany se zavazují o tomto převzetí sepsat předávací protokol.
      6. Pokud kterékoliv z jednotlivých dílčích plnění nesplňuje stanovená akceptační kritéria nebo je splňuje s vadami, které jsou přípustné, sdělí Objednatel své připomínky písemně Dodavateli; pokud Objednatel takové dílčí plnění současně akceptuje, uvede své připomínky v předávacím protokolu. Nesdělení připomínek nebo neoznámení některé vady při akceptaci nemá vliv na povinnost Dodavatele tuto vadu odstranit, pokud o ní ví, dodatečně ji zjistí či mu bude dodatečně oznámena.
      7. Dodavatel se zavazuje vypořádat připomínky Objednatele bez zbytečného odkladu a neprodleně předložit příslušné dílčí plnění k opakované akceptaci dle této Smlouvy, za přiměřeného použití ostatních ustanovení čl. 9 této Smlouvy. Akceptační procedura, včetně procesu testování a případných následných oprav, se bude opakovat, dokud příslušné dílčí plnění nesplní akceptační kritéria pro příslušný akceptační test. V případě, že se jedná o vypořádání připomínek k dílčímu plnění, které již bylo akceptováno, namísto předávacího protokolu strany potvrdí písemně, že připomínky byly vypořádány.
      8. Dohodnuté termíny pro akceptaci dílčího plnění nejsou dotčeny trváním akceptační procedury ani jakýmkoli jejím prodloužením z důvodu vad bránících akceptaci.
   4. Lhůty uvedené v čl. 9 této Smlouvy platí, pokud se Smluvní strany nedohodnou písemně jinak.
4. DALŠÍ POVINNOSTI DODAVATELE
   1. Dodavatel se dále zavazuje:
      1. poskytovat Předmět plnění vlastním jménem, na vlastní odpovědnost a v souladu s pokyny Objednatele řádně a včas, zejména se zohledněním délky trvání akceptační procedury;
      2. poskytovat Předmět plnění s péčí řádného hospodáře odpovídající podmínkám sjednaným v této Smlouvě; dostane-li se Dodavatel do prodlení s plněním, aniž by prodlení způsobil Objednatel či nastala překážka vylučující povinnost k náhradě škody po dobu delší než 30 kalendářních dnů, je Objednatel oprávněn zajistit náhradní plnění po dobu prodlení Dodavatele jinou osobou; v takovém případě se Dodavatel zavazuje nahradit v plném rozsahu náklady spojené s náhradním plněním;
      3. upozorňovat Objednatele včas na všechny hrozící vady či výpadky svého plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro poskytování Předmětu plnění nezbytné;
      4. neprodleně oznámit písemnou formou Objednateli překážky, které mu brání v poskytování Předmětu plnění a výkonu dalších činností s tím souvisejících;
      5. upozornit Objednatele na potenciální rizika vzniku škod či újmy a včas a řádně dle svých možností provést taková opatření, která riziko vzniku škody či jiné újmy zcela vyloučí nebo sníží;
      6. i bez pokynů Objednatele provést nutné úkony, které, ač nejsou součástí Předmětu plnění, budou s ohledem na nepředvídané okolnosti pro poskytování Předmětu plnění nezbytné nebo jsou nezbytné pro zamezení vzniku škody či jiné újmy; jde-li o zamezení vzniku škody či jiné újmy nezapříčiněných Dodavatelem, má Dodavatel právo na úhradu nezbytných a účelně vynaložených nákladů;
      7. postupovat při poskytování Předmětu plnění s odbornou péčí a aplikovat procesy „*best practice*“;
      8. v případě potřeby průběžně komunikovat s Objednatelem a třetími osobami, vyžaduje-li to řádné poskytnutí Předmětu plnění, přičemž veškerá taková komunikace bude probíhat v českém jazyce (případně slovenském), nebo za využití překladatele do českého jazyka;
      9. informovat Objednatele o plnění svých závazků vyplývajících z této Smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností smluvních stran;
      10. informovat Objednatele o významné změně kontroly nad Dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k poskytování Předmětu plnění;
      11. zajistit, aby všechny osoby podílející se na plnění závazků Dodavatele vyplývajících z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy Objednatele, s nimiž Objednatel Dodavatele obeznámil;
      12. chránit osobní údaje, data a duševní vlastnictví Objednatele a třetích osob;
      13. upozorňovat Objednatele na možné rozšíření či změny Nástroje PAM za účelem lepšího využívání pro jeho účel;
      14. upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele.
   2. Dodavatel se zavazuje udržovat v platnosti a účinnosti po celou dobu trání smluvního vztahu založeného touto Smlouvou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy, nesmí být nižší než 20.000.000,- Kč za rok. Pojistnou smlouvu dle tohoto odstavce, pojistku potvrzující uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy se Dodavatel zavazuje předložit Objednateli kdykoliv bezodkladně po písemném vyžádání Objednatele. Nepředložením pojistné smlouvy, pojistky nebo pojistného certifikátu do 1 kalendářního měsíce od vyžádání ze strany Objednatele vzniká právo Objednatele na odstoupení od této Smlouvy.
   3. Dodavatel se zavazuje poskytnout Objednateli veškeré informace potřebné ke splnění povinností Objednatele dle § 219 ZZVZ, zejména, nikoli však výlučně, nejpozději do 15. března kalendářního roku informaci o ceně uhrazené za poskytování Předmětu plnění v předchozím kalendářním roce plnění této Smlouvy.
5. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA
   1. Vzhledem k tomu, že součástí poskytovaného Předmětu plnění je i plnění, které může naplňovat znaky autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“), je k těmto součástem plnění poskytována licence za podmínek sjednaných dále v tomto článku Smlouvy.
   2. Všechna data, ať už v jakékoliv podobě, a jejich hmotné nosiče, která vznikla či vzniknou při poskytování Předmětu plnění, jsou výlučným vlastnictvím Objednatele a má k nim primárně užívací právo. Dodavatel se zavazuje chránit data v systémech Objednatele před ztrátou nebo poškozením a přistupovat k nim a užívat je pouze v souladu s touto Smlouvou, obecně závaznými právními předpisy a zájmy Objednatele.
   3. Objednatel je oprávněn veškeré výstupy dle této Smlouvy považované za autorské dílo ve smyslu autorského zákona (dále jen „autorská díla“) užívat dle níže uvedených podmínek.
      1. Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu dle odst. 11.3.3 této Smlouvy užívat toto autorské dílo k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že Objednatel je oprávněn užívat autorské dílo v neomezeném množstevním a územním rozsahu, a to všemi v úvahu přicházejícími způsoby a s časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv k takovémuto autorskému dílu. Součástí licence je neomezené oprávnění Objednatele provádět jakékoliv modifikace, úpravy, změny autorského díla tvořícího výsledky plnění dle této Smlouvy a dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob. Objednatel je bez potřeby jakéhokoliv dalšího svolení Dodavatele oprávněn udělit třetí osobě podlicenci k užití autorského díla nebo svoje oprávnění k užití autorského díla třetí osobě postoupit. Licence k autorskému dílu je poskytována jako neomezená nevýhradní. Objednatel není povinen licenci využít.
      2. V případě korelací a pravidel se licence vztahuje ve stejném rozsahu na autorské dílo ve strojovém i zdrojovém kódu, jakož i koncepční přípravné materiály.
      3. Dodavatel touto Smlouvou poskytuje Objednateli licenci k autorským dílům dle odst. 11.3.1 této Smlouvy, přičemž účinnost této licence nastává okamžikem akceptace dílčího plnění, které příslušné autorské dílo obsahuje; do té doby je Objednatel oprávněn autorské dílo užít v rozsahu a způsobem nezbytným k provedení akceptace příslušné součásti dílčího plnění.
      4. Udělení licence nelze ze strany Dodavatele vypovědět a její účinnost trvá i po ukončení smluvního vztahu založeného touto Smlouvou, nedohodnou-li se smluvní strany jinak.
      5. Smluvní strany výslovně prohlašují, že pokud při poskytování Předmětu plnění vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se smluvní strany jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Dodavatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Smluvní strany se dohodly, že Dodavateli nevzniká v případě vytvoření díla spoluautorů nárok na odměnu.
      6. Dodavatel se zavazuje postupovat tak, aby udělení licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.
      7. Součástí poskytovaného Předmětu plnění může být i tzv. standardní software anebo tzv. open source software (dále společně také jen „**standardní software**“), u kterého není Dodavatel oprávněn udělit Objednateli oprávnění dle předchozích ustanovení odst. 11.3 této Smlouvy nebo to po něm nelze spravedlivě požadovat (pro vyloučení veškerých pochybností smluvní strany uvádí, že v případě, kdy je vývoj software hrazen Objednatelem, je Objednatel oprávněn vždy požadovat udělení oprávnění dle předchozích ustanovení odst. 11.3 této Smlouvy), pouze při splnění některé z následujících podmínek:
         1. Jedná se o software výrobců, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty oprávněnými takovýto software upravovat, a který je v době uzavření této Smlouvy prokazatelně užíván v produktivním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů. Dodavatel se zavazuje poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
         2. Jedná se o software, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty, který je v době uzavření Smlouvy prokazatelně užíván v produktivním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů, a k němuž není poskytnutí licence v rozsahu dle předchozích ustanovení odst. 11.3 této Smlouvy účelné a nebrání dalšímu rozvoji ze strany Objednatele (zejména vývojový software, integrační software, software typu “software factory“, databázový software aj.). Dodavatel se zavazuje poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
         3. Jedná se o software, který je veřejnosti poskytován zdarma, včetně detailně komentovaných zdrojových kódů, úplné uživatelské, provozní a administrátorské dokumentace a práva software měnit. Dodavatel se zavazuje poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
         4. Jedná se o software, u kterého Dodavatel poskytne s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost bez nutnosti vynakládání výraznějších prostředků, písemnou garanci, že další rozvoj Nástroje PAM jinou osobou než Dodavatelem je možné provádět bez toho, aby tím byla dotčena práva autorů takovéhoto softwaru, neboť nebude nutné zasahovat do zdrojových kódů takovéhoto softwaru anebo proto, že případné nahrazení takovéhoto softwaru nebude představovat výraznější komplikaci a náklad na straně Objednatele. Dodavatel se zavazuje poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
         5. Jedná se o software, jehož API (*Application Programming Interface*) pokrývá všechny moduly a funkcionality software, je dobře dokumentované, umožňuje zapouzdření software a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele bez nutnosti zásahu do zdrojových kódů softwaru, a Dodavatel poskytne Objednateli právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako software. Dodavatel se zavazuje poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.
         6. Dodavatel se zaváže Objednateli po ukončení implementace na písemnou výzvu Objednatele nejpozději do 30 kalendářních dnů poskytnout (i) úplné komentované zdrojové kódy softwaru a bezpodmínečné právo software měnit nebo (ii) API (*Application Programming Interface*), které pokrývá všechny moduly a funkcionality softwaru, je dobře dokumentované, umožňuje zapouzdření softwaru a jeho adaptaci v rámci měnících se podmínek IT prostředí Objednatele bez nutnosti zásahu do zdrojových kódů softwaru, a právo užít toto rozhraní pro programování aplikací ve stejném rozsahu jako software. Dodavatel se zavazuje na výzvu Objednatele tuto skutečnost prokázat.

V případě že Dodavatel poruší povinnost či prohlášení dle tohoto odst. 11.3.7 Smlouvy, je Objednatel oprávněn požadovat úhradu smluvní pokuty ve výši 20.000,- Kč za každý jednotlivý případ a náhradu škody či jiné újmy v plné výši.

* + 1. Pokud se bude jednat o standardní software Dodavatele nebo třetích stran dle odst. 11.3.7 této Smlouvy, tak na rozdíl od licence ke zbývajícím výstupům z Nástroje PAM či Doplňkových služeb udělované dle odst. 11.3.1 až 11.3.6 této Smlouvy postačí, aby udělená licence k takovému software zahrnovala nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu trvání této Smlouvy a po dobu 1 kalendářního roku následujícího po roce, ve kterém byl ukončen smluvní vztah založený touto smlouvou, a to na území České republiky a v množstevním rozsahu, který je nezbytný pro pokrytí potřeb Objednatele stanovených touto Smlouvou, a to včetně práva Objednatele do standardního software zasahovat, pokud tak stanoví příslušné ustanovení odst. 11.3.7 této Smlouvy. V případě ukončení smluvního vztahu založeného touto Smlouvou formou výpovědi či odstoupení se Dodavatel zavazuje nabídnout Objednateli právo užívat takovýto standardní software v rozsahu, v jakém je to nezbytné pro poskytování Nástroje PAM, Technické podpory a Doplňkových služeb dle této Smlouvy. Tím není dotčeno právo Objednatele pořídit standardní software i od třetí osoby bez ohledu na licence pořízené dříve Dodavatelem. V případě využití tohoto přednostního práva se Dodavatel zavazuje, že právo užívat standardní software dle tohoto odstavce Smlouvy nabídne Objednateli za běžných tržních podmínek a bude vycházet z účetní hodnoty licencí, které pořídil.
    2. Nelze-li to po Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními odst. 11.3.7 této Smlouvy, není Dodavatel povinen předat Objednateli k standardnímu softwaru zdrojové kódy ani není povinen poskytnout právo Objednateli do standardního softwaru zasahovat, vždy se však Dodavatel zavazuje předat Objednateli kompletní Dokumentaci.
    3. Dodavatel se zavazuje ve svých řešeních pro Objednatele omezit využití takového standardního softwaru, který je co do licence omezen ve smyslu odst. 11.3.8 nebo odst. 11.3.9 této Smlouvy.
    4. Dodavatel se zavazuje samostatně zdokumentovat veškeré využití standardního software v rámci poskytování Předmětu plnění a předložit Objednateli písemný ucelený přehled využitého standardního software, jeho licenčních podmínek a alternativních dodavatelů.
    5. Jestliže jsou s užitím standardního software, služeb podpory k němu, či jiných souvisejících plnění spojeny jednorázové či pravidelné poplatky, Dodavatel se zavazuje v rámci ceny plnění dle této Smlouvy řádně uhradit všechny tyto poplatky za celou dobu trvání Smlouvy a po dobu 1 kalendářního roku následujícího po roce, ve kterém byl ukončen smluvní vztah založený touto Smlouvou.
  1. Práva získaná v rámci poskytování Předmětu plnění přechází i na případného právního nástupce Objednatele. Smluvní strany dohodly, že případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.
  2. Odměna za poskytnutí, zprostředkování nebo postoupení licence (či podlicence) k autorským dílům dle tohoto čl. 11 Smlouvy je zahrnuta v ceně plnění dle této Smlouvy. Dodavatel se zavazuje zajistit poskytnutí licence dle podmínek stanovených touto Smlouvou, a to bez ohledu na případný rozdílný obsah standardních licenčních podmínek vykonavatele majetkových práv k takovým autorským dílům.

1. ZÁRUKA
   1. Dodavatel poskytuje záruku, že každá část výstupu Předmětu plnění má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou, zejména v technické specifikaci uvedené v Příloze 1 této Smlouvy, a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.
   2. Dodavatel poskytuje záruku na každou jednotlivou část výstupu Předmětu plnění od okamžiku její akceptace po dobu 24 kalendářních měsíců ode dne akceptace výstupu Předmětu plnění jako celku. Tato záruka se prodlužuje po každém rozšíření výstupu Předmětu plnění provedeném v rámci Doplňkových služeb tak, že bude trvat po dobu 24 kalendářních měsíců ode dne akceptace takového rozšíření či úpravy předmětného výstupu provedených v rámci Doplňkových služeb.
   3. Objednatel je oprávněn vady výstupu Předmětu plnění nahlásit Dodavateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.
   4. Doba od zjištění vady do jejího odstranění se do běhu záruční doby nezapočítává.
   5. Dodavatel prohlašuje, že veškeré části Předmětu plnění poskytnutého na základě této Smlouvy budou prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady Dodavatelem poskytnutého Předmětu plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s Dodavatelem poskytnutým Předmětem plnění, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání Nástroje PAM či jeho části, zavazuje se Dodavatel zajistit náhradní služby a minimalizovat dopady takovéto situace, a to bez dopadu na cenu plnění dle této Smlouvy, přičemž současně nebude dotčen ani nárok Objednatele na náhradu škody či jiné újmy.
   6. Dodavatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorským dílům, která budou součástí poskytovaného Předmětu plnění, resp. že má souhlas všech relevantních třetích osob k poskytnutí licence k autorským dílům podle čl. 11 této Smlouvy; toto prohlášení zahrnuje i taková práva, která by vytvořením autorského díla teprve vznikla.
2. OPRÁVNĚNÉ OSOBY
   1. Každá ze smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby jsou oprávněny zastupovat smluvní stranu ve smluvních a technických záležitostech souvisejících s touto Smlouvou. Pro vyloučení pochybností se smluvní strany dohodly, že:
      1. osoby oprávněné jednat ve věcech smluvních jsou oprávněny vést s druhou smluvní stranou jednání obchodního charakteru a měnit či rušit tuto Smlouvu a uzavírat k ní dodatky dle odst. 23.1 této Smlouvy;
      2. osoby oprávněné ve věcech technických jsou oprávněny
         1. vést s druhou smluvní stranou jednání technického charakteru;
         2. jednat v rámci změnového řízení dle čl. 8 této Smlouvy;
         3. jednat v rámci akceptačních procedur při předávání a převzetí plnění dle čl. 9 této Smlouvy a provádět veškeré úkony v rámci akceptačních procedur; zejména podepisovat příslušné akceptační, předávací či jiné protokoly dle této Smlouvy;
         4. jednat s výrobcem Nástroje PAM i Dodavatelem při řešení bezpečnostních incidentů, konfigurace Nástroje PAM a dalších otázek souvisejících s implementací a provozem Nástroje PAM;
         5. poskytovat stanoviska v technických a bezpečnostních otázkách;
         6. připravovat dodatky ke Smlouvě pro jejich písemné schválení ze strany osob oprávněných ve věcech smluvních, nebo jejich zplnomocněným zástupcům;
         7. jednat jménem smluvních stran v rámci reklamace vad a při uplatňování záruky podle čl. 12 této Smlouvy;
         8. připravovat podklady, zejména zadání pro Doplňkové služby dle odst. 3.4 této Smlouvy, Služby exitu dle odst. 3.5 této Smlouvy a rozšíření Nástroje PAM dle odst. 6.3 této smlouvy a jednat o nich s druhou smluvní stranou.

Osoby oprávněné ve věcech technických a bezpečnostních nejsou oprávněny k jednání, jenž by mělo za přímý následek změnu této Smlouvy nebo jejího předmětu.

* 1. Identifikace oprávněných osob dle tohoto čl. 13 Smlouvy je uvedena v Příloze 5 této Smlouvy a jejich role stanoví tato Smlouva.
  2. Smluvní strany jsou oprávněny změnit oprávněné osoby dle tohoto čl. 13 Smlouvy, jsou však povinny na takovou změnu druhou smluvní stranu písemně upozornit. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.

1. OCHRANA OSOBNÍCH ÚDAJŮ

**Předmět zpracování, kategorie subjektů údajů a typ osobních údajů**

* 1. S ohledem na předmět této Smlouvy smluvní strany předpokládají, že Dodavatel bude zpracovávat osobní údaje nebo zvláštní kategorie osobních údajů (citlivé údaje) (dále společně jen „**osobní údaje**“) obsažené v datech koncových uživatelů monitorovaného prostředí ICT Objednatele (dále jen „**koncoví uživatelé**“). Nedílnou součástí Smlouvy je tak i ujednání o zpracování osobních údajů mezi Objednatelem jako správcem a Dodavatelem jako zpracovatelem, uvedené níže v tomto čl. 14 Smlouvy.
  2. Podrobněji jsou předmět zpracování, kategorie subjektů údajů, typ osobních údajů a rozsah zpracování osobních údajů popsány v Technické specifikaci uvedené v Příloze 1 této Smlouvy.

**Povaha, účel a prostředky zpracování**

* 1. Dodavatel zpracovává osobní údaje automatizovanými prostředky, a to za účelem poskytování Nástroje PAM, případně za dalšími účely, které vyplývají z této Smlouvy a jejích příloh.
  2. Podrobněji jsou povaha, účel a prostředky zpracování osobních údajů popsány v Technické specifikaci uvedené v Příloze 1 této Smlouvy.

**Doba zpracování**

* 1. Zpracování osobních údajů bude ze strany Dodavatele probíhat po dobu trvání smluvního vztahu založeného touto Smlouvou. Povinnosti Dodavatele týkající se ochrany osobních údajů se Dodavatel zavazuje plnit po celou dobu trvání smluvního vztahu založeného touto Smlouvou, pokud z ustanovení této Smlouvy nevyplývá, že mají trvat i po ukončení smluvního vztahu.

**Obecné zásady zpracování osobních údajů**

* 1. Dodavatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli vyplývají z právních předpisů o ochraně osobních údajů, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.
  2. Dodavatel v souvislosti se zpracováním osobních údajů:
     1. zpracovává osobní údaje výlučně na základě pokynů Objednatele učiněných v souladu se zásadami komunikace dle této Smlouvy, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládá právo Evropské unie nebo členského státu, které se na Objednatele vztahuje; v takovém případě Dodavatel Objednatele informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;
     2. v případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Dodavatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Dodavatelem, oznámí tuto skutečnost okamžitě Objednateli a poskytne mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení;
     3. poskytne Objednateli součinnost při komunikaci s dozorovým orgánem a dle pokynů Objednatele bude spolupracovat při přípravě odpovědí dozorovému úřadu ohledně činností prováděných Dodavatelem;
     4. nezpracovává osobní údaje získané za účelem plnění této Smlouvy pro své vlastní účely;
     5. nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele;
     6. zohledňuje povahu zpracování;
     7. je Objednateli nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění Objednatelovy povinnosti reagovat na žádosti o výkon práv koncových uživatelů;
     8. je Objednateli nápomocen při zajišťování souladu s povinnostmi Objednatele zajistit úroveň zabezpečení zpracování a ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu a případně též koncovým uživatelům, posuzovat vliv na ochranu osobních údajů (výstupem tohoto posouzení bude poskytnutí podkladových materiálů a vlastních odborných vyjádření) a realizovat předchozí konzultace s dozorovým úřadem, a to při zohlednění povahy zpracování a informací, jež má Dodavatel k dispozici;
     9. v souladu s rozhodnutím Objednatele všechny osobní údaje buď vymaže, nebo vrátí Objednateli, a vymaže existující kopie, pokud právo Evropské unie nebo členského státu nepožaduje uložení daných osobních údajů;
     10. poskytne Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto čl.14 Smlouvy, a umožní audity, včetně inspekcí, prováděné Objednatelem nebo jiným auditorem, kterého Objednatel pověřil, a k těmto auditům přispěje;
     11. není oprávněn osobní údaje koncových uživatelů jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností vyplývajících z této Smlouvy;
     12. umožní Objednateli na vyžádání kontrolu dodržování povinností dle tohoto čl. 14 Smlouvy, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložení seznamu osob s přístupem k osobním údajům či doložení, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby, jak je tato definována níže;
     13. umožní Objednateli přístup do informačního systému užívaného pro zpracování a k probíhajícím operacím zpracování;

přičemž činnosti Dodavatele dle odst. 14.7.7, 14.7.8 a 14.7.10 této Smlouvy budou hrazeny v režimu Doplňkových služeb dle odst. 3.4 této Smlouvy a příslušných příloh, a to dle objednávek Objednatele a skutečně provedených činností; v případě, že některé žádosti se rozhodne Objednatel provádět samostatně, nevznikne ve vztahu k nim Dodavateli právo na úhradu. Pro vyloučení pochybností smluvní strany sjednávají, že Objednatel není povinen tyto služby poptat.

* 1. V souvislosti se zpracováním osobních údajů se Dodavatel zavazuje vést v souladu s právními předpisy o ochraně osobních údajů záznamy o všech kategoriích činností zpracování prováděných pro Objednatele, jež obsahují zejména:
     1. jméno a kontaktní údaje Dodavatele, Objednatele a případného zástupce Objednatele nebo Dodavatele a pověřence pro ochranu osobních údajů;
     2. kategorie zpracování prováděného pro Objednatele;
     3. informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci; a
     4. popis technických a organizačních bezpečnostních opatření.

Dodavatel se na základě písemné výzvy Objednatele zavazuje Objednateli vedené záznamy zpřístupnit.

* 1. Dodavatel zajišťuje, kontroluje a odpovídá za
     1. plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,
     2. zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
     3. zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
     4. opatření, která umožní určit a ověřit, komu byly osobní údaje předány.
  2. V případě, že je podle právních předpisů o ochraně osobních údajů vyžadováno jakékoli oznámení nebo jiný úkon vůči správnímu orgánu, upozorní na tuto skutečnost Dodavatel Objednatele v dostatečném předstihu a v případě, že tím Objednatel Dodavatele pověří a zmocní, zajistí provedení těchto úkonů.
  3. Pokud Dodavatel zjistí, že Objednatel porušuje povinnosti podle právních předpisů o ochraně osobních údajů, zavazuje se Objednatele na tuto skutečnost neprodleně upozornit.
  4. Vznikne-li Objednateli v důsledku nesplnění povinnosti Dodavatele dle právních předpisů o ochraně osobních údajů škoda či jiná újma, zavazuje se Dodavatel Objednateli tuto škodu či jinou újmu v plném rozsahu uhradit. Škodou či jinou újmou vzniklou Objednateli se pro účely tohoto ustanovení rozumí zejména (i) náhrada škody či jiné újmy subjektům údajů ve smyslu právních předpisů o ochraně osobních údajů a (ii) pokuty uložené Úřadem pro ochranu osobních údajů či jiným správním úřadem.
  5. V případě ukončení této Smlouvy se Dodavatel zavazuje předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Dodavatel od Objednatele písemně jiné pokyny, pokud právo Evropské unie nebo členského státu nepožaduje uložení daných osobních údajů.

**Pověření Dodavatele k poskytování součinnosti Objednateli**

* 1. Dodavatel se zavazuje proaktivně poskytovat součinnost Objednateli při výkonu jeho povinností týkajících se práv koncových uživatelů jakožto subjektů údajů, popř. tyto činnosti z části zajistit, a to v následujícím rozsahu:
     1. přijetí žádostí a jejich celková administrace;
     2. ověření identity koncového uživatele;
     3. případná kalkulace ceny za vyřízení žádosti (např. pokud se bude jednat o opakovanou žádost);
     4. prvotní odborné posouzení žádosti;
     5. přeposlání žádosti a návrhu jejího vypořádání Objednateli k potvrzení navrhovaného řešení či k vyřešení žádosti;
     6. následné vyřízení žádosti jménem Objednatele;
     7. v případě, že žádost vyžaduje určitou konkrétní operaci, provedení této operace.
  2. V rámci provádění činností dle odst. 14.14 této Smlouvy se Dodavatel zavazuje postupovat tak, aby mohl Objednatel ověřit kvalitu navrhovaného vyřízení požadavků subjektu údajů, a to zejména s ohledem na čas potřebný k tomuto ověření. Smluvní strany sjednávají, že nejkratší doba, kterou musí Objednatel mít k dispozici pro tento účel, je 5 pracovních dnů.
  3. Činnosti dle odst. 14.14 této Smlouvy budou hrazeny v režimu Doplňkových služeb dle odst. 3.4 této Smlouvy a příslušných příloh, a to dle objednávek Objednatele a skutečně provedených činností; v případě, že některé žádosti se rozhodne Objednatel provádět samostatně, nevznikne ve vztahu k nim Dodavateli právo na úhradu. Pro vyloučení pochybností smluvní strany sjednávají, že Objednatel není povinen tyto služby poptat.
  4. Činnosti dle odst. 14.14 této Smlouvy se vztahují k následujícím právům subjektů údajů:
     1. **Právo na přístup k osobním údajům**. Dodavatel se zavazuje navrhovat odpovědi na přijaté žádosti a tyto odpovědi po potvrzení ze strany Objednatele odesílat koncovým uživatelům. Součástí těchto odpovědí budou v řadě případů i konkrétní osobní údaje vztahující se ke koncovému uživateli subjektu údajů, k jejichž kopii bude nutno koncovému uživateli umožnit přístup;
     2. **Právo na opravu**. Dodavatel se zavazuje vyřizovat žádosti o opravu a informovat o tom koncového uživatele. V případě, že žádost o opravu nebude jednoznačná co do nové požadované verze obsahu záznamu o koncovém uživateli, Dodavatel se zavazuje tuto skutečnost eskalovat k Objednateli; v opačném případě lze Dodavatele pověřit proaktivním řešením žádosti s tím, že Objednatele bude o řešení žádosti průběžně informovat;
     3. **Práva na výmaz a omezení zpracování**. V případě, že žádost nevzbuzuje pochybnosti o její oprávněnosti, Objednatel Dodavatele pověřuje prováděním požadovaných výmazů či zaznamenávání omezení zpracování a následnou komunikací se subjektem údajů. O provedených opatřeních se Dodavatel zavazuje informovat Objednatele. V případě, že žádost vzbuzuje pochybnosti o její oprávněnosti se Dodavatel zavazuje provést eskalaci věci k Objednateli a poskytnout mu nezbytnou součinnost;
     4. **Právo na přenositelnost údajů**. V případě, že žádost nevzbuzuje pochybnosti o její oprávněnosti, Objednatel Dodavatele pověřuje exportováním zpracovávaných údajů a jejich zasíláním koncovému uživateli. O výsledku se zavazuje Dodavatel informovat Objednatele. V případě, že žádost vzbuzuje pochybnosti o její oprávněnosti se Dodavatel zavazuje provést eskalaci věci k Objednateli a poskytnout mu nezbytnou součinnost;
     5. **Právo vznést námitku**. Dodavatel se zavazuje provádět administraci žádosti a technickou realizaci blokování údajů, a to na základě pokynu Objednatele, v jehož kompetenci je vždy posouzení důvodnosti námitky.

**Zabezpečení osobních údajů**

* 1. Dodavatel se zavazuje přijmout a udržovat taková technická a organizační opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.
  2. Dodavatel se zavazuje zajistit, že přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Dodavateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním (dále jen **„pověřené osoby**“). Splnění této povinností zajistí Dodavatel vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou.
  3. Dodavatel se zavazuje vhodným způsobem zajistit, že pověřené osoby budou zpracovávat osobní údaje na základě smlouvy s Dodavatelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Dodavatelem stanoveném a odpovídajícím této Smlouvě a právními předpisy, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.
  4. Dodavatel se zavazuje přijmout a udržovat zejména následující opatření k zajištění úrovně zabezpečení:
     1. zajištění toho, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby;
     2. zajištění toho, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;
     3. pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány;
     4. zabránění neoprávněnému přístupu k datovým nosičům;
     5. schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování – zavedená opatření a jejich korektní fungování budou pravidelně kontrolovány;
     6. schopnost obnovit dostupnost osobních údajů a přístup k nim včas a v případě fyzických či technických incidentů;
     7. proces pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;
     8. antivirovou ochranu a kontrolu neoprávněných přístupů;
     9. šifrovaný přenos dat prostřednictvím IT technologií;
     10. přístup k osobním údajům mají pouze pověřené osoby Dodavatele;
     11. servery s osobními údaji jsou uzamčeny v serverovně.
  5. Při zpracování osobních údajů se Dodavatel zavazuje osobní údaje uchovávat výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat, jedná-li se o osobní údaje v elektronické podobě.
  6. Při zpracování osobních údajů v jiné než elektronické podobě se Dodavatel zavazuje osobní údaje uchovávat v místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby.
  7. Dodavatel se zavazuje na písemnou žádost Objednatele přijmout v přiměřené lhůtě stanovené Objednatelem další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.
  8. V případě zjištění porušení záruk dle odst. 14.19 této Smlouvy se Dodavatel zavazuje zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do 3 pracovních dnů poté, co je k tomu Objednatelem vyzván.
  9. V případě, že Dodavatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu, nejpozději do 24 hodin, Objednateli.

1. OCHRANA INFORMACÍ
   1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků vyplývajících z této Smlouvy:
      1. mohou si vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „důvěrné informace“),
      2. mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejím opominutím přístup k důvěrným informacím druhé smluvní strany.
   2. Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé smluvní strany.
   3. Za třetí osoby podle odst. 15.2 této Smlouvy se nepovažují:
      1. zaměstnanci smluvních stran a osoby v obdobném postavení,
      2. orgány smluvních stran a jejich členové,
      3. ve vztahu k důvěrným informacím Objednatele poddodavatelé Dodavatele,
      4. ve vztahu k důvěrným informacím Dodavatele externí dodavatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s plněním této Smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

* 1. Veškeré informace poskytnuté Objednatelem Dodavateli se považují za důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Dodavatelem Objednateli se považují za důvěrné, pouze pokud na jejich důvěrnost Dodavatel Objednatele předem písemně upozornil a Objednatel Dodavateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat. Pokud jsou důvěrné informace Dodavatele poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), Dodavatel se zavazuje upozornit Objednatele na důvěrnost takového materiálu též jejím vyznačením alespoň na titulní stránce nebo přední straně média.
  2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak než za účelem plnění této Smlouvy.
  3. Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této Smlouvy a příslušné dokumentaci považují výlučně za důvěrné informace Objednatele a Dodavatel se zavazuje tyto informace chránit v souladu s touto Smlouvou. Dodavatel při tom bere na vědomí, že povinnost ochrany těchto informací podle tohoto čl. 15 se vztahuje pouze na Dodavatele, příp. jeho poddodavatele.
  4. Za důvěrné informace Objednatele se dále bezpodmínečně považují veškerá data, která monitorované prostředí ICT Objednatele obsahuje, která do něj mají být, byla nebo budou Dodavatelem, Objednatelem či třetími osobami vložena i data, která z něj byla získána.
  5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
     1. se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající smluvní strany či právních předpisů,
     2. měla přijímající smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
     3. jsou výsledkem postupu, při kterém k nim přijímající smluvní strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
     4. po podpisu této Smlouvy poskytne přijímající smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi,
     5. je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU nebo závazným rozhodnutím oprávněného orgánu veřejné moci,
     6. jsou obsažené v této Smlouvě a/nebo jsou zveřejněné na příslušných webových stránkách dle § 219 ZZVZ.
  6. Za důvěrné informace se ve smyslu odst. 15.8.5 této Smlouvy nepovažují zejména:
     1. ustanovení této Smlouvy včetně jejích příloh,
     2. výše ceny uhrazené za plnění této Smlouvy v jednotlivém kalendářním roce.
  7. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel oprávněn uveřejnit na profilu zadavatele či registru smluv v souladu s § 219 ZZVZ:
     1. tuto Smlouvu včetně všech jejích změn a dodatků,
     2. výši skutečně uhrazené ceny za plnění Veřejné zakázky.
  8. Za porušení povinnosti mlčenlivosti smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst. 15.3 této Smlouvy, které daná smluvní strana poskytla důvěrné informace druhé smluvní strany.
  9. Poruší-li Dodavatel povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací, se zavazuje zaplatit Objednateli uhradit smluvní pokutu ve výši 500.000,- Kč za každé porušení takové povinnosti.
  10. Ukončení smluvního vztahu založeného touto Smlouvou z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku Smlouvy a jejich účinnost včetně ustanovení o sankcích přetrvá bez omezení i po ukončení účinnosti této Smlouvy.

1. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE
   1. Smluvní strany se zavazují vzájemně spolupracovat a předávat si veškeré informace potřebné pro řádné plnění svých závazků vyplývajících z této Smlouvy. Smluvní strany se zavazují vzájemně se informovat o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.
   2. Smluvní strany se zavazují plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením s úhradou jednotlivých peněžních závazků.
   3. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob dle čl. 13 této Smlouvy, statutárních orgánů smluvních stran, popř. jimi písemně pověřených pracovníků.
   4. Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé smluvní straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce této Smlouvy, není-li stanoveno nebo mezi smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost této Smlouvy, připouští se též doručení prostřednictvím datové schránky nebo e-mailu, na čísla a adresy uvedené v Příloze 5 této Smlouvy. Pro vyloučení pochybností se smluvní strany dohodly, že prostřednictvím e-mailu lze doručit zejména připomínky, výhrady či výzvy v souladu s ustanoveními čl. 9 této Smlouvy. Dodavatel je oprávněn komunikovat s Objednatelem prostřednictvím datové schránky. Dodavatel bere na vědomí, že dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, se Objednatel zavazuje v zásadě doručovat veškerou korespondenci právnické osobě, která má zpřístupněnu svou datovou schránku, prostřednictvím datové schránky.
   5. Ukládá-li tato Smlouva doručit některý dokument v písemné podobě, může být doručen buď v tištěné podobě nebo v elektronické (digitální) podobě v dohodnutém formátu, např. jako dokument aplikací Microsoft Office 2021 a vyšší či PDF na dohodnutém médiu apod.
   6. Smluvní strany se zavazují, že v případě změny své poštovní adresy, faxového čísla nebo e-mailové adresy budou o této změně druhou smluvní stranu informovat nejpozději do 5 pracovních dnů.
   7. Dodavatel se zavazuje ve lhůtě 5 pracovních dnů ode dne doručení odůvodněné písemné žádosti Objednatele o výměnu oprávněné osoby Dodavatele dle odst. 13.1.2 této Smlouvy podílející se na plnění této Smlouvy, s níž Objednatel nebyl z jakéhokoliv důvodu spokojen, nahradit jinou vhodnou osobou s odpovídající kvalifikací.
   8. Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.
2. NÁHRADA ŠKODY
   1. Každá ze smluvních stran se zavazuje nahradit způsobenou škodu či jinou újmu v rámci platných právních předpisů a této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
   2. Dodavatel se zavazuje nahradit Objednateli veškeré škody či újmy, způsobené porušením této Smlouvy či povinností uložených Dodavateli dle 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). Dodavatel se zároveň zavazuje Objednatele odškodnit za jakékoliv škody či újmy, které mu v důsledku porušení povinností Dodavatele vzniknou na základě pravomocného rozhodnutí soudu či jiného státního orgánu.
   3. Žádná ze smluvních stran není povinna nahradit škodu či jinou újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytovat všechny části Předmětu plnění s odbornou péčí mohl a měl chybnost takového zadání zjistit, je Dodavatel oprávněn se ustanovení dle předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.
   4. Žádná ze smluvních stran nemá povinnost nahradit škodu či jinou újmu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě škody ve smyslu § 2913 odst. 2 občanského zákoníku.
   5. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě škody bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě škody.
   6. Smluvní strany se dohodly, že omezují právo na náhradu škody, která může při plnění této Smlouvy jedné smluvní straně vzniknout, a to na celkovou částku odpovídající 200 % z celkové částky za poskytování Nástroje PAM po celou dobu trvání této Smlouvy. Ustanovení § 2898 občanského zákoníku není ustanovením dle předchozí věty dotčeno.
   7. Případná náhrada škody bude uhrazena v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku škody.
   8. Každá ze smluvních stran je oprávněna požadovat náhradu škody či jiné újmy i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta či sleva z ceny, a to v celém rozsahu.
3. SANKCE
   1. Smluvní strany se dohodly, že:
      1. v případě překročení limitů nedostupnosti Nástroje PAM stanovených v Technické specifikaci uvedené v Příloze 1 této Smlouvy (sekce Obecné požadavky) se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč za každý jednotlivý případ překročení a 3.000,- Kč za každou započatou hodinu nedostupnosti nad limit stanovený v Technické specifikaci uvedené v Příloze 1 této Smlouvy;
      2. v případě prodlení Dodavatele s poskytnutím Služeb exitu ve smyslu odst. 3.5 této Smlouvy, se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč za každý i započatý den prodlení;
      3. v případě prodlení Dodavatele s vypracováním Exitového plánu nebo v případě prodlení s poskytnutím plnění nezbytných k jeho realizaci do 1 kalendářního měsíce od doručení požadavku Objednatele dle odst. 7.2 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 50.000,- Kč za každý i započatý den prodlení;
      4. V případě, že Dodavatel poruší svoji povinnost reagovat na požadavek Objednatele nebo jím určené třetí strany a zahájit poskytování součinnosti dle odstavce 7.4 této Smlouvy nejpozději do 5 pracovních dnů ode dne doručení takovéhoto požadavku Objednatele, se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení;
      5. v případě porušení povinnosti Dodavatele poskytovat Předmět plnění za účasti členů realizačního týmu a provádět jejich změny pouze se souhlasem Objednatele dle odst. 3.9 této Smlouvy nebo poskytovat Předmět plnění s využitím poddodavatelů uvedených v Příloze 6 této Smlouvy dle odst. 3.10 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč za každé jednotlivé porušení takovéto povinnosti. Ustanovení dle předchozí věty se neaplikuje na pracovníky výrobce Nástroje PAM;
      6. v případě prodlení Dodavatele s dokončením Základní implementace dle Harmonogramu plnění, který je uveden v Příloze 3 této Smlouvy, se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 100.000,- Kč za každý i započatý den prodlení;
      7. v případě porušení povinnosti Dodavatele zahájit poskytování Nástroje PAM po rozšíření dle odst. 6.3 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 25.000,- Kč za každý i započatý den prodlení.
   2. Smluvní strany se dále dohodly, že:
      1. v případě porušení povinnosti Dodavatele stanovené v odst. 5.9 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč za každý i započatý den prodlení, kdy Dodavatel nepředloží originál bankovní záruky;
      2. v případě porušení povinnosti Dodavatele dle odst. 10.2 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč za každý i  započatý den, kdy Dodavatel nepředloží pojistnou smlouvu dle odst. 10.2 této Smlouvy, pojistku potvrzující uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy;
      3. v případě porušení povinnosti Dodavatele dodržet veškeré záruky o technickém a organizačním zabezpečení osobních údajů dle čl. 14 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 10.000,- Kč za každý jednotlivý případ takového porušení;
      4. v případě porušení jakékoliv povinnosti Dodavatele dle čl. 19 této Smlouvy zjištěném při zákaznickém auditu dle odst. 19.5 této Smlouvy se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 20.000,‑ Kč za každý jednotlivý případ porušení;
      5. za každý případ neumožnění anebo odepření provedení kontroly a auditu dle odst. 19.5 se Dodavatel zavazuje uhradit Objednateli smluvní pokutu ve výši 300.000,- Kč za každý jednotlivý případ takového porušení. Ustanovení dle předchozí věty se neaplikuje, pokud je Dodavatel pro poskytování Předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „**ZKB**“).
   3. Smluvní pokuty a/nebo úroky z prodlení jsou splatné 30. den ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší. Slevy z ceny se Dodavatel zavazuje zohlednit při fakturaci, nestane-li se tak, je Objednatel oprávněn slevu z ceny uplatnit písemnou výzvou obdobně jako v případě smluvní pokuty.
   4. Není-li dále stanoveno jinak, uhrazení jakékoliv sjednané smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.
   5. Smluvní pokuty mohou být započteny vůči ceně za poskytnutí Nástroje PAM, kterou se Objednatel zavazuje hradit dle odst. 5.1 této Smlouvy.
4. KYBERNETICKÁ BEZPEČNOST
   1. Dodavatel tímto bere na vědomí, že
      1. Objednatel je správcem informačních systémů kritické informační infrastruktury dle ustanovení § 3 písm. c) ZKB správcem komunikačního systému kritické informační infrastruktury dle ustanovení § 3 písm. d) ZKB a správcem významných informačních systémů dle ustanovení § 3 písm. e) ZKB. Dodavatel dále tímto bere na vědomí, že poskytnutí služeb specifikovaných shora jako Předmět plnění bude prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systémů.
      2. Objednatel považuje Dodavatele za významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
   2. Smluvní strany potvrzují, že rozsah zapojení Dodavatele na zajištění bezpečnosti aktiv informačních a komunikačních systémů kritické informační infrastruktury a aktiv významných informačních systému je určen předmětem této Smlouvy.
   3. Dodavatel prohlašuje, že on i jeho poddodavatelé mají zavedena všechna bezpečnostní opatření, procesy a technologie, které prohlásil za zavedené (odpověděl ANO) v dotazníku pro hodnocení technické úrovně kybernetické bezpečnosti dodavatele, který tvoří Přílohu 10 této Smlouvy (dále jen „**Bezpečnostní** **opatření na straně Dodavatele**“).
   4. Dodavatel se zavazuje v rozsahu plnění této Smlouvy naplnit všechny bezpečnostní požadavky uvedené v Příloze 9 této Smlouvy (dále jen „**Kybernetické požadavky**“) a to do začátku poskytování Nástroje PAM dle odst. 3.1 této Smlouvy.
   5. Dodavatel se zavazuje umožnit Objednateli v roční periodě po dobu trvání smluvního vztahu založeného touto Smlouvou a 1 kalendářní rok po ukončení smluvního vztahu provedení zákaznického auditu (kontroly):
      1. jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Dodavatele, a
      2. jehož předmětem bude naplnění Kybernetických požadavků, Bezpečnostních opatření na straně dodavatele a vyhodnocení rizik dle čl. 3 Přílohy 9 této Smlouvy.
   6. Objednatel je oprávněn při kontrole Kybernetických požadavků a Bezpečnostních opatření na straně dodavatele využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou škodu či jinou újmu.
   7. Dodavatel se zavazuje umožnit Objednateli kontrolu Kybernetických požadavků a Bezpečnostních opatření na straně Dodavatele provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.
   8. Dodavatel se nad rámec poskytování Předmětu plnění zavazuje poskytnout Objednateli součinnost minimálně v rozsahu 10 ČD (1 ČD = 8 pracovních hodin) při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.
   9. Dále se Dodavatel zavazuje nedostatky zjištěné:
      * 1. na základě provedení hodnocení rizik dle čl. 3 Přílohy 9 této Smlouvy nebo
        2. v rámci zákaznického auditu dle odst. 19.5 této Smlouvy

odstranit ve lhůtě určené v písemném oznámení Objednatele nebo ve lhůtě přiměřené.

* 1. Odstavce 19.5 až 19.9 této Smlouvy se neaplikují, pokud je Dodavatel pro poskytování předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB.
  2. Dodavatel se nad rámec čl. 10 této Smlouvy také zavazuje:
     1. Poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků a Bezpečnostních opatření na straně Dodavatele.
     2. Na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Předmětu plnění detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a Bezpečnostních opatření na straně Dodavatele a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.
     3. Neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků a Bezpečnostních opatření na straně dodavatele, které nastanou kdykoli v průběhu trvání smluvního vztahu založeného touto Smlouvou.
     4. Bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků a Bezpečnostních opatření na straně Dodavatele, pokud stávající řešení přestalo být funkční a efektivní.
     5. Po ukončení smluvního vztahu založeného tuto Smlouvou všechna data předat Objednateli a případné kopie na straně Poskytovatele řádně zlikvidovat dle ustanovení Kybernetické legislativy.
     6. Bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit poskytování Předmětu plnění.
     7. Při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům a jejichž následkem může vzniknout škoda či jiná újma nebo nesoulad se zákony nebo obecně závaznými právními předpisy.
     8. Po ukončení smluvního vztahu založeného tuto Smlouvou předat Objednateli všechna data a případné kopie na straně Dodavatele řádně zlikvidovat dle ustanovení Kybernetické legislativy.
  3. Porušení povinností Dodavatele dle odst. 19.11 této Smlouvy je považováno za porušení smluvní povinnosti dle bodu 18.2.4 této Smlouvy a v případě nedodržení Kybernetických požadavků ze strany Dodavatele platí adekvátně ustanovení odst. 18.3 a 18.4 této Smlouvy.

1. PLATNOST A ÚČINNOST SMLOUVY
   1. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Tato Smlouva se uzavírá na dobu určitou v trvání 48 kalendářních měsíců od zahájení poskytování Nástroje PAM dle odst. 4.1.1 této Smlouvy. Pro vyloučení pochybností smluvní strany uvádějí, že Dodavatel je oprávněn poskytnout Služby exitu i před termínem stanoveným dle odst. 4.1 této Smlouvy.
   2. Objednatel je oprávněn bez jakýchkoliv sankcí písemně odstoupit od této Smlouvy v případě:
      1. prodlení Dodavatele s poskytnutím Služeb exitu po dobu delší než 15 pracovních dnů oproti termínu plnění stanovenému ve Smlouvě nebo na základě této Smlouvy, pokud Dodavatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 10 pracovních dnů od doručení takovéto výzvy,
      2. že celková výše smluvních pokut, na jejichž uhrazení by měl Objednatel dle této Smlouvy nárok, dosáhne trojnásobku měsíční ceny za poskytování Nástroje PAM,
      3. porušení povinnosti ochrany důvěrných informací či osobních údajů dle této Smlouvy ze strany Dodavatele,
      4. že nebude schválena částka ze státního rozpočtu, či z jiných zdrojů (např. z EU), která je potřebná k úhradě za plnění této Smlouvy v následujícím kalendářním roce,
      5. Dodavatel do začátku poskytování Předmětu plnění dle odst. 3.1 a 3.2 této Smlouvy a harmonogramu v Příloze 3 této Smlouvy nenaplní všechny Kybernetické požadavky uvedené v Příloze 9 této Smlouvy.
   3. Objednatel je dále oprávněn bez jakýchkoliv sankcí odstoupit od této Smlouvy, pokud:
      1. bylo příslušným orgánem vydáno pravomocné rozhodnutí zakazující plnění této Smlouvy;
      2. na majetek Dodavatele je prohlášen úpadek nebo Dodavatel sám podá dlužnický návrh na zahájení insolvenčního řízení;
      3. dojde k významné změně kontroly nad Dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění dle této Smlouvy a tato změna bude Objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu Kybernetické legislativy;
      4. Dodavatel vstoupí do likvidace; nebo
   4. Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele s uhrazením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 kalendářních dnů, pokud Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 15 pracovních dnů od doručení takovéto výzvy.
   5. Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
   6. Po uplynutí 6 kalendářních měsíců po nabytí účinnosti Smlouvy dle odst. 20.1 této Smlouvy je Objednatel oprávněn tuto Smlouvu písemně vypovědět bez udání důvodů, a to s výpovědní dobou 3 kalendářních měsíců ode dne doručení písemné výpovědi Dodavateli, které počíná běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi.
   7. Výpověď dle odst. 20.6 této Smlouvy může být i částečná a Objednatel je oprávněn tuto Smlouvu vypovídat ve vztahu k jakékoli části plnění Dodavatele.
   8. Ukončením smluvního vztahu založeného touto Smlouvou nejsou dotčena ustanovení Smlouvy týkající se licencí, záruk, práv z vady, povinnosti nahradit škodu či jinou újmu a povinnosti hradit smluvní pokuty, ustanovení o ochraně informací a osobních údajů, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po ukončení smluvního vztahu.
2. ŘEŠENÍ SPORŮ
   1. Práva a povinnosti smluvních stran touto Smlouvou výslovně neupravené se řídí občanským zákoníkem a příslušnými právními předpisy.
   2. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad či platnost a usilovat o jejich vyřešení nejprve smírně prostřednictvím jednání oprávněných osob nebo pověřených zástupců. Tím není dotčeno právo smluvních stran obrátit se ve věci na příslušný obecný soud České republiky.
3. VÝHRADA ROZŠÍŘENÍ PŘEDMĚTU PLNĚNÍ
   1. Objednatel si vyhrazuje právo rozšířit Předmět plnění ve smyslu § 66 a § 100 odst. 3 ZZVZ, a to za podmínek dále sjednaných v tomto článku.
   2. Objednatel může s Dodavatelem sjednat rozšíření Předmětu plnění spočívající v prodloužení doby plnění
      1. poskytování Nástroje PAM, a to nejvýše o 24 měsíců,
      2. Technické podpory, a to nejvýše o 24 měsíců,
      3. Doplňkových služeb, a to nejvýše o 24 měsíců a 150 ČD.
   3. Rozšíření Předmětu plnění bude sjednáno v jednacím řízení bez uveřejnění, které může být Objednatelem zahájeno nejpozději 3 roky od uzavření Smlouvy. Objednatel nemá povinnost využít rozšíření Předmětu plnění.
   4. Bude-li sjednáno rozšíření Předmětu plnění dle tohoto článku, prodlužuje se zároveň doba účinnosti Smlouvy o sjednanou prodlouženou dobu plnění, přičemž veškerá práva a povinnosti Smluvních stran dle Smlouvy se uplatní během takto prodloužené doby plnění, ledaže se Smluvní strany dohodnou jinak. Znamená to zejména zachování povinností Dodavatele vázaných na účinnost, platnost či trvání Smlouvy ve vztahu k prodloužení účinnosti Smlouvy, tedy prodloužená doba plnění Smlouvy dopadá především na dobu poskytování Služeb exitu, povinnost udržovat pojištění odpovědnosti a bankovní záruku, dobu poskytování Nástroje PAM či dobu plnění Kybernetických požadavků.
   5. Rozšíření Předmětu plnění bude provedeno tak, že skutečná cena služeb sjednaných jako rozšíření Předmětu plnění nepřesáhne o více než 30 % jejich předpokládanou hodnotu stanovenou v zadávacím řízení Veřejné zakázky, tj. 22 441 200 Kč bez DPH.
4. ZÁVĚREČNÁ USTANOVENÍ
   1. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy uzavřených v souladu s příslušnými ustanoveními ZZVZ a podepsaných osobami oprávněnými jednat jménem smluvních stran, není-li v této Smlouvě výslovně uvedeno jinak.
   2. Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce smluvních stran.
   3. Dodavatel není oprávněn postoupit peněžité nároky vůči Objednateli na třetí osobu bez předchozího písemného souhlasu Objednatele.
   4. Tato Smlouva je uzavřena elektronicky, tj. prostřednictvím uznávaného elektronického podpisu ve smyslu zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, opatřeného časovým razítkem
   5. Nedílnou součást Smlouvy tvoří tyto přílohy:

|  |  |
| --- | --- |
| [Příloha 1](#Annex01) | Technická specifikace |
| [Příloha 2](#Annex02) | Popis ICT prostředí Objednatele |
| [Příloha 3](#Annex03) | Harmonogram Základní implementace |
| Příloha 4 | Realizační tým Dodavatele |
| [Příloha 5](#Annex05) | Oprávněné osoby |
| [Příloha 6](#Annex06) | Seznam poddodavatelů |
| [Příloha 7](#Annex07) | Cena |
| Příloha 8 | Etický kodex |
| Příloha 9 | Kybernetické požadavky |
| Příloha 10 | Dotazník pro hodnocení technické úrovně kybernetické bezpečnosti |

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

|  |  |
| --- | --- |
| Objednatel  V Praze dne dle elektronického podpisu | **Dodavatel**  V Praze dne dle elektronického podpisu |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Česká republika – Ministerstvo práce a sociálních věcí** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **NTT Czech Republic s.r.o.** |

Příloha č. 1

Technická specifikace nástroje pro řízení privilegovaných účtů a oprávnění

Nástroj PAM, který je poskytovaný dle odst. 3.1 této Smlouvy, musí splňovat všechny níže uvedené požadavky a funkce.

|  |  |
| --- | --- |
| **Základní funkční požadavky** | |
| Řízení přístupů | Účelem nástroje PAM je komplexní centrální evidence a správa privilegovaných osobních, sdílených, servisních a aplikačních účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. |
| Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. |
| Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné. |
| Striktní oddělení přístupových oprávnění | Nástroj PAM plně podporuje striktní oddělení rolí. |
| Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci atp. |
| V nástroji PAM jsou definovatelné minimálně tyto role:   * + - 1. správce/administrátor – má možnost spravovat systém, přidávat uživatele a řídit povolené objekty   administrátor organizační jednotky – tato role bude sloužit k delegaci částí administrátorských oprávnění v rámci nástroje PAM na subjekt/organizační jednotku  c) auditor – má přístup k auditním informacím a nahrávkám d) uživatel – má umožněný přístup k poptávanému řešení a jeho běžné užívání |
| Správce/administrátor nástroje PAM má povolen přístup pouze k vybraným složkám a konfiguraci. |
| Víceúrovňové schvalování přístupů | Nástroj PAM umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu nebo na daný časový úsek. |
| Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu nebo pro připojení na koncový systém. |
| O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému CA, na který bude nástroj PAM integrovaný. |
| Bezpečnostní parametry | Nástroj PAM zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). |
| Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. |
| Nástroj PAM musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům nebo nahrávkám, bez autorizace vlastníků dat. |
| Nástroj PAM jako celek musí být certifikovaný bezpečnostním standardem Common Criteria anebo ekvivalentní certifikaci. |
| Jednotná centrální správa | Správa nástroje PAM je umožněna pomocí jednotné centrální správy. |
| Nástroj PAM musí umožňovat konfiguraci systému pomocí RestAPI – správa uživatelů, zakládání a editace účtů, změny přihlašovacích údajů, terminace spojení atp. |
| Uživatelské rozhraní | Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem MS Authenticator. |
| Po přihlášení je uživateli zobrazen seznam pouze těch privilegovaných účtů, ke kterým má přidělen přístup. Veškeré ostatní privilegované účty zůstávají v systému pro uživatele skryté a nedostupné. |
| **Správa hesel** | |
| Vyhledávání a přidávání privilegovaných účtů | Nástroj PAM umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. |
| Vyhledávání účtů nevyžaduje instalaci agentů na koncová zařízení. |
| Nástroj PAM umožňuje vyhledávání v on-premise i cloud prostředí Azure. |
| Řízení hesel a SSH klíčů | Nástroj PAM umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo) nebo v pravidelných intervalech dle bezpečnostní politiky. Hesla a SSH klíče se vyměňují prostřednictvím bezagentního řešení. |
| Rotaci hesla/SSH klíče lze vynutit i uživatelem. |
| Ověřování hesel | Nástroj PAM kontroluje v pravidelných intervalech shodu uloženého hesla v systému řízení přístupů a cílovém bodu. V případě neshody vynutí synchronizaci nebo zašle upozornění správci. |
| Řízení servisních účtů | Nástroj PAM umožňuje vyhledat účty v MS Windows prostředí a jejich návaznost na další služby/aplikace (services, sheduled tasks, IIS pool, COM+ object,...). |
| Při vynucení změny hesla je heslo propsáno i do navázných služeb. |
| Vyhledání tzv. backdoor účtů a automatický onboarding | Nástroj PAM umožňuje pravidelné vyhledávání účtů, které nejsou nástrojem PAM spravovány, ale jsou používány pro přístupy na koncové systémy. |
| Nástroj PAM takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. |
| Nástroj PAM zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla. |
| Úprava správy hesel | Nástroj PAM musí umožňovat možnost úpravy modulu pro správu hesel tak, aby bylo možné integrovat PAM na další systémy MPSV. |
| Úpravy je možné provádět pomocí nástroje dodávaného výrobcem a případně úpravou konfiguračních souborů. |
| Rotace přihlašovacích údajů na samostatných koncových bodech | Nástroj PAM umožňuje automatickou výměnu hesel privilegovaných účtů na koncových systémech s OS MS Windows, které nejsou standardně připojeny do korporátní sítě. |
| Rotace hesel je vynucena lokálně v pravidelných intervalech dle bezpečnostní politiky. |
| Nástroj PAM zaznamenává a uchovává historii hesel (například poslední tři hesla nebo podle časového období) a umožňuje jednoduchý přístup k historii přes webové rozhraní. |
| Offline přístup k heslům pro uživatele | Nástroj PAM poskytuje možnost správy přihlašovacích údajů i pro stanice a servery na OS MS Windows, které nejsou trvale připojeny do korporátní sítě. |
| Nástroj PAM musí poskytovat mobilní aplikaci pro bezpečný offline přístup k vybraným privilegovaným účtům a jejich přihlašovacím údajům |
| Ověření do aplikace musí být dostatečně silné na bázi biometriky. |
| Mobilní aplikace PAM umožňuje zobrazit hesla i v případě, kdy nemá síťové připojení k nástroji PAM (např. není dostupná mobilní datová síť nebo je PAM nedostupný z internetu). |
| Vyzvednutí hesla z offline klíčenky musí být zaznamenáno a záznam o zobrazení hesla po opětovné konektivitě zaslán do nástroje PAM. |
| **Řízení vzdálených relací** | |
| Izolace relací | Správcovský přístup na cílový systém je zprostředkován pomocí tzv. terminal/jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. |
| Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace - např. MS SQL Management Studio, WinSCP, atp.), uživatel tedy nemá na cílovém systému možnost přístupu k jiným než pro tuto relaci definovaným aplikacím. |
| Po ukončení aplikace se uzavře spojení celé relace. |
| Vzdálené připojení k relaci lze navázat jak přes vlastní GUI nástroje PAM, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. |
| U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS). |
| Izolace SSH relací | Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes SSH Proxy, kde bude uživatel ověřený svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojený zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky |
| Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče). |
| SSH klíče | Nástroj PAM zajišťuje:   * reporting o stavu SSH klíče, jako je jeho platnost, délka klíče apod. Zároveň identifikuje nesoulad s politikou. * bezpečné uchovávní SSH klíče v centrálním zabezpečeném úložišti a zároveň kontrolovat a řídit přístupy k těmto klíčům. * podporovat automatickou výměnu klíčů. Podporuje také rotaci páru SSH klíčů (výměnu privátního a veřejného klíče na cílovém zařízení). * spravovat a chránit SSH klíče, které jsou používané aplikacemi pro autentizaci. * posílat notifikace při použití vybraného SSH klíče.   zabezpečuje správu SSH klíčů a je integrováno do stejné infrastruktury jako zabezpečení privilegovaných účtů a hesel. |
| Dočasně přidělený přístup - Just In Time SSH | Nástroj PAM musí poskytovat funkci časově omezeného přidělení přístupu pro SSH připojení tzv. Just In Time přístup. |
| Nástroj PAM tedy nevynucuje ukládání/onboarding všech lokálních účtů, ale generuje dočasný přístup autorizovaným uživatelům. |
| Nástroj PAM pouze generuje jednorázový přihlašovací token (tzv. short-lived certificate) k vybranému účtu na koncovém systému. |
| Vzdálené připojení pomocí prohlížeče | Nástroj PAM poskytuje možnost vytvářet vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS (není tedy například nutné otevírat z klientské stanice RDP/SSH protokoly); mezi uživatelem a jump serverem bude vždy otevřený pouze bezpečný WebSocket protokol (port 443). |
| Nahrávání relací | Nástroj PAM musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace permanentních agentů na koncový systém. |
| Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. |
| V nahrávkách je možné zpětně vyhledávat v záznamu ve formě metadat – minimálně u RDP spuštěné aplikace a události, u SSH relací jednotlivé příkazy, u webových aplikací click na jednotlivé odkazy, u jiných typů relací alespoň stisky kláves. |
| Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI nástroje PAM. |
| Automatické označení podezřelých aktivit v nahrávkách | Nástroj PAM poskytuje možnost automaticky vyhodnocovat a označovat nahrávky relací. na základě vybraných spuštěných příkazů a aplikací, tak aby bylo možné vyhledávat potenciálně nebezpečné činnosti. |
| Nástroj PAM zároveň umožňuje alerting takových událostí, včetně možnosti exportu logů v reálném čase pomocí syslog na SIEM atp. |
| Pozastavení/terminace relací | Nástroj PAM nabízí možnost automatického pozastavení nebo terminace potenciálně nebezpečných relací. |
| Pravidla pro detekci potenciálně nebezpečných relací je možné plně editovat – typ události, uživatelé (možnost nastavení výjimek na úrovni skupin v AD) a typ reakce. |
| Možnost sledování relací v reálném čase | Nástroj PAM umožňuje sledovat aktivní relace dalším uživatelem (například auditor) a v případě nutnosti ukončit sledovanou relaci. |
| Sledování "živých" relací je také možné pomocí prohlížeče a protokolu HTTPS (není nutné otevírat z klientské stanice RDP protokol). |
| Kontrola relací | Nástroj PAM umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data, uživatele a spuštěného příkazu. |
| Analýza a detekce potenciálně škodlivého chování | Součástí nástroje PAM je nástroj umožňující provádět průběžnou analýzu využívání privilegovaných účtů a následnou detekci potenciálně škodlivého chování – uživatel se připojuje z nestandardní IP, uživatel se připojuje na systémy, na které běžně nemá přístup, uživatel používá privilegovaný přístupy v nestandardní časy apod. |
| Detekce a blokování podezřelých aktivit | Nástroj PAM umožňuje detekci podezřelých aktivit chování uživatelů v reálném čase a musí umožňovat automatické vynucení nápravných opatření – alerting, změna přihlašovacích údajů, terminace/pozastavení relací. |
| **Bezpečný vzdálený přístup** | |
| Spojení bez VPN | Nástroj PAM umožňuje připojit vzdáleného uživatele k cílovému systému privilegovaným účtem okamžitě na vyžádání přes PAM – bez nutnosti vystavovat uživateli VPN, zavádět ho do Active Directy a distribuci druhého faktoru. |
| Při takto zvoleném vzdáleném přístupu musí být zachovaná vysoká bezpečnost  - šifrované spojení od uživatele k PAM  - silné ověření do PAM  - autorizace v PAM pouze na vybraný cílový systém a cílový účet. |
| Okamžité zavedení uživatelů do systému | Nástroj PAM umožňuje okamžité zavedení nových uživatelů do systému. |
| Správce nástroje PAM dokáže přes webové rozhraní vytvořit uživatele, přiřadit mu oprávnění s jakými privilegovanými účty může disponovat a pro jaké časového období. |
| Nástroj PAM následně zašle email novému uživateli a umožní mu do nástroje bezpečné vzdálené připojení. |
| Vícefaktorová autentizace | Před bezpečným vzdáleným připojením uživatele k nástroji PAM je uživatel ověřen pomocí druhého faktoru. |
| Šifrované spojení | Spojení mezi externím uživatelem a nástrojem PAM musí být plně šifrované. |
| Není umožněno přímé spojení mezi stanicí uživatele a cílovým systémem – je využit princip bezpečného 'jump' serveru. |
| Bezagentní řešení | Nástroj PAM nevyžaduje instalaci agenta na stanice uživatelů a na cílové systémy. |
| Uživatelům je umožněno bezpečně přistupovat pomocí webového prohlížeče do nástroje PAM bez nutnosti VPN, pouze s druhým faktorem. |
| **Vícefaktorová autentizace** | |
| MFA | Součástí nástroje PAM musí být i vlastní systém pro vícefaktorové ověření uživatelů. |
| MFA - autentizační mechanismy | Nástroj PAM musí podporovat alespoň následující metody autentizace: SMS, email, push do mobilní aplikace, telefonní hovor, jednorázové heslo (OTP), bezpečnostní otázka, autentizace pomocí QR kódu. |
| Pokročilé nastavení MFA pro PAM | Nástroj PAM musí umožňovat pokročilá nastavení MFA ověření pro přístupy k PAM formou autentizačních profilů, které se budou automaticky vynucovat podle a) definovaných pravidel (uživatel se k PAM připojuje mimo běžné pracovní hodiny/připojení z důvěryhodných lokalit/vybraného webového prohlížeče/důvěryhodného zařízení = vynucení silnějšího ověření) NEBO b) na základě behaviorální analýzy a vyhodnocení rizikovosti uživatele. |
| **Audit a reporting** | |
| Zobrazení aktivit uživatele | Nástroj PAM musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty – zobrazení hesla, změny uložených údajů, vytvoření relace. |
| Audit administrátorských akcí | Nástroj PAM musí umožňovat vygenerování reportu veškerých aktivit administrátora nástroje. |
| Typy reportů | Nástroj PAM disponuje vlastními předdefinovanými reporty o aktivitách uživatelů a auditech používání spravovaných přihlašovacích údajů. Podporuje plánování automatického generování těchto reportů:   * Oprávnění uživatelů * Aktivity uživatelů * Přehled privilegovaných účtů * Přehled činností konkrétního uživatele * Přehled přístupů dle konkrétního koncového bodu |
| Přístup k reportům | Nástroj PAM umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele. |
| Export auditních dat | Nástroj PAM musí umožňovat export auditních záznamů pro nástroje typu Crystal reports atp. |
| Nezpochybnitelný auditní záznam | Nástroj PAM zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. |
| Zabezpečení auditních záznamů | Nástroj PAM musí umožňovat nesmazatelnost logů po dobu minimálně 30 dní. |
| Auditní záznamy musí být bezpečně uloženy v zašifrované podobě, tak aby k nim měl přístup pouze oprávněný uživatel nástroje PAM. |
| Monitoring pomocí RestAPI | Nástroj PAM umožňuje monitoring jednotlivých komponent pomocí RestAPI – integrace s monitoring systémy MPSV. |
| Pravidelná recertifikace přístupů k PAM | Nástroj PAM musí poskytovat nástroj pro pravidelnou recertifikaci přístupů ke spravovaným privilegovaným účtům. |
| Správce PAM/vlastníci účtů/auditor/případně další role v nástroji PAM mohou v pravidelných intervalech vyhodnocovat přidělená oprávnění a potvrdit nebo zamítnout přístupy uživatelů pomocí webové konzole. |
| **Podporované platformy a integrace** | |
| Podpora systémů MPSV | Nástroj PAM musí umožňovat správu privilegovaných účtů minimálně pro následující systémy a technologie:  - Všechny aktuálně podporované verze Microsoft Windows (32-bit, 64-bit)  - Všechny aktuálně podporované verze Microsoft Windows Server (32-bit, 64-bit)  - Všechny enterprise distribuce Linux (Debian, Ubuntu, Red Hat, SuSE Linux Enterprise server, CentOS, Rocky linux)  - Všechny aktuálně podporované verze Apple macOS (OS X, MAC OS X)  - Active Directory  - HP iLO  - Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+  - VMWare, HyperV, Citrix  - MS SQL, MySQL, PostreSQL, Oracle  - Checkpoint, Fortinet, Palo Alto, Symantec  - Cisco, Juniper, F5, HP, Blue Coat  - Office 365, Microsoft Azure Application Keys |
| Nástroj PAM musí umožňovat konfiguraci a vývoj vlastních konektorů pro změnu hesel a vzdálených přístupů. |
| Podpora MS Active Directory | Nástroj PAM nabízí plnou integraci s Microsoft Active Directory na úrovni informací o uživatelích, příslušnosti ke skupinám a emailech. |
| Integrace musí umožňovat mapování rolí v nástroji PAM v návaznosti na skupiny v AD. |
| MFA - vícefaktorová autentizace | Nástroj PAM musí poskytovat vlastní nástroj na vícefaktorovou autentizaci uživatelů, minimálně prostřednictvím PUSH notifikace, OTP anebo SMS klíčem pro všechny uživatele systému PAM. |
| Nástroj PAM musí podporovat integraci s nástroji třetích stran pro vynucení vícefaktorové autentizace minimálně na úrovní LDAP/S, SAML, RADIUS, PKI, OIDC. |
| Správa nástroje PAM pomocí Rest API | Nástroj PAM je možné spravovat pomocí Rest API, a to minimálně na úrovni – vytváření uživatelů a účtů, nastavení oprávnění, změny politik, system health monitoring, schvalování požadavků, autentizace atp. |
| Integrace s dalšími nástroji | Nástroj PAM musí umožňovat integraci se SIEM a odesílat auditní záznamy do bezpečnostního dohledu Objednatele, viz Standard bezpečnostního dohledu (součást Přílohy 2). |
| Nástroj PAM musí umožňovat integraci s nástroji HSM a ukládat šifrovací klíče k databázi do HSM Thales 750, které má Objednatel ve svém ICT prostředí. |
| Nástroj PAM musí umožňovat integraci s ticketing nástroji třetích stran – žádost o schválení přístupu, přístup na základě existujícího ticketu apod. |
| Nástroj PAM musí být integrovatelný na CA Service Desk, který provozuje Objednatel. Integrace je součástí Základní implementace provedené dle odst. 3.3 této Smlouvy. |
| Veřejně dostupný seznam podporovaných systémů | Výrobce musí poskytovat veřejně dostupný (ideálně URL na veřejnou webovou stránku) seznam integrovaných řešení na úrovni Password Management, Remote Session Management, SIEM apod. |
| **Architektura nástroje PAM** | |
| Architektura řešení | Veškeré komponenty (pro HA i DR) musí splňovat nároky na vysoké zabezpečení a automaticky vynucovat tzv. hardening. |
| Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent nástroje PAM. |
| Bezpečné úložiště musí být instalovatelné na fyzický – nevirtualizovaný – hardware, aby byla zajištěna možnost přístupu k zabezpečeným datům i v případě nedostupnosti virtuálního prostředí. Ostatní komponenty řešení musí být nainstalované z bezpečnostních a provozních důvodů na jiném systému, než je bezpečné úložiště. |
| Databáze dat je součástí nástroje PAM a není nutné využívat nástroje třetích stran. |
| Vysoká dostupnost nástroje PAM | Nástroj PAM musí podporovat nasazení ve vysoké dostupnosti a vlastní technologické možnosti (nejsou používány nástroje/SW třetích stran) pro zabezpečení High Availability, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat. |
| Disaster recovery a HA proces je plně automatický a není závislý na nástrojích třetích stran (MS cluster atp.). |
| Všechny komponenty nástroje PAM jsou redundantní, aby byla zajištěna geo-redundance (minimálně active-passive) ve dvou datových centrech Objednatele. |
| Zálohování systému | Nástroj PAM musí umožňovat bezpečné zálohování dat systému – zálohy musí být šifrované a přístup k zálohovaným datům je umožněn pouze pomocí zabezpečených Disaster Recovery klíčů. |
| Automatická instalace | Veškeré komponenty nástroje PAM musí umožňovat automatickou instalaci v cloud i on-premise prostředí. |
| Nástroj PAM minimálně poskytuje skripty pro kopírování instalačních souborů, instalaci pre-requisite, instalaci komponent, hardening a základní konfiguraci. |
| Automatickou instalaci je možné řešit například pomocí Ansible roles. |
| Testovací prostředí | Licence zároveň pokrývá možnost instalace dvou separátních testovacích prostředí s plnou funkčností a v plném rozsahu. |
| Šifrování a zabezpečení dat | Nástroj PAM musí splňovat standard FIPS 140-2 a šifrovací algoritmy minimálně na úrovni AES-256 a RSA-2048. |
| **Řízení přístupů běžných administrátorů** | |
| Řízení přístupů k webovým aplikacím | Nástroj PAM musí poskytovat zabezpečení přístupu k webovým aplikacím pomocí SSO integrací a nebo vkládaní jména a hesla do webových aplikací. |
| Web portál | Uživatel má k dispozici webový portál s SSO integracemi aplikací anebo položky jména a hesla pro URL |
| Ověření uživatele | Pro autentizaci k webovému portálu se používá jméno + heslo a vynucení vícefaktorového ověření. |
| Podporované integrace – SSO | Nástroj PAM musí podporovat minimálně následující SSO integrace: - Browser plugin - NTLM - Basic auth - Client Oauth2 - Server Oauth2 - OpenID Connect - SAML - Uživatelské jméno a heslo |
| Password Manager pro neprivilegované účty | Nástroj PAM poskytuje centrálně spravovaný nástroj pro ukládání hesel, poznámek a dalších údajů pro běžné (neprivilegované) uživatele. |
| Nástroj PAM umožňuje bezpečné uložení a případné sdílení uložených dat s vybranými uživateli individuálně anebo příslušnosti ke skupině |
| Přístup k uloženým heslům, poznámkám apod. je možný přes webové rozhraní nebo mobilní aplikaci. |
| Integrace Password Manager s PAM | Nástroj PAM musí poskytovat možnost ukládání hesel běžných uživatelů do centrálního PAM systému. |
| Aplikační brána | Nástroj PAM musí poskytovat funkci tzv. aplikační brány, která uživatelům umožňuje připojení k webovým aplikacím ve vnitřní síti bez nutnosti připojení přes VPN z vlastního zařízení. |
| Před připojením je uživatel ověřen. |
| Způsob nasazení | Při publikování interní webové aplikace pro přístup bez nutnosti použití VPN není nutné upravovat danou aplikaci. |
| Přístup do nástroje PAM je možné poskytnout buď na stávající URL nebo na vygenerováním unikátního řetězce. |
| **Řízení aplikačních a technických účtů** | |
| Řízení aplikačních a technických účtů | Nástroj PAM poskytuje zabezpečení aplikačních a technických privilegovaných účtů a jejich přihlašovacích údajů. |
| Nástroj PAM umožňuje odstranění tzv. hard-coded přihlašovacích údajů ze skriptů, konfiguračních souborů a aplikací. |
| Nástroj PAM musí umožňovat různé API pro bezpečné vyzvedávání přihlašovacích údajů pro aplikace a skripty. |
| Nástroj PAM musí poskytovat vlastní SDK, minimálně pro Java, .NET, C/C++ a CLI. |
| Bezpečná autentizace aplikací | Nástroj PAM musí umožňovat silnou autentizaci skriptů a aplikací pro vyzvedávání přihlašovacích údajů, a to minimálně na úrovni – hostname/IP adresa aplikačního serveru, certifikátu uživatele, pod kterým je aplikace/skript spuštěna, cesty k aplikaci, případně MD5 hash. |
| Lokální cache | Nástroj PAM umožňuje poskytování přihlašovacích údajů aplikacím a skriptům pomocí agentního řešení, které obsahuje možnost bezpečné cache. |
| V případě síťového výpadku bude aplikace/skript mít stále k dispozici přihlašovací údaje k privilegovanému účtu. |
| Bezagentní řešení | Pro méně kritické aplikace a skripty systém umožňuje vyzvednutí přihlašovacích údajů pomocí webového volání přes RestAPI - bez nutnosti instalovat agenta na koncový systém. |
| Webový server musí umožňovat vynucení autentizace volání minimálně na úrovni hostname/IP adresa aplikačního serveru a certifikátu. |
| Vulnerability Scanners – RPA – Orchestration/Response | Pro automatické a bezpečné vyzvedávání secrets pomocí API rozhraní musí nástroj PAM umožňovat plnou integraci s nástrojem Qualys, který Objednatel využívá k řízení technických zranitelností ve svém ICT prostředí. |
| Veřejně dostupný popis API a SDK | Výrobce musí poskytovat veřejně dostupný (URL na veřejnou webovou stránku) popis jednotlivých API a SDK pro konfiguraci skriptů a aplikací. |
| **Řízení aplikačních účtů pro DevOPS** | |
| Správa secrets pro DevOPS | Nástroj PAM umožňuje centrální správu účtů, hesel, klíčů a dalších typů tzv. secrets v prostředí agilního vývoje aplikací dle metodiky DevOps. |
| Nástroj PAM musí poskytovat možnosti bezpečného uložení, vyzvednutí a rotace secrets pro aplikace, mikroslužby, kontejnery a CI/CD nástroje jako jsou – Jenkins, Ansible, Puppet, Terraform, Kubernetes, OpenShift, WMware Tanzu, Spring Boot, atp. |
| Možnosti nasazení | Nástroj PAM musí být možné instalovat jako kontejner (Docker, Podman, atp.). |
| Bezpečná autentizace aplikací | Nástroj PAM musí poskytovat možnosti identifikace, autentizace a autorizace pro vyzvednutí secrets z centrálního repositáře. Minimálně musí podporovat tyto možnosti: - API Klíč, - Certifikát, - IAM role v Azure/AWS, - Dočasný access token generovaný v rámci dynamického procesu spuštění aplikace/kontejneru/mikroslužby, - JWT autentizace, - Pro platformy Kubernetes/OpenShift je nutná podpora autentizace aplikace na základě názvu Podu, Namespace, Stateful set, servisního účtu, atd. |
| Vyzvedávání secrets | Nástroj PAM musí poskytovat minimálně některé z následujících mechanismů pro vyzvednutí secrets: - API (podpora pro: Ruby, GO, Java, .Net) - Vložení do Environment Variable,  - Pomocí tzv. proxy, která umožní bezpečné vyzvednutí secrets a vzdálené připojení |
| Správa politik přes API a CLI | Nástroj PAM umožňuje vytváření a správu politik v kódu 'Security as a code'. |
| Synchronizace s PAM | Nástroj PAM synchronizuje všechny secrets a své logy a umožňuje tak centrální správu, rotaci hesel v DevOPS prostředí a auditní stopu. |
| **Řízení privilegovaných přístupů pro správu cloud služeb v Microsoft Azure** | |
| Jednorázové přidělování privilegovaných přístupů – Just In Time | Nástroj PAM umožňuje vytváření pravidel pro přidělování jednorázových přístupů s vyšším/privilegovaným oprávněním k portálu Microsoft Azure. |
| Nástroj PAM umožňuje vynutit koncept tzv. Least Privilege – uživatel nepotřebuje stále přidělená privilegovaná oprávnění, ta jsou přidělena pouze pro aktivní relaci a silně ověřeného uživatele. |
| Silné ověření uživatelů | Uživatel je před přidělením oprávnění a spuštěním aktivní relace bezpečně ověřen – podpora dodaného IDP nebo nástroje třetích stran. |
| Podpora nativního připojení | Uživatel se může připojit přímo ze své pracovní stanice pomocí webového prohlížeče nebo cloud CLI. |
| Nezpochybnitelný auditní záznam | Nástroj PAM vynucuje plný auditní záznam jednotlivých aktivit a operací uživatele. |
| Auditní stopa obsahuje i grafickou nahrávku ve formě záznamu obrazovky a jednotlivých aktivit. |
| **Řízení aplikačních účtů v Microsoft Azure Key Vault** | |
| Centrální Secrets Management | Nástroj PAM umožňuje centrální správu aplikačních účtů/secrets v cloud i on-prem prostředí. |
| Synchronizace s PAM | Nástroj PAM synchronizuje vybrané secrets uložené v Azure Key Vault s nástrojem PAM a umožňuje tak centrální správu, včetně rotaci secrets v Azure prostředí. |
| Jednotná auditní stopa | Nástroj PAM poskytuje auditní záznam a monitoring přístupů k secrets a případné vyhodnocení neobvyklého chování. |
| **Řízení účtů na koncových zařízeních** | |
| Řízení privilegií na koncovém zařízení | Nástroj PAM umožňuje řízení oprávnění uživatelů na koncových zařízeních (OS platformy Windows, MacOS a Linux), tak aby bylo možné granulárně definovat, který příkaz, aplikaci a akci je uživatel schopný spustit a pod jakými oprávněními. |
| Schvalování privilegovaných činností | Nástroj PAM je schopné vynutit autorizaci (zadání důvodu, schvalování) pro každý úkon, který vyžaduje vyšší oprávnění, jako je spuštění aplikace vyžadující vyšší oprávnění, konfigurace systému, editace systémových nastavení atp. |
| Odstranění práv lokálního administrátora | Nástroj PAM umožňuje, aby uživatel na koncovém zařízení, ať se jedná o uživatelské pracovní stanice, notebooky nebo servery, mohl pracovat pouze pod standardním neprivilegovaným uživatelským oprávněním. |
| Veškeré požadavky na vyšší oprávnění jsou řízeny podle stanovené bezpečnostní politiky. |
| Oprávnění jsou následně povyšována jednorázově pro vybrané aktivity. |
| Přidělení oprávnění pro vybrané aplikace | Administrátor nástroje PAM může centrálně definovat, jaké aplikace budou spuštěny se standardním oprávněním, a které se budou spouštět s vyšším oprávněním. |
| Nástroj PAM musí umožnit běžným (neprivilegovaným) uživatelům bezproblémovou práci se standardními prostředky a zároveň zajistit maximální bezpečnost systému. |
| Dočasné povýšení oprávnění – Just In Time Windows | Nástroj PAM umožňuje dočasné povýšení oprávnění běžných (neprivilegovaných) uživatelů na úroveň administrátora (lze vybrat lokální skupinu pro přidělení oprávnění) na koncových systémech na platformě Microsoft Windows bez nutnosti instalace agentního řešení. |
| Nástroj PAM umožňuje povýšení oprávnění na základě požadavku, příslušnosti do AD skupiny, případně na časově omezené období. |
| Oprávnění jsou následně automaticky odebrána po předem definovaném intervalu. |
| Monitoring spuštěných aplikací | Nástroj PAM dokáže monitorovat spuštěné aplikace na koncových systémech a na základě monitoringu vytvářet politiky, které aplikace následně systém umožní na koncových bodech spustit a které nikoliv. |
| Omezení oprávnění neznámých aplikací | Nástroj PAM umožňuje spuštění neznámých aplikací na koncových bodech, ale v omezeném režimu tím, že - omezí práva, pod kterými je aplikace na koncovém zařízení spuštěna - omezí přístup k síťovým zdrojům - omezí přístup na internet. |
| Zabezpečení přihlašovacích údajů na koncovém zařízení | Nástroj PAM umožňuje detekci a blokování aktivit, které vedou ke zcizení přihlašovacích údajů uživatelů na koncových bodech. |
| Nástroj PAM poskytuje zabezpečení minimálně na úrovni ochrany Windows credentials (SAM, LSASS, LSA, NTDS.dit), přihlašovacích údajů uložených v cache prohlížečů (Edge, Chrome, Firefox), přihlašovacích údajů uložených v různých nástrojích pro vzdálenou správu (WinSCP, VNC, Putty,...) a případně dalších standardních nástrojích (Git, Total Commander,...). |
| **Technická podpora dodavatel a výrobce nástroje PAM** | |
| Síť certifikovaných partnerů na lokálním trhu | Výrobce garantuje síť certifikovaných partnerů na lokálním trhu, kde je zaručena technická znalost řešení, zkušenosti s implementací a řízením projektů PAM. |
| Konzultační služby | Výrobce poskytuje vlastní konzultační služby v rámci projektů implementace nástroje PAM. |
| V rámci služeb jsou poskytovány konzultace a best practices ohledně zabezpečení privilegovaných účtů, vedení PAM projektů a postupná analýza aktuálního stavu zabezpečení MPSV. |
| Implementační služby | Výrobce poskytuje vlastní implementační služby v rámci projektů implementace nástroje PAM na lokálním trhu. |
| PAS Assessment | Výrobce poskytuje metodiku, včetně odborných konzultací, který umožňuje pravidelné vyhodnocení zabezpečení privilegovaných účtů v prostředí MPSV, vzhledem k předem definovaným rizikům. |
| Celý koncept PAS Assessment nástroje umožňuje porovnání aktuálního stavu s anonymními údaji ostatních zákazníků i v jiných zemích. |
| Program zabezpečení privilegovaných účtů | Výrobce poskytuje metodologii postupného zabezpečení privilegovaných účtů, včetně osobních konzultací na lokálním trhu. |
| Metodologie popisuje základní témata a rizika svázaná s oblastí privilegovaných přístupů do IT infrastruktury a zároveň navrhuje patřičná nápravná opatření. |
| Discovery tool | Výrobce poskytuje zdarma nástroj na vyhledání privilegovaných účtů v prostředí MPSV a s nimi svázaných zranitelností. Zároveň poskytuje vlastní konzultační služby pro vyhodnocení a před-implementační podporu. |
| On line dokumentace | Nástroj PAM disponuje online dokumentací ke všem modulům. |
| Technická podpora dodavatele poskytovaná dle odst. 3.3 | Dodavatel musí zajistit technickou podporu:   * V pracovní dny v době 8-18 hod v českém jazyce (email, telefon) / SLA 2 hodiny * Garantovanou výrobcem 24x7x365 minimálně v anglickém jazyce / SLA 4 hodiny |
| Jako součást pořízení Nástroje PAM musí být zajištěno školení minimálně pro 5 osob, provedené v českém jazyce a v minimálním rozsahu 2 dny (2 x 6 hodin). |
| **HW zajištěný Objednatelem a prostor pro HW Dodavatele** | |
| Objednatel zajistí pro provoz nástroje PAM následující prostředky virtualizační platformy:   * 500 vCPU * 1 TB RAM * 10 TB SSD   Parametry jsou maximální možné a Objednatel je bude uvolňovat podle potřeby Nástroje PAM. | |
| Objednatel umožní umístit do svých datových center HW (appliance) pro provoz nástroje PAM, který bude plně ve správě Dodavatele. | |
| Objednatel pro HW Dodavatele poskytne umístění v racku, elektrickou energii a konektivitu do svého prostředí a na internet. | |

Příloha č. 2

Popis ICT prostředí Objednatele

*neveřejný údaj*

Příloha č. 3

Harmonogram Základní implementace

|  |  |  |
| --- | --- | --- |
| Činnost | Výstup / Akceptační kritérium | Délka trvání dílčí fáze plnění (počet pracovních dnů) |
| Návrh architektury nástroje PAM a zpracování před-implementační analýzy | Je dokončený a Objednatelem akceptovaný dokument ve struktuře a s obsahem, který je specifikován dále v této příloze. | 130 |
| Příprava ICT prostředí na straně Objednatele | Připravené virtuální servery, konektivita, prostupy a další zdroje pro zprovoznění nástroje PAM | ------  (termín je závislý na Objednateli) |
| **Poskytnutí licencí nástroje PAM**  **FAKTURAČNÍ MILNÍK 1** | **Objednatel má k dispozici počet účtů a konektorů požadovaných v rámci Základní implementace** | **5** |
| Integrace s AD/LDAP, prostupy | Nástroj PAM je integrovaný s AD/LDAP a rozděleny přístupy a role | 35 |
| Integrace s dalšími infrastrukturní systémy | Systém je integrován se systémy:   * SIEM * NTP * HSM * Load balancing * PKI * SMTP | 20 |
| Základní implementace v rozsahu odst. 6.1 této smlouvy | Nástroj PAM řídí všechny privilegované účty, přístupy a oprávnění minimálně v rozsahu Základní implementace dle odst. 6.1 | 250 |
| Nastavení reportingu | Jsou funkční reporty v souladu s technickou specifikací v Příloze 1 | 4 |
| Testování Nástroje PAM | Nástroj PAM je otestovaný a plně funkční dle předem schválených akceptačních scénářů | 40 |
| Plán obnovy po havárii (DRP) | Je dokončený a Objednatelem akceptovaný dokument ve struktuře a s obsahem, který je specifikován dále v této příloze. | 25  *(Praktické provedení obnovy bude provedeno v dohodnutém termínu až po ukončení Základní implementace, tzn. že testování DRP není součástí tohoto kroku)* |
| Úprava a doplnění řídící dokumentace Objednatele | Aktuální řídící dokumentace v elektronické podobě (DOCx, XLSx…), včetně dokumentace skutečného provedení a příruček jsou dokončené a Objednatelem akceptované a jsou ve struktuře a s obsahem, který je specifikován dále v této příloze. | 34 |
| Školení max. 5 pracovníků Objednatele | Realizace on-site školení pro interní a externí pracovníky MPSV v rozsahu max. 8 hodin | 4 |
| **Akceptace základní implementace**  **FAKTURAČNÍ MILNÍK 2** | **Plně funkční Nástroj PAM v rozsahu Základní implementace** | **2**  **Součet 549**  *(hodnotící kritérium - součet všech výše uvedených dílčích částí plnění)* |
| Aktivace podpory poskytované dle odst. 3.3 | Je aktivována Technická podpora | ------ |

Do počtu dnů nebudou započteny dny, které Objednatel stráví revizí a formálním schvalováním výstupů a dny čekání na vstupy od Objednatele, tzn. dny, jejichž počet Dodavatel nemůže ovlivnit. Všechny dokumenty po jejich dokončení projdou akceptací dle odst. 9.2.

Krok: Návrh architektury nástroje PAM a zpracování před-implementační analýzy

Dodavatel v rámci prvního kroku Základní implementace provede analýzu a návrh celkové koncepce používání, správy a řízení privilegovaných účtů, které budou do Nástroje PAM připojeny. V rámci této aktivity bude provedeno několik workshopů s pracovníky Objednatele, kdy dojde k vysvětlení aktuálních procesů nakládání s privilegovanými účty a vysvětlení technologického zázemí MPSV. Dodavatel navrhne optimální způsob, jak různé typy privilegovaných účtů řídit a spravovat a toto řešení udržovat efektivní v čase.

Dodavatel zpracuje dokument, který bude v následující struktuře a bude minimálně obsahovat:

1. Architektura nástroje PAM
   1. Základní popis nástroje PAM, technologií a technických konceptů.
   2. Obecné technické předpoklady a požadavky na realizaci nástroje PAM.
   3. Architektura nástroje PAM s jejím vysvětlením.
   4. Procesy a služby systému s jejich rozpisem a vysvětlením jejich účelu v rámci nástroje PAM.
   5. Popis systémů třetích stran a jejich integrace.
   6. Integrační architektura se systémy MPSV (bezpečnostní dohled, AD, SMTP, NTP atd.).
   7. Popis nakládání s daty, jejich uložení, zabezpečení, ochrana.
   8. Detailní síťový a komunikační model nástroje PAM včetně interní komunikace mezi vnitřními prvky nástroje PAM.
   9. Návrh politik nástroje PAM detailně specifikovaných během analýzy a vycházející z „best practice“ doporučení výrobce technologie.
   10. Technologické požadavky na zajištění provozu.
   11. Popis konfigurace komponent nástroje PAM.
   12. Detailní popis instalačních postupů, a to včetně testovacího prostředí.
   13. Detailní popis zálohování a obnovy nástroje PAM, řešení DR scénářů včetně návrhů testovacích scénářů zahrnujících totální výpadek a obnovy do provozního stavu (bude součástí akceptačních testů).
   14. Popis způsobů aktualizace nástroje PAM (všechny části PAM).
   15. Monitoring nástroje PAM.
2. Implementace nástroje PAM
   1. Návrh harmonogramu projektu a procesních kroků pro implementaci nástroje PAM včetně návrhu konfigurace nástroje PAM v jednotlivých fázích implementace a definice finální podoby dodávaného nástroje PAM.
   2. Popis náběhu systému (popis pilotní/zkušební fáze až do doby akceptace).
   3. Postup testování a testovacích scénářů.
   4. Akceptační kritéria včetně postupu akceptace.
   5. Požadavky na součinnost MPSV.
   6. Detailní specifikace lokální podpory vybraného dodavatele potažmo výrobce a definování postupů pro její využití.
   7. Specifikace a rozsah školení pracovníků MPSV (v rozsahu standardizovaných školení administrátorů od výrobce technologie).
   8. Návrh automatizovaného discovery procesu privilegovaných účtů po zavedení PAM.
   9. Návrh na provádění analýz nástroje PAM (četnost, rozsah, hlavní oblasti assesmentu, automatizace assesment procesu, scoring apod.).
   10. Návrh procesu technické profylaxe nástroje PAM (musí probíhat minimálně jednou ročně) ze strany vybraného dodavatele, případně za součinnosti s výrobcem.

Krok: Plán obnovy po havárii (DRP)

Dokument bude obsahovat detailní model pro break-glass účty a scénáře pro obnovu nástroje PAM po havárii (Disaster Recovery Plan). Dodavatel zpracuje nový interní akt řízení, který bude v následující struktuře a bude minimálně obsahovat:

1. Scénáře obnovy po havárii
   1. Kompletní výpadek celého nástroje PAM
   2. Výpadek některého ze základních systémů, např. virtualizační platforma
   3. Výpadek konektivity na některé ze základních prvků PAM
   4. Selhání některého z prvků PAM a doporučený postup pro jeho zálohování a obnovu
   5. Výpadek bezpečného úložiště dat včetně fatálního výpadku, jak primárního, tak sekundárního nodu
   6. Výpadek webového portálu a scénáře pro přístup k úložišti dat
   7. Výpadek konektivity v prostředí MPSV a řešení přihlašování privilegovaných uživatelů
   8. Výpadek přístupu administrátorů k síťovým prvkům (je nutné se k nim připojovat pomocí lokálního fyzického připojení privilegovaným účtem)
2. Doporučené postupy pro nasazení break-glass účtů:
   1. Způsob úschovy
   2. Periodicita změn
   3. Nakládání s nimi
3. Návrh scénářů pro otestování postupů obnovy

Krok: Úprava a doplnění řídící dokumentace Objednatele

Dodavatel aktualizuje stávající řídící akty nebo zpracuje nový interní akt řízení, který bude v následující struktuře a bude minimálně obsahovat:

1. Vytvoření nového uživatele v PAM – Založení nového účtu na úrovni nástroje PAM pro uživatele PAM (např. interní/externí administrátor, správce PAM, auditor, popř. další subjekty)
2. Zrušení uživatele PAM – Zrušení účtu na úrovni nástroje PAM v případě, že účet není nadále používán (např. v případě ukončení zaměstnaneckého poměru zaměstnance u MPSV, odebrání účtu externího dodavatele apod.).
3. Dynamické přidělování/odebírání licencí pro externí uživatele PAM – Návrh postupu dynamického přidělování/odebírání licencí externích uživatelů, který bude optimalizován podle maximálního počtu souběžně připojených externích uživatelů PAM a povede k efektivnímu využití licencí externích uživatelů PAM.
4. Přidělení/odebrání role uživateli PAM – Přidělení/odebrání role (např. správce PAM, uživatel, auditor) uživateli PAM.
5. Přidání nového privilegovaného účtu do PAM – Přidání privilegovaného účtu do PAM (např. v případě objevení nového privilegovaného účtu, který má být spravován pomocí PAM), nastavení politik a přidělení privilegovaného účtu k používání konkrétním uživatelům PAM (tj. administrátorům).
6. Použití privilegovaného účtu – Poskytnutí přístupu uživatele PAM (interního/externího administrátora) k privilegovanému účtu prostřednictvím nástroje PAM (tj. v případě že má uživatel přístup schválen).
7. Použití privilegovaného účtu na vyžádání (elevace oprávnění) – Poskytnutí přístupu uživatele PAM (interního/externího administrátora) k privilegovanému účtu na vyžádání na definované časové období (tj. v případě že daný administrátor nemá standardně k privilegovanému účtu oprávnění, přístup je umožněn pouze na dočasnou dobu na základě schválení). Popis bude zahrnovat i případné zavedení nového účtu, a to se zaměřením na externí privilegované uživatele.
8. Použití privilegovaného účtu (nouzový přístup) – Poskytnutí nouzového přístupu v případě, kdy je potřeba získat okamžitě přístup k privilegovanému účtu a není dostupný příslušný odpovědný administrátor.
9. Proces obnovy po havárii – Poskytnutí přístupu k privilegovaným účtům v případě, že PAM infrastruktura nebo její část není dostupná (např. z důvodu havárie nebo jiné neočekávané události).
10. Žádost o změnu konfigurace – Zpracování žádosti o změnu konfigurace PAM (např. vytvoření nové/změna stávající politiky).
11. Revize uživatelů PAM – Provedení revize uživatelů PAM a privilegovaných účtů, kterými jednotliví uživatelé disponují (může být vyřešeno v rámci bodů pro Discovery a Assesment procesy).
12. Sledování či ukončení relace – Sledování aktivní relace nebo její předčasné ukončení odpovědnou osobou (např. člen dohledového týmu).
13. Žádost o nahrávání relace – Zpracování žádosti o nahrávání relací pro konkrétního uživatele (na vyžádání, pokud PAM systém není nastaven k nahrávání všech relací).
14. Žádost o zpřístupnění nahrávky – Zpracování žádosti o zpřístupnění nahrávky relace pořízené pomocí nástroje PAM.

Příloha č. 4

Realizační tým Dodavatele

Skupina pracovníků s uvedením kontaktu (změna pracovníka musí být provedena v souladu s čl. 3.9 této Smlouvy). Jeden pracovník nesmí zastávat více rolí, tzn. že pro role Dodavatel uvede min. 5 různých pracovníků.

|  |  |
| --- | --- |
| **Člen realizačního týmu** | **Kontaktní údaje** |
| **Projektový manažer** | Jméno a příjmení: *neveřejný údaj*  Telefon: *neveřejný údaj*  E-mail: *neveřejný údaj* |
| **Bezpečnostní specialista nástroje PAM** | Jméno a příjmení: *neveřejný údaj*  Telefon: *neveřejný údaj*  E-mail: *neveřejný údaj* |
| **Architekt nástroje PAM** | Jméno a příjmení: *neveřejný údaj*  Telefon: *neveřejný údaj*  E-mail: *neveřejný údaj* |
| **Servisní specialista nástroje PAM 1** | Jméno a příjmení: *neveřejný údaj*  Telefon: *neveřejný údaj*  E-mail: *neveřejný údaj* |
| **Servisní specialista nástroje PAM 2** | Jméno a příjmení: *neveřejný údaj*  Telefon: *neveřejný údaj*  E-mail: *neveřejný údaj* |

Příloha č. 5

Oprávněné osoby

**Za Objednatele:**

ve věcech smluvních:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Role/Pozice | vrchní ředitel sekce informačních technologií |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

ve věcech technických:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Role/Pozice | Odbor kybernetické bezpečnosti ICT (97) |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

ve věcech bezpečnostních:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Role/Pozice | Odbor kybernetické bezpečnosti ICT (97) |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

**Za Dodavatele:**

ve věcech smluvních:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Adresa | NTT Czech Republic s.r.o., Milevská 2095/5, 140 00 Praha 4 |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

ve věcech technických:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Adresa | NTT Czech Republic s.r.o., Milevská 2095/5, 140 00 Praha 4 |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

ve věcech bezpečnostních:

|  |  |
| --- | --- |
| Jméno a příjmení | *neveřejný údaj* |
| Adresa | NTT Czech Republic s.r.o., Milevská 2095/5, 140 00 Praha 4 |
| E-mail | *neveřejný údaj* |
| Telefon | *neveřejný údaj* |

Příloha č. 6

Seznam poddodavatelů

**1)**

**Název:** ANECT a.s.

**Sídlo:** Purkyňova 646/107, Medlánky, 612 00 Brno

**Právní forma:** akciová společnost

**Identifikační číslo:** 25313029

**Rozsah plnění Smlouvy:**

Poddodavatel bude spolupracovat na vedení projektu, zajištění dodávky subscripcí a zajištění L2 podpory na část plnění. Věcný popis části plnění uvažovaného zadat poddodavateli:

* + spolupráce s projektovým řízením,
  + spolupráce na řízení zdrojů,
  + spolupráce na řízení rizik,
  + zajištění dodávky subscripcí.

**2)**

**Název:** ISECO.CZ s.r.o.

**Sídlo:** Bartůňkova 2349/3a, Chodov, 149 00 Praha 4

**Právní forma:** společnost s ručením omezeným

**Identifikační číslo:** 03641074

**Rozsah plnění Smlouvy:**

Poddodavatel bude spolupracovat na implementaci nabízeného řešení. Poddodavatel bude spolupracovat s realizačním týmem na implementaci nabízeného řešení. Bude se jednat o spolupráci na tvorbě analýzy, nastavení pravidel, podpory řešení, přípravě a udržování dokumentace atd.

**3)**

**Název:** NTT Europe GDC s.r.o.

**Sídlo:** Pikrtova 1737/1a, Nusle, 140 00 Praha 4

**Právní forma:** společnost s ručením omezeným

**Identifikační číslo:** 06247377

**Rozsah plnění Smlouvy:**

Poddodavatel bude zajišťovat služby ServiceDesku. Poddodavatel bude zajišťovat přijetí, registraci, aktualizaci a ukončení ticketu.

Příloha č. 7

Cena

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Položka** | **Předmět plnění** | **Typ skenů a dalších služeb** | **Měrná jednotka (MJ)** | **Jednotková cena**  **v Kč bez DPH** | **Počet jednotek** | **Počet let** | **Celkem za 4 roky** |
| 1 | 3.1 | Privilegovaný účet standard - interní admin | Uživatel v AD | *neveřejný údaj* | 250 | 4 | *neveřejný údaj* |
| 2 | 3.1 | Privilegovaný účet remote - externí admin (dodavatel) | Uživatel v AD | *neveřejný údaj* | 350 | 4 | *neveřejný údaj* |
| 3 | 3.1 | Cloudový účet | Uživatel v AD | *neveřejný údaj* | 40 | 4 | *neveřejný údaj* |
| 4 | 3.1 | Správce hesel | Uživatel v AD | *neveřejný údaj* | 100 | 4 | *neveřejný údaj* |
| 5 | 3.1 | Privilegovaný účet pro správu koncových zařízení | Uživatel v AD | *neveřejný údaj* | 100 | 4 | *neveřejný údaj* |
| 6 | 3.1 | Aplikační účet pro automatizované operace | Technický účet | *neveřejný údaj* | 20 | 4 | *neveřejný údaj* |
| 7 | 3.1 | Správa aplikačních účtů v Azure | Konektor do Azure | *neveřejný údaj* | 1 | 4 | *neveřejný údaj* |
| 8 | 3.1 | Správa aplikačních účtů v DevOps prostředí | Konektor do Azure | *neveřejný údaj* | 1 | 4 | *neveřejný údaj* |
| 9 | 3.2 | Základní implementace nástroje PAM do prostředí MPSV | Fixní cena | *neveřejný údaj* | - | - | *neveřejný údaj* |
| 10 | 3.3 | Technická podpora | Fixní cena | *neveřejný údaj* | 1 | 4 | *neveřejný údaj* |
| 11 | 3.4 | Doplňkové služby, rollout na nové systémy a aplikace | Člověkoden | *neveřejný údaj* | 300 | - | *neveřejný údaj* |
| 12 | 3.5 | Vytvoření exitové strategie na přechod k jinému dodavateli | Fixní cena | *neveřejný údaj* | - | - | *neveřejný údaj* |
| **Celková nabídková cena** | |  |  |  |  |  | **74 764 000 Kč** |
|  |  |  |  |  |  |  |  |
| MD = člověkoden v rozsahu 8 pracovních hodin | | |  |  |  |  |  |
| Pro položku 11 (Doplňkové služby) vychází počet MD z předpokládaného odhadu zadavatele a slouží pouze pro kalkulaci nabídkové ceny. | | | | |  |  |  |
| Cena za položku 12 (Služby exitu) musí být stanovena maximálně ve výši 3 % celkového plnění, tzn. že cena nesmí překročit 3 % z celkové nabídkové ceny. | | | | |  |  |  |

Příloha č. 8

Etický kodex

1. **FÉROVÁ HOSPODÁŘSKÁ SOUTĚŽ**

Smluvní strany se tímto společně hlásí k hodnotám férové hospodářské soutěže, vedené etickými postupy a prostředky a odmítají chování mající charakter pletich, zjednávání výhod, přijímání či poskytování úplatků v jakékoliv formě (finanční prostředky, dary, výhody, aj.), a to bez ohledu na skutečnost, dosahuje-li intenzity relevantní z pohledu trestního práva.

1. **STŘET ZÁJMŮ**

Smluvní strany se zavazují předcházet jakémukoliv střetu zájmů při navazování obchodních vztahů, a to v jakékoliv formě, čímž se rozumí zejména propojení členů managementu, ať už na úrovni rodinné, bez ohledu na stupeň příbuzenství, politické, přátelské či jiné. Kromě prokazatelného střetu zájmů se smluvní strany zavazují v maximální možné míře předcházet i vzniku důvodného podezření, které má potenciál, aby dalo vzniknout negativnímu obrazu dotčených v mínění široké veřejnosti.

1. **PŘIJATELNÉ PRACOVNÍ PODMÍNKY**

Smluvní strany se hlásí k hodnotám zajištění důstojných pracovních podmínek osob podílejících se na plnění dle Smlouvy, a to zejména jedná-li se o nízko kvalifikované profese (vyloučeny však nejsou ani jakékoliv jiné skupiny zaměstnanců). Smluvní strany se zavazují zejména striktně dodržovat veškerá ustanovení právních předpisů, která se týkají minimální i zaručené mzdy, bezpečnosti práce, přijatelných pracovních podmínek a poskytování spravedlivé odměny za práci. Součástí společně přejatého závazku je i to, že se smluvní strany vyvarují jakékoliv snahy, ať už zjevné či skryté, která by směřovala k obcházení pracovněprávních předpisů.

1. **ZÁKAZ DISKRIMINACE A ZAJIŠTĚNÍ ROVNÝCH PŘÍLEŽITOSTÍ**

Smluvní strany se hlásí k hodnotám odsuzujícím diskriminaci v jakékoliv podobě, resp. k hodnotám zajišťujícím rovné příležitosti všech skupin osob bez ohledu na rozdíly mezi nimi, čímž se rozumí zejména potírání nerovného zacházení vznikajícího na základě rasy, etnického původu, pohlaví, sexuální orientace, přesvědčení či světového názoru. Za nežádoucí a nepřijatelné jednání je považováno rovněž i neposkytování rovných příležitostí ve vedení společnosti a jiných řídících funkcí a při odměňování.

1. **EKONOMICKÉ ASPEKTY**

Smluvní strany se hlásí k hodnotám odsuzujícím jednání nežádoucí z ekonomického hlediska, čímž se rozumí zejména snaha o praní špinavých peněz, snaha o legalizaci nezákonných   
a neetických zisků, důvěryhodnost dodavatele z hlediska sídla podnikání a realizace finančních transakcí (sídlo dodavatele nebo platební instituce, kterou používá, se nesmí nacházet v zemi zapsané na seznamu zemí nespolupracujících daňových jurisdikcí vytvořených Evropskou unií). Dodavatel se zavazuje, že všem svým obchodním partnerům v pod-dodavatelském řetězci zajistí férové smluvní podmínky, tím se rozumí zejména nastavení stejné nebo kratší splatnosti faktur (a její dodržování), jaká je ujednána ve Smlouvě, resp. podpora malých a středních podniků.

1. **EKOLOGICKÉ ASPEKTY**

Smluvní strany se hlásí k hodnotám odsuzujícím jednání nežádoucí z ekologického hlediska, čímž se rozumí zejména jakékoliv jednání, které je v rozporu se správním či trestním právem a jehož cílem, vedlejším efektem či konečným nebo dílčím důsledkem je poškozování životního prostředí v jakékoliv formě, ať už z hlediska ekologické zátěže, udržitelnosti, nežádoucího vlivu na lidský organismus či živou a neživou přírodu, vypouštění zplodin do ovzduší, nebo jakoukoliv obdobnou činnost.

Příloha č. 9

Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)

Za účelem povinností stanovených Objednateli jakožto povinné osobě vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), se Dodavatel zavazuje nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy 10 této Smlouvy.

Dodavatel se zavazuje plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této Příloze 10 této Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

**Čl. 1 Systém řízení bezpečnosti informací**

Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 3 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**VKB**“), které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

* 1. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění.
  2. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
  3. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.
  4. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
  5. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

**Čl. 2 Řízení aktiv**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této Smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této Smlouvy, systémy ICT, moduly, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do 30 dnů od podpisu této smlouvy a následně na vyžádání, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

**Čl. 3 Řízení rizik**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
   2. V minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
      1. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok
      2. Identifikaci a hodnocení rizik s vazbou na předmět plnění
      3. Realizovaná bezpečnostní opatření
      4. Nepokrytá bezpečnostní rizika a návrh opatření
      5. Vyhodnocení bezpečnostních událostí a incidentů
      6. Aktuální stav souladu Dodavatele s těmito Kybernetickými požadavky

**Čl. 4 Organizační bezpečnost**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Jmenovat nejpozději do 30 dnů po uzavření této smlouvy odpovědnou kontaktní osobu pro kybernetickou bezpečnost pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Smluvními stranami (dále také jen „**Kontaktní osoba**“), pokud tato osoba není explicitně uvedena mezi oprávněnými osobami určenými touto Smlouvou. Kontaktní osobu sdělí Dodavatel písemně Objednateli v téže lhůtě.
   2. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

**Čl. 5 Řízení dodavatelů**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Dodavatel zavazuje doložit Objednateli do 10 dnů od podpisu příslušné Prováděcí smlouvy, na jejímž plnění se budou poddodavatelé podílet v případě služeb Rozvoje, nebo do 10 dnů od počátku poskytování jiných služeb, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.
   2. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit nad rámec čl. 18 Smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této smlouvy) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

**Čl. 6 Bezpečnost lidských zdrojů**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Zajistit, aby Kontaktní osoba nebo osoba oprávněná jednat ve věcech bezpečnostních nejpozději do 30 dnů od uzavření smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Dodavatel byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.
   2. Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Dodavatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.
   3. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
   4. Zajistit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:
      1. Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva);
      2. Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
      3. Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
      4. Nenavštěvovali internetové stránky s eticky nevhodným obsahem;
      5. Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
      6. Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;
      7. Nepodíleli se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.
2. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele *zpracování osobních údajů* pracovníků Dodavatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

**Čl. 7 Řízení provozu a komunikací**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
   2. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.
   3. Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a autorský zákon.

**Čl. 8 Řízení změn**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
   2. Aktivně spolupracovat při testování významné změny.

**Čl. 9 Řízení přístupu**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
   2. Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Dodavatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této smlouvy a 2 roky po ukončení její platnosti.
   3. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT Objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
   4. Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
   5. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují do prostředí Objednatele.
2. Dodavatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Dodavatele / poddodavatele Dodavatele zaevidované v *Active Directory MPSV* (registr identit), a to na základě požadavku Dodavatele na přístup.
3. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové.
4. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

**Čl. 10 Akvizice, vývoj a údržba**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
   2. Předat Objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
      1. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů
      2. dokumentaci obsahující popis autorizačního konceptu a oprávnění
      3. dokumentaci obsahující instalační a konfigurační postupy

**Čl. 11 Zvládání kybernetických bezpečnostních událostí a incidentů**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.
   2. Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby nebo osoby oprávněné jednat ve věcech bezpečnostních.
   3. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
   4. V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele.
   5. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.
   6. Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
2. Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné škody či jiné újmy Dodavateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená ve Smlouvě nejsou tímto ustanovením dotčena.

**Čl. 12 Řízení kontinuity činností**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
   2. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.

**Čl. 13 Kontrola a audit**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Úřadu dle § 23 ZKB.

**Čl. 14 Fyzická bezpečnost**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 17 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.
   2. V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Dodavatel seznámen.

**Čl. 15 Bezpečnostní nástroje**

1. Dodavatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:
   1. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
   2. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.
   3. Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této smlouvě.
   4. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Dodavatele.
   5. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:
      1. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
      2. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
      3. Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
      4. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
      5. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.
   6. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.
   7. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
   8. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.
   9. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
   10. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
   11. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.
2. Dodavatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Dodavatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato smlouva nestanoví jinak.
3. Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty Objednatele, se kterými byl Dodavatel seznámen.

Příloha č. 10

Dotazník pro hodnocení technické úrovně kybernetické bezpečnosti

NTT Czech Republic s.r.o.

|  |  |  |
| --- | --- | --- |
| **SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY** | | **0** |
| 1 | Které standardy a nejlepší praktiky dodavatel aplikuje na své ICT prostředí, které bude využívat pro nabízené plnění (systémy řízení nemusí být certifikované): | |
| a. | ISO 9001 | ANO |
| b. | ISO 22301, BS 25999 | ANO |
| c. | ISO/IEC 20000-1, ITIL, CobIT | ANO |
| **SEKCE B – ZÁKLADNÍ OPATŘENÍ** | | |
| 2 | Je jmenovaný manažer bezpečnosti nebo jiná určená osoba s ekvivalentní odpovědností, která zajišťuje kybernetickou bezpečnost ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 3 | Byl v posledních 12ti měsících proveden třetí stranou audit či bezpečnostní analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti a v rozsahu byla aktiva z ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 4 | Realizoval dodavatel v posledních 12ti měsících hodnocení kybernetických rizik v ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 5 | Které oblasti pokrývá dokument bezpečnostní politiky, v jehož rozsahu je ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | |
| a. | Procesy řízení rizik | ANO |
| b. | Klasifikace aktiv | ANO |
| c. | Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti | ANO |
| d. | Ochrana osobních údajů | ANO |
| e. | Identifikace a autentizace uživatelů | ANO |
| f. | Přístup k datům na základě rolí (RBAC, Role Based Access Control) | ANO |
| g. | Řízení privilegovaných přístupů | ANO |
| h. | Ochrana koncových stanic | ANO |
| i. | Ochrana mobilních zařízení a vzdáleného přístupu | ANO |
| j. | Ochrana emailu a vnitrofiremní komunikace (instant messaging) | ANO |
| k. | Ochrana přístupu do internetu | ANO |
| l. | Bezpečnost cloudového prostředí (Azure, AWS, M365 apod.) | ANO |
| m. | Ochrana médií | ANO |
| n. | Procesy řízení změn | ANO |
| o. | Ochrana bezdrátových sítí a komunikace | ANO |
| p. | Fyzická bezpečnost informačních aktiv | ANO |
| q. | Bezpečnostní školení koncových uživatelů a administrátorů | ANO |
| r. | Ochrana proti škodlivému softwaru | ANO |
| s. | Ochrana při výměně dat | ANO |
| t. | Procesy zvládání kybernetických incidentů | ANO |
| u. | Procesy řízení rizik dodavatelů | ANO |
| v. | Bezpečnost lidských zdrojů | ANO |
| w. | Bezpečnostní audity a analýzy | ANO |
| x | Řízení kontinuity činností a havarijní plánování | ANO |
| **SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE** | | |
| 6 | Které níže uvedené bezpečnostní technologie provozuje dodavatel s cílem předcházet bezpečnostním hrozbám v rámci ICT prostředí, které bude využívat pro nabízené plnění? | |
| a. | Antivirový software na pracovních stanicích | ANO |
| b. | Antivirový software na mobilních zařízeních | NE |
| c. | Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System) | ANO |
| d. | Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management) | ANO |
| e. | Více-faktorová autentizace | ANO |
| f. | Automatizovaný nástroj pro řízení technologických zranitelností | ANO |
| g. | Nástroj pro řízení přístupu k síti (NAC, Network Access Control) | ANO |
| h. | Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service) | ANO |
| i. | Šifrovací nástroje a techniky | ANO |
| j. | Firewall | ANO |
| k. | Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management) | ANO |
| 7 | Bylo ICT prostředí, které bude dodavatel využívat pro nabízené plnění, v posledních 12ti měsících podrobeno penetračnímu testování? | ANO |
| **SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ** | | |
| 8 | Je zaveden proces zvládání bezpečnostních incidentů pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 9 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v identifikaci bezpečnostních incidentů? | ANO |
| **SEKCE E – PROCES ŘÍZENÍ KONTINUITY** | | |
| 10 | Jsou vytvořeny plány kontinuity a obnovy pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 11 | Testuje dodavatel pravidelně (min. 1x za 24 měsíců) plány kontinuity a obnovy pro ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 12 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v oblasti řízení kontinuity, tzn. že se uživatelé účastní pravidelných testů a jsou prokazatelně seznamováni s postupy pro kontinuity a obnovu? | ANO |
| **SEKCE F – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ** | | |
| 13 | Je zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro všechny uživatele s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 14 | Jsou všichni uživatelé s přístupem do ICT prostředí, které bude využívat pro nabízené plnění, vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? | ANO |
| 15 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání individuální dohody o mlčenlivosti (NDA)? | ANO |
| 16 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání etického kodexu? | ANO |

Dotazník pro hodnocení technické úrovně kybernetické bezpečnosti

NTT Europe GDC s.r.o.

|  |  |  |
| --- | --- | --- |
| **SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY** | | **0** |
| 1 | Které standardy a nejlepší praktiky dodavatel aplikuje na své ICT prostředí, které bude využívat pro nabízené plnění (systémy řízení nemusí být certifikované): | |
| a. | ISO 9001 | ANO |
| b. | ISO 22301, BS 25999 | ANO |
| c. | ISO/IEC 20000-1, ITIL, CobIT | ANO |
| **SEKCE B – ZÁKLADNÍ OPATŘENÍ** | | |
| 2 | Je jmenovaný manažer bezpečnosti nebo jiná určená osoba s ekvivalentní odpovědností, která zajišťuje kybernetickou bezpečnost ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 3 | Byl v posledních 12ti měsících proveden třetí stranou audit či bezpečnostní analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti a v rozsahu byla aktiva z ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 4 | Realizoval dodavatel v posledních 12ti měsících hodnocení kybernetických rizik v ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 5 | Které oblasti pokrývá dokument bezpečnostní politiky, v jehož rozsahu je ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | |
| a. | Procesy řízení rizik | ANO |
| b. | Klasifikace aktiv | ANO |
| c. | Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti | ANO |
| d. | Ochrana osobních údajů | ANO |
| e. | Identifikace a autentizace uživatelů | ANO |
| f. | Přístup k datům na základě rolí (RBAC, Role Based Access Control) | ANO |
| g. | Řízení privilegovaných přístupů | ANO |
| h. | Ochrana koncových stanic | ANO |
| i. | Ochrana mobilních zařízení a vzdáleného přístupu | ANO |
| j. | Ochrana emailu a vnitrofiremní komunikace (instant messaging) | ANO |
| k. | Ochrana přístupu do internetu | ANO |
| l. | Bezpečnost cloudového prostředí (Azure, AWS, M365 apod.) | ANO |
| m. | Ochrana médií | ANO |
| n. | Procesy řízení změn | ANO |
| o. | Ochrana bezdrátových sítí a komunikace | ANO |
| p. | Fyzická bezpečnost informačních aktiv | ANO |
| q. | Bezpečnostní školení koncových uživatelů a administrátorů | ANO |
| r. | Ochrana proti škodlivému softwaru | ANO |
| s. | Ochrana při výměně dat | ANO |
| t. | Procesy zvládání kybernetických incidentů | ANO |
| u. | Procesy řízení rizik dodavatelů | ANO |
| v. | Bezpečnost lidských zdrojů | ANO |
| w. | Bezpečnostní audity a analýzy | ANO |
| x | Řízení kontinuity činností a havarijní plánování | ANO |
| **SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE** | | |
| 6 | Které níže uvedené bezpečnostní technologie provozuje dodavatel s cílem předcházet bezpečnostním hrozbám v rámci ICT prostředí, které bude využívat pro nabízené plnění? | |
| a. | Antivirový software na pracovních stanicích | ANO |
| b. | Antivirový software na mobilních zařízeních | NE |
| c. | Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System) | ANO |
| d. | Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management) | ANO |
| e. | Více-faktorová autentizace | ANO |
| f. | Automatizovaný nástroj pro řízení technologických zranitelností | ANO |
| g. | Nástroj pro řízení přístupu k síti (NAC, Network Access Control) | ANO |
| h. | Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service) | ANO |
| i. | Šifrovací nástroje a techniky | ANO |
| j. | Firewall | ANO |
| k. | Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management) | ANO |
| 7 | Bylo ICT prostředí, které bude dodavatel využívat pro nabízené plnění, v posledních 12ti měsících podrobeno penetračnímu testování? | ANO |
| **SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ** | | |
| 8 | Je zaveden proces zvládání bezpečnostních incidentů pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 9 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v identifikaci bezpečnostních incidentů? | ANO |
| **SEKCE E – PROCES ŘÍZENÍ KONTINUITY** | | |
| 10 | Jsou vytvořeny plány kontinuity a obnovy pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 11 | Testuje dodavatel pravidelně (min. 1x za 24 měsíců) plány kontinuity a obnovy pro ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 12 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v oblasti řízení kontinuity, tzn. že se uživatelé účastní pravidelných testů a jsou prokazatelně seznamováni s postupy pro kontinuity a obnovu? | ANO |
| **SEKCE F – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ** | | |
| 13 | Je zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro všechny uživatele s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 14 | Jsou všichni uživatelé s přístupem do ICT prostředí, které bude využívat pro nabízené plnění, vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? | ANO |
| 15 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání individuální dohody o mlčenlivosti (NDA)? | ANO |
| 16 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání etického kodexu? | ANO |

Dotazník pro hodnocení technické úrovně kybernetické bezpečnosti

ANECT a.s.

|  |  |  |
| --- | --- | --- |
| **SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY** | | **0** |
| 1 | Které standardy a nejlepší praktiky dodavatel aplikuje na své ICT prostředí, které bude využívat pro nabízené plnění (systémy řízení nemusí být certifikované): | |
| a. | ISO 9001 | ANO |
| b. | ISO 22301, BS 25999 | ANO |
| c. | ISO/IEC 20000-1, ITIL, CobIT | ANO |
| **SEKCE B – ZÁKLADNÍ OPATŘENÍ** | | |
| 2 | Je jmenovaný manažer bezpečnosti nebo jiná určená osoba s ekvivalentní odpovědností, která zajišťuje kybernetickou bezpečnost ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 3 | Byl v posledních 12ti měsících proveden třetí stranou audit či bezpečnostní analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti a v rozsahu byla aktiva z ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 4 | Realizoval dodavatel v posledních 12ti měsících hodnocení kybernetických rizik v ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 5 | Které oblasti pokrývá dokument bezpečnostní politiky, v jehož rozsahu je ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | |
| a. | Procesy řízení rizik | ANO |
| b. | Klasifikace aktiv | ANO |
| c. | Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti | ANO |
| d. | Ochrana osobních údajů | ANO |
| e. | Identifikace a autentizace uživatelů | ANO |
| f. | Přístup k datům na základě rolí (RBAC, Role Based Access Control) | ANO |
| g. | Řízení privilegovaných přístupů | ANO |
| h. | Ochrana koncových stanic | ANO |
| i. | Ochrana mobilních zařízení a vzdáleného přístupu | ANO |
| j. | Ochrana emailu a vnitrofiremní komunikace (instant messaging) | ANO |
| k. | Ochrana přístupu do internetu | ANO |
| l. | Bezpečnost cloudového prostředí (Azure, AWS, M365 apod.) | ANO |
| m. | Ochrana médií | ANO |
| n. | Procesy řízení změn | ANO |
| o. | Ochrana bezdrátových sítí a komunikace | ANO |
| p. | Fyzická bezpečnost informačních aktiv | ANO |
| q. | Bezpečnostní školení koncových uživatelů a administrátorů | ANO |
| r. | Ochrana proti škodlivému softwaru | ANO |
| s. | Ochrana při výměně dat | ANO |
| t. | Procesy zvládání kybernetických incidentů | ANO |
| u. | Procesy řízení rizik dodavatelů | ANO |
| v. | Bezpečnost lidských zdrojů | ANO |
| w. | Bezpečnostní audity a analýzy | ANO |
| x | Řízení kontinuity činností a havarijní plánování | ANO |
| **SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE** | | |
| 6 | Které níže uvedené bezpečnostní technologie provozuje dodavatel s cílem předcházet bezpečnostním hrozbám v rámci ICT prostředí, které bude využívat pro nabízené plnění? | |
| a. | Antivirový software na pracovních stanicích | ANO |
| b. | Antivirový software na mobilních zařízeních | ANO |
| c. | Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System) | ANO |
| d. | Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management) | ANO |
| e. | Více-faktorová autentizace | ANO |
| f. | Automatizovaný nástroj pro řízení technologických zranitelností | ANO |
| g. | Nástroj pro řízení přístupu k síti (NAC, Network Access Control) | ANO |
| h. | Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service) | ANO |
| i. | Šifrovací nástroje a techniky | ANO |
| j. | Firewall | ANO |
| k. | Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management) | ANO |
| 7 | Bylo ICT prostředí, které bude dodavatel využívat pro nabízené plnění, v posledních 12ti měsících podrobeno penetračnímu testování? | ANO |
| **SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ** | | |
| 8 | Je zaveden proces zvládání bezpečnostních incidentů pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 9 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v identifikaci bezpečnostních incidentů? | ANO |
| **SEKCE E – PROCES ŘÍZENÍ KONTINUITY** | | |
| 10 | Jsou vytvořeny plány kontinuity a obnovy pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 11 | Testuje dodavatel pravidelně (min. 1x za 24 měsíců) plány kontinuity a obnovy pro ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 12 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v oblasti řízení kontinuity, tzn. že se uživatelé účastní pravidelných testů a jsou prokazatelně seznamováni s postupy pro kontinuity a obnovu? | ANO |
| **SEKCE F – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ** | | |
| 13 | Je zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro všechny uživatele s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 14 | Jsou všichni uživatelé s přístupem do ICT prostředí, které bude využívat pro nabízené plnění, vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? | ANO |
| 15 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání individuální dohody o mlčenlivosti (NDA)? | ANO |
| 16 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání etického kodexu? | ANO |

Dotazník pro hodnocení technické úrovně kybernetické bezpečnosti

ISECO.CZ s.r.o.

|  |  |  |
| --- | --- | --- |
| **SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY** | | **0** |
| 1 | Které standardy a nejlepší praktiky dodavatel aplikuje na své ICT prostředí, které bude využívat pro nabízené plnění (systémy řízení nemusí být certifikované): | |
| a. | ISO 9001 | ANO |
| b. | ISO 22301, BS 25999 | ANO |
| c. | ISO/IEC 20000-1, ITIL, CobIT | ANO |
| **SEKCE B – ZÁKLADNÍ OPATŘENÍ** | | |
| 2 | Je jmenovaný manažer bezpečnosti nebo jiná určená osoba s ekvivalentní odpovědností, která zajišťuje kybernetickou bezpečnost ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 3 | Byl v posledních 12ti měsících proveden třetí stranou audit či bezpečnostní analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti a v rozsahu byla aktiva z ICT prostředí, které bude využívat pro nabízené plnění? | NE |
| 4 | Realizoval dodavatel v posledních 12ti měsících hodnocení kybernetických rizik v ICT prostředí, které bude využívat pro nabízené plnění? | ANO |
| 5 | Které oblasti pokrývá dokument bezpečnostní politiky, v jehož rozsahu je ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | |
| a. | Procesy řízení rizik | ANO |
| b. | Klasifikace aktiv | ANO |
| c. | Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti | ANO |
| d. | Ochrana osobních údajů | ANO |
| e. | Identifikace a autentizace uživatelů | ANO |
| f. | Přístup k datům na základě rolí (RBAC, Role Based Access Control) | ANO |
| g. | Řízení privilegovaných přístupů | ANO |
| h. | Ochrana koncových stanic | ANO |
| i. | Ochrana mobilních zařízení a vzdáleného přístupu | ANO |
| j. | Ochrana emailu a vnitrofiremní komunikace (instant messaging) | ANO |
| k. | Ochrana přístupu do internetu | ANO |
| l. | Bezpečnost cloudového prostředí (Azure, AWS, M365 apod.) | ANO |
| m. | Ochrana médií | ANO |
| n. | Procesy řízení změn | ANO |
| o. | Ochrana bezdrátových sítí a komunikace | ANO |
| p. | Fyzická bezpečnost informačních aktiv | ANO |
| q. | Bezpečnostní školení koncových uživatelů a administrátorů | ANO |
| r. | Ochrana proti škodlivému softwaru | ANO |
| s. | Ochrana při výměně dat | ANO |
| t. | Procesy zvládání kybernetických incidentů | ANO |
| u. | Procesy řízení rizik dodavatelů | ANO |
| v. | Bezpečnost lidských zdrojů | ANO |
| w. | Bezpečnostní audity a analýzy | ANO |
| x | Řízení kontinuity činností a havarijní plánování | ANO |
| **SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE** | | |
| 6 | Které níže uvedené bezpečnostní technologie provozuje dodavatel s cílem předcházet bezpečnostním hrozbám v rámci ICT prostředí, které bude využívat pro nabízené plnění? | |
| a. | Antivirový software na pracovních stanicích | NE |
| b. | Antivirový software na mobilních zařízeních | NE |
| c. | Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System) | ANO |
| d. | Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management) | ANO |
| e. | Více-faktorová autentizace | ANO |
| f. | Automatizovaný nástroj pro řízení technologických zranitelností | ANO |
| g. | Nástroj pro řízení přístupu k síti (NAC, Network Access Control) | ANO |
| h. | Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service) | ANO |
| i. | Šifrovací nástroje a techniky | ANO |
| j. | Firewall | ANO |
| k. | Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management) | ANO |
| 7 | Bylo ICT prostředí, které bude dodavatel využívat pro nabízené plnění, v posledních 12ti měsících podrobeno penetračnímu testování? | NE |
| **SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ** | | |
| 8 | Je zaveden proces zvládání bezpečnostních incidentů pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 9 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v identifikaci bezpečnostních incidentů? | ANO |
| **SEKCE E – PROCES ŘÍZENÍ KONTINUITY** | | |
| 10 | Jsou vytvořeny plány kontinuity a obnovy pro ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 11 | Testuje dodavatel pravidelně (min. 1x za 24 měsíců) plány kontinuity a obnovy pro ICT prostředí, které bude využívat pro nabízené plnění? | NE |
| 12 | Jsou uživatelé s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, pravidelně (min. 1x za 24 měsíců) vzděláváni v oblasti řízení kontinuity, tzn. že se uživatelé účastní pravidelných testů a jsou prokazatelně seznamováni s postupy pro kontinuity a obnovu? | ANO |
| **SEKCE F – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ** | | |
| 13 | Je zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro všechny uživatele s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění? | ANO |
| 14 | Jsou všichni uživatelé s přístupem do ICT prostředí, které bude využívat pro nabízené plnění, vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? | ANO |
| 15 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání individuální dohody o mlčenlivosti (NDA)? | NE |
| 16 | Je po uživatelích s přístupem do ICT prostředí, které bude dodavatel využívat pro nabízené plnění, vyžadováno podepsání etického kodexu? | NE |